FortiWeb™ Web Application Firewall

Version 4.0 MR2
CLI Reference

FORTINET.

FortiWeb™ Web Application Firewall CLI Reference

Version 4.0 MR2

Revision 2

15 March 2011

© Copyright 2011 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

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 9

Registering your Fortinet product 9

Scope 10

Characteristics of XML threats 10

Characteristics of HTTP threats 11

Customer service and technical support 13

Training 13

Documentation 13

Documentation Conventions 14

IP addresses 14

Notes, Tips and Cautions 14

Typographic conventions 15

Command syntax conventions 15

What's new 17

Using the CLI 19

Connecting to the CLI 19

Connecting to the CLI using a local console 19

Enabling access to the CLI through the network (SSH or Telnet) 20

Connecting to the CLI using SSH 22

Connecting to the CLI using Telnet 23

Command syntax 23

Subcommands 26

Permissions 29

Tips and tricks 30

Help 31

Shortcuts and key commands 31

Command abbreviation 32

Environment variables 32

Special characters 32

Language support & regular expressions 33

Screen paging 35

Baud rate 35

Editing the configuration file on an external host 35

config 37

log alertemail 39

log attack-log 40

log custom-sensitive-rule 42

log disk 44

log email-policy **46**
log event-log **49**
log forti-analyzer **50**
log fortianalyzer-policy **51**
log memory **52**
log reports **53**
log sensitive **61**
log syslogd **62**
log syslog-policy **64**
log traffic-log **65**
log trigger-policy **66**
router setting **68**
router static **69**
server-policy allow-hosts **71**
server-policy custom-application application-policy **74**
server-policy custom-application url-replacer **76**
server-policy health **78**
server-policy http-content-routing-policy **80**
server-policy http-conversion-policy **82**
server-policy pattern custom-data-type **84**
server-policy pattern custom-susp-url **85**
server-policy pattern custom-susp-url-rule **86**
server-policy pattern data-type-group **87**
server-policy pattern suspicious-url-rule **90**
server-policy policy **92**
server-policy pserver **101**
server-policy pservers **102**
server-policy service custom **106**
server-policy service predefined **107**
server-policy vserver **108**
system accprofile **110**
system admin **113**
system autoupdate override **115**
system autoupdate schedule **116**
system autoupdate tunneling **118**
system certificate ca **119**

system certificate ca-group **120**
system certificate crl **121**
system certificate intermediate-certificate **122**
system certificate intermediate-certificate-group **123**
system certificate local **124**
system certificate remote **126**
system certificate verify **127**
system conf-sync **128**
system console **129**
system dns **130**
system dos-prevention **132**
system fail-open **133**
system global **134**
system ha **138**
system interface **142**
system raid **146**
system report-lang **147**
system settings **148**
system snmp community **150**
system snmp sysinfo **154**
system v-zone **156**
user ldap-user **158**
user local-user **160**
user ntlm-user **161**
user radius-user **162**
user user-group **163**
wad website **164**
waf allow-method-exceptions **167**
waf allow-method-policy **169**
waf brute-force-login **170**
waf custom-protection-group **173**
waf custom-protection-rule **174**
waf file-upload-restriction-policy **176**
waf file-upload-restriction-rule **177**
waf hidden-fields-protection **179**
waf hidden-fields-rule **180**

waf http-authen http-authen-policy **183**
waf http-authen http-authen-rule **185**
waf http-constraints-exceptions **187**
waf http-protocol-parameter-restriction **190**
waf input-rule **193**
waf ip-list **198**
waf page-access-rule **200**
waf parameter-validation-rule **203**
waf robot-control **205**
waf server-protection-exception **209**
waf server-protection-rule **212**
waf start-pages **220**
waf url-access url-access-policy **223**
waf url-access url-access-rule **225**
waf url-rewrite url-rewrite-policy **227**
waf url-rewrite url-rewrite-rule **228**
waf web-custom-robot **231**
waf web-protection-profile autolearning-profile **232**
waf web-protection-profile inline-protection **234**
waf web-protection-profile offline-protection **239**
waf web-robot **242**
wvs policy **243**
wvs profile **245**
wvs schedule **246**
xml-protection filter-rule **247**
xml-protection intrusion-prevention-rule **250**
xml-protection key-file **252**
xml-protection key-management **253**
xml-protection period-time onetime **254**
xml-protection period-time recurring **255**
xml-protection schema-files **256**
xml-protection web-service **257**
xml-protection web-service-group **258**
xml-protection wsdl-content-routing-table **259**
xml-protection xml-protection-profile **260**

diagnose 265
debug application 266
debug cli 267
debug console 268
debug crashlog 269
debug disable/enable 270
debug failopen-poweron-bypass 271
debug flow 272
debug info 273
debug proxy 274
debug reset 275
debug upload 276
hardware 277
network arp 278
network ip 279
network route 280
network sniffer 281
network tcp/udp 283
system flash 284
system kill 285
system mount 286
system raid 287
system top 288
execute 291
backup 292
create-raid 293
date 294
factoryreset 295
ping 296
ping-options 298
reboot 300
restore 301
shutdown 302
time 303
traceroute 304
update-now 306

get **307**
router all **309**
system logged-users **310**
system performance **311**
system status **312**
show **313**
Index **315**

Introduction

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

FortiWeb units are designed specifically to protect web servers.

The FortiWeb family of web application firewalls provides specialized, layered application threat protection. FortiWeb's integrated web application and XML firewalls protect your web-based applications and internet-facing data from attack and data loss. Using advanced techniques to provide bidirectional protection against sophisticated threats like SQL injection and cross-site scripting, FortiWeb helps you prevent identity theft, financial fraud and corporate espionage. FortiWeb delivers the technology you need to monitor and enforce government regulations, industry best practices, and internal policies.

FortiWeb significantly reduces deployment costs by consolidating a web application firewall, XML filtering, web traffic acceleration, and application traffic balancing into a single device. It drastically reduces the time required to protect your internet-facing data and eases the challenges associated with policy enforcement and regulatory compliance.

Its intelligent, application-aware, load-balancing engine:

- increases application performance
- improves resource utilization
- improves application stability
- reduces server response times.

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 the following topics:

- Registering your Fortinet product
- Scope
- Characteristics of XML threats
- Characteristics of HTTP threats
- Scope
- Documentation
- Documentation Conventions

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.

Scope

This document describes how to use the command line interface (CLI) of the FortiWeb unit. It assumes that you have already successfully installed the FortiWeb unit and completed basic setup by following the instructions in the *FortiWeb Installation Guide*.

At this stage:

- The FortiWeb unit is integrated into your network and is powered on.
- You have completed firmware updates, if applicable.
- You configured a port on the FortiWeb unit during installation. You must configure at least one port to access the web-based manager or CLI.
- You have administrative access to the web-based manager through a browser, and you can log in successfully.
- You have given the default administrator a password.
- You have set the operation mode.
- You have configured additional network interfaces.
- You have configured the system time.
- You have configured the DNS.
- You have configured a default gateway.
- You have configured basic logging.
- You have created at least one server policy.

If you missed any of the above steps, consult the *FortiWeb Installation Guide*.

Once that basic installation and setup is complete, you can use this document to learn how to use the CLI to:

- maintain the FortiWeb unit, including backups
- reconfigure and expand features that were configured during installation
- configure advanced features, such as customized antispam scans, email archiving, logging, and reporting

This document does ***not*** cover the web-based manager. For information on the web-based manager, see the *FortiWeb Administration Guide*.

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 1 lists several XML-related threats and describes how FortiWeb units protect against them.

Table 1: XML-related threats

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 2 lists several Web-related threats and describes how FortiWeb units protect against them.

Table 2: 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 2: 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

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet products install quickly, configure easily, and operate 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.

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.

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.

Comments on Fortinet technical documentation

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

Documentation 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.

Notes, Tips and Cautions

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

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

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

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

Typographic conventions

Fortinet documentation uses the following typographical conventions:

Table 3: 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`
	`  set primary <address_ipv4>`
	`end`

CLI output	`FGT-602803030703 # get system settings`
	`comments  : (null)`
	`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>` `<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.

For command syntax conventions such as braces, brackets, and command constraints such as `<address_ipv4>`, see “Notation” on page 25.

What's new

This document describes the CLI commands available with FortiWeb Version 4.0 MR2. The table below identifies the commands which have changed since FortiWeb Version 4.0 MR1 Patch 1.

Command	Change
config alertemail filter	Obsolete.
config alertmail setting	Obsolete.
config log forti-analyzer	New.
config log fortianalyzer-policy	New.
config server-policy custom-application application-policy	New.
config server-policy custom-application url-replacer	New.
config server-policy service predefined	New.
config system conf-sync	New.
config system alertemail	Obsolete.
config user radius-user	New.
config waf allow-method-policy	New.
config waf black-ipaddress-list	Obsolete. Replaced by config waf ip-list.
config waf file-upload-restriction-policy	New.
config waf file-upload-restriction-rule	New.
config waf http-constraints-exceptions	New.
config waf ip-list	New. Replaces config waf black-ipaddress-list and config waf trust-ipaddress-list.
config waf trust-ipaddress-list	Obsolete. Replaced by config waf ip-list.
config wvs policy	New.
config wvs profile	New.
config wvs schedule	New.
diagnose ip address list	Obsolete.
diagnose debug	New. Includes several new debug commands.
diagnose hardware	New.
diagnose network	New. Includes several new commands.
diagnose network sniffer	New syntax for diagnose sniffer packet.
execute update-now	New.

Using the CLI

The command line interface (CLI) is an alternative to the web-based manager.

Use can use either interface or both to configure the FortiWeb unit. In the web-based manager, you use buttons, icons, and forms, while, in the CLI, you either type text commands or upload batches of commands from a text file, like a configuration script.

If you are new to Fortinet products, or if you are new to the CLI, this section can help you to become familiar.

This section contains the following topics:

- Connecting to the CLI
- Command syntax
- Subcommands
- Permissions
- Tips and tricks

Connecting to the CLI

You can access the CLI in two ways:

- **Locally**: Connect your computer directly to the FortiWeb unit's console port.
- **Through the network:** Connect your computer through any network attached to one of the FortiWeb unit's network ports. To connect using an Secure Shell (SSH) or Telnet client, enable the network interface for Telnet or SSH administrative access. Enable HTTP/HTTPS administrative access to connect using the *CLI Console* widget in the web-based manager.

Local access is required in some cases.

- If you are installing your FortiWeb unit for the first time and it is not yet configured to connect to your network, you may only be able to connect to the CLI using a local serial console connection unless you reconfigure your computer's network settings for a peer connection. See the *FortiWeb Administration Guide*.
- Restoring the firmware utilizes a boot interrupt. Network access to the CLI is not available until ***after*** the boot process completes, and therefore local CLI access is the only viable option.

This section includes the following:

- Connecting to the CLI using a local console
- Enabling access to the CLI through the network (SSH or Telnet)
- Connecting to the CLI using SSH
- Connecting to the CLI using Telnet

Connecting to the CLI using a local console

Local console connections to the CLI are formed by directly connecting your management computer or console to the FortiWeb unit, using its DB-9 console port.

Requirements

- a computer with an available serial communications (COM) port
- the null modem cable included in your FortiWeb package
- terminal emulation software such as HyperTerminal for Microsoft Windows

Note: The following procedure describes connection using Microsoft HyperTerminal software; steps may vary with other terminal emulators.

To connect to the CLI using a local serial console connection

1. Using the null modem cable, connect the FortiWeb unit's console port to the serial communications (COM) port on your management computer.
2. On your management computer, start HyperTerminal.
3. On *Connection Description*, enter a *Name* for the connection, and select *OK*.
4. On *Connect To*, from *Connect using*, select the communications (COM) port where you connected the FortiWeb unit.
5. Select *OK*.
6. Select the following *Port* settings and select *OK*.

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

7. Press Enter to connect to the CLI.

   The login prompt appears.
8. Type a valid administrator account name (such as `admin`) and press Enter.
9. Type the password for that administrator account and press Enter. (In its default state, there is no password for the `admin` account.)

   The CLI displays the following text:

   ```
   Welcome!

   Type ? to list available commands.
   ```

   You can now enter CLI commands, including configuring access to the CLI through SSH or Telnet. For details, see "Enabling access to the CLI through the network (SSH or Telnet)" on page 20.

Enabling access to the CLI through the network (SSH or Telnet)

SSH or Telnet access to the CLI is formed by connecting your computer to the FortiWeb unit using one of its RJ-45 network ports. You can either connect directly, using a peer connection between the two, or through any intermediary network.

Note: If you do not want to use an SSH/Telnet client and you have access to the web-based manager, you can alternatively access the CLI through the network using the *CLI Console* widget in the web-based manager. For details, see the *FortiWeb Administration Guide*.

You must enable SSH and/or Telnet on the network interface associated with that physical network port. If your computer is ***not*** connected directly or through a switch, you must also configure the FortiWeb unit with a static route to a router that can forward packets from the FortiWeb unit to your computer.

You can do this using either:

- a local console connection (see the following procedure)
- the web-based manager (see the*FortiWeb Administration Guide*)

Requirements

- a computer with an available serial communications (COM) port and RJ-45 port
- terminal emulation software such as HyperTerminal for Microsoft Windows
- the null modem cable included in your FortiWeb package
- a network cable
- prior configuration of the operating mode, network interface, and static route (for details, see the *FortiWeb Installation Guide.*

To enable SSH or Telnet access to the CLI using a local console connection

1 Using the network cable, connect the FortiWeb unit's network port either directly to your computer's network port, or to a network through which your computer can reach the FortiWeb unit.

2 Note the number of the physical network port.

3 Using a local console connection, connect and log into the CLI. For details, see "Connecting to the CLI using a local console" on page 19.

4 Enter the following command:

```
config system interface
  edit <interface_str>
    set allowaccess <protocols_list>
    next
  end
```

where:

- `<interface_str>` is the name of the network interface associated with the physical network port and containing its number, such as `port1`
- `<protocols_list>` is the complete, space-delimited list of permitted administrative access protocols, such as `https ssh telnet`

For example, to exclude HTTP, HTTPS, SNMP, and PING, and allow only SSH and Telnet administrative access on `port1`:

```
set system interface port1 config allowaccess ssh telnet
```

Caution: Telnet is not a secure access method. SSH should be used to access the CLI from the Internet or any other untrusted network.

5 To confirm the configuration, enter the command to display the network interface's settings.

```
get system interface <interface_str>
```

The CLI displays the settings, including the allowed administrative access protocols, for the network interfaces.

To connect to the CLI through the network interface, see "Connecting to the CLI using SSH" on page 22 or "Connecting to the CLI using Telnet" on page 23.

Connecting to the CLI using SSH

Once you configure the FortiWeb unit to accept SSH connections, you can use an SSH client on your management computer to connect to the CLI. SSH provides both secure authentication and secure communications to the CLI.

Note: FortiWeb units support 3DES and Blowfish encryption algorithms for SSH.

Before you can connect to the CLI using SSH, you must first configure a network interface to accept SSH connections. For details, see "Enabling access to the CLI through the network (SSH or Telnet)" on page 20.

Note: The following procedure uses PuTTY. Steps may vary with other SSH clients.

To connect to the CLI using SSH

1 On your management computer, start an SSH client.

2 In *Host Name (or IP Address)*, type the IP address of a network interface on which you have enabled SSH administrative access.

3 In *Port*, type 22.

4 From *Connection type*, select *SSH*.

5 Select *Open*.

The SSH client connects to the FortiWeb unit.

The SSH client may display a warning if this is the first time you are connecting to the FortiWeb unit and its SSH key is not yet recognized by your SSH client, or if you have previously connected to the FortiWeb unit but it used a different IP address or SSH key. If your management computer is directly connected to the FortiWeb unit with no network hosts between them, this is normal.

6 Click *Yes* to verify the fingerprint and accept the FortiWeb unit's SSH key. You will not be able to log in until you have accepted the key.

The CLI displays a login prompt.

7 Type a valid administrator account name (such as `admin`) and press Enter.

8 Type the password for this administrator account and press Enter.

Note: If three incorrect login or password attempts occur in a row, you will be disconnected. Wait one minute, then reconnect to attempt the login again.

The FortiWeb unit displays a command prompt (its host name followed by a `#`). You can now enter CLI commands.

Connecting to the CLI using Telnet

Once you configure the FortiWeb unit to accept Telnet connections, you can use a Telnet client on your management computer to connect to the CLI.

Caution: Telnet is not a secure access method. SSH should be used to access the CLI from the Internet or any other untrusted network.

Before you can connect to the CLI using Telnet, you must first configure a network interface to accept SSH connections. For details, see "Enabling access to the CLI through the network (SSH or Telnet)" on page 20.

To connect to the CLI using Telnet

1. On your management computer, start a Telnet client.
2. Connect to a FortiWeb network interface on which you have enabled Telnet.
3. Type a valid administrator account name (such as `admin`) and press Enter.
4. Type the password for this administrator account and press Enter.

Note: If three incorrect login or password attempts occur in a row, you will be disconnected. Wait one minute, then reconnect to attempt the login again.

The FortiWeb unit displays a command prompt (its host name followed by a `#`). You can now enter CLI commands.

Command syntax

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

Fortinet documentation uses the following conventions to describe valid command syntax.

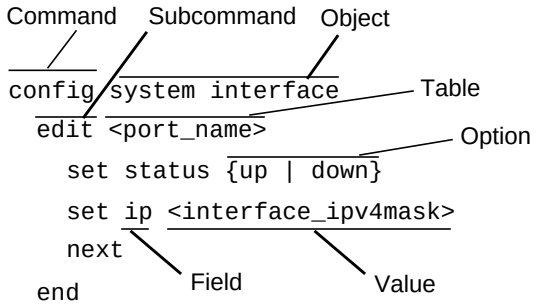
Terminology

Each command line consists of a command word followed by words for the configuration data or other specific item that the command uses or affects, for example:

```
get system admin
```

Fortinet documentation uses terms in Figure 1 to describe the function of each word in the command line.

Figure 1: Command syntax terminology



- **command**: A word that begins the command line and indicates an action that the FortiWeb unit should perform on a part of the configuration or host on the network, such as `config` or `execute`. Together with other words, such as fields or values, that you terminate by pressing the Enter key, it forms a command line. Exceptions include multi-line command lines, which can be entered using an escape sequence. (See "Shortcuts and key commands" on page 31.)

  Valid command lines must be unambiguous if abbreviated. (See "Command abbreviation" on page 32.) Optional words or other command line permutations are indicated by syntax notation. (See "Notation" on page 25.)

Note: This CLI Reference is organized alphabetically by object for the `config` command, and by the name of the command for remaining top-level commands.

- **subcommand**: A kind of command that is available only when nested within the scope of another command. After entering a command, its applicable subcommands are available to you until you exit the scope of the command, or until you descend an additional level into another subcommand. Indentation is used to indicate levels of nested commands. (See "Indentation" on page 25.)

  Not all top-level commands have subcommands. Available subcommands vary by their containing scope. (See "Subcommands" on page 26.)
- **object**: A part of the configuration that contains tables and/or fields. Valid command lines must be specific enough to indicate an individual object.
- **table**: A set of fields that is one of possibly multiple similar sets that each have a name or number, such as an administrator account, policy, or network interface. These named or numbered sets are sometimes referenced by other parts of the configuration that use them. (See "Notation" on page 25.)
- **field**: The name of a setting, such as `ip` or `hostname`. Fields in some tables must be configured with values. Failure to configure a required field will result in an invalid object configuration error message, and the FortiWeb unit will discard the invalid table.
- **value**: A number, letter, IP address, or other type of input that is usually the configuration setting held by a field. Some commands, however, require multiple input values which may not be named but are simply entered in sequential order in the same command line. Valid input types are indicated by constraint notation. (See "Notation" on page 25.)
- **option**: A kind of value that must be one or more words from a fixed set of options. (See "Notation" on page 25.)

Indentation

Indentation indicates levels of nested commands, which indicate what other subcommands are available from within the scope.

For example, the `edit` subcommand is available only within a command that affects tables, and the `next` subcommand is available only from within the `edit` subcommand:

```
config system interface
  edit port1
    set status up
    next
  end
```

For information about available subcommands, see "Subcommands" on page 26.

Notation

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 4: Command syntax notation

Convention	Description

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

Curly braces `{ }`	A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [ ].
Options delimited by vertical bars |	Mutually exclusive options. For example: `{enable | disable}` indicates that you must enter either `enable` or `disable`, but must not enter both.

Options delimited by spaces	Non-mutually exclusive options. For example:
	`{http https ping snmp ssh telnet}`
	indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as:
	`ping https ssh`
	Note: To change the options, you must re-type the entire list. For example, to add `snmp` to the previous example, you would type:
	`ping https snmp ssh`
	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.

Table 4: Command syntax notation

Angle brackets < >	A word constrained by data type. 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: `<retries_int>` indicates that you should enter a number of retries, such as `5`. Data types include: • `<xxx_name>`: A name referring to another part of the configuration, such as `policy_A`. • `<xxx_index>`: An index number referring to another part of the configuration, such as `0` for the first static route. • `<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`. • `<xxx_fqdn>`: A fully qualified domain name (FQDN), such as `mail.example.com`. • `<xxx_email>`: An email address, such as `admin@mail.example.com`. • `<xxx_ipv4>`: An IPv4 address, such as `192.168.1.99`. • `<xxx_v4mask>`: A dotted decimal IPv4 netmask, such as `255.255.255.0`. • `<xxx_ipv4mask>`: A dotted decimal IPv4 address and netmask separated by a space, such as `192.168.1.99 255.255.255.0`. • `<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`. • `<xxx_ipv4range>`: A hyphen (`-`)-delimited inclusive range of IPv4 addresses, such as `192.168.1.1-192.168.1.255`. • `<xxx_ipv6>`: A colon(`:`)-delimited hexadecimal IPv6 address, such as `3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234`. • `<xxx_v6mask>`: An IPv6 netmask, such as `/96`. • `<xxx_ipv6mask>`: A dotted decimal IPv6 address and netmask separated by a space. • `<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 “Special characters” on page 32. • `<xxx_int>`: An integer number that is ***not*** another data type, such as `15` for the number of minutes.

Subcommands

Once you connect to the CLI, you can enter commands.

Each command line consists of a command word that is usually followed by words for the configuration data or other specific item that the command uses or affects, for example:

```
get system admin
```

Subcommands are available from within the scope of some commands.When you enter a subcommand level, the command prompt changes to indicate the name of the current command scope. For example, after entering:

```
config system admin
```

the command prompt becomes:

```
(admin)#
```

Applicable subcommands are available to you until you exit the scope of the command, or until you descend an additional level into another subcommand.

For example, the `edit` subcommand is available only within a command that affects tables; the `next` subcommand is available only from within the `edit` subcommand:

```
config system interface
  edit port1
    set status up
    next
  end
```

Available subcommands vary by command.From a command prompt within `config`, two types of subcommands might become available:

- commands that affect fields
- commands that affect tables

Table 5: Commands for tables

delete <table>	Remove a table from the current object. For example, in `config system admin`, you could delete an administrator account named `newadmin` by typing `delete newadmin` and pressing Enter. This deletes `newadmin` and all its fields, such as `newadmin`'s `first-name` and `email-address`. `delete` is only available within objects containing tables.
edit <table>	Create or edit a table in the current object. For example, in `config system admin`: • edit the settings for the default `admin` administrator account by typing `edit admin`. • add a new administrator account with the name `newadmin` and edit `newadmin`'s settings by typing `edit newadmin`. `edit` is an interactive subcommand: further subcommands are available from within `edit`. `edit` changes the prompt to reflect the table you are currently editing. `edit` is only available within objects containing tables.
end	Save the changes to the current object and exit the `config` command. This returns you to the top-level command prompt.
get	List the configuration of the current object or table. • In objects, `get` lists the table names (if present), or fields and their values. • In a table, `get` lists the fields and their values. For more information on `get` commands, see "get" on page 307.
purge	Remove all tables in the current object. For example, in `config user local-user`, you could type `get` to see the list of all local user names, then type `purge` and then `y` to confirm that you want to delete all users. `purge` is only available for objects containing tables. **Caution:** Back up the FortiWeb unit before performing a `purge` because it cannot be undone. To restore purged tables, the configuration must be restored from a backup. For details, see "execute backup" on page 292. **Caution:** Do not purge `system interface` or `system admin` tables. This can result in being unable to connect or log in, requiring the FortiWeb unit to be formatted and restored.
show	Display changes to the default configuration. Changes are listed in the form of configuration commands. For more information on `get` commands, see "show" on page 313.

Note: Subcommand scope is indicated in this CLI Reference by indentation. See "Indentation" on page 25.

Note: Syntax examples for each top-level command in this CLI Reference do not show all available subcommands. However, when nested scope is demonstrated, you should assume that subcommands applicable for that level of scope are available.

Example of table commands

From within the `system admin` object, you might enter:

```
edit admin_1
```

The CLI acknowledges the new table, and changes the command prompt to show that you are now within the `admin_1` table:

```
new entry 'admin_1' added
(admin_1)#
```

Table 6: Commands for fields

abort	Exit both the `edit` and/or `config` commands without saving the fields.
end	Save the changes made to the current table or object fields, and exit the `config` command. (To exit without saving, use `abort` instead.)
get	List the configuration of the current object or table. • In objects, `get` lists the table names (if present), or fields and their values. • In a table, `get` lists the fields and their values.
next	Save the changes you have made in the current table's fields, and exit the `edit` command to the object prompt. (To save and exit completely to the root prompt, use `end` instead.) `next` is useful when you want to create or edit several tables in the same object, without leaving and re-entering the `config` command each time. `next` is only available from a table prompt; it is not available from an object prompt.
set <field> <value>	Set a field's value. For example, in `config system admin`, after typing `edit admin`, you could type `set password newpass` to change the password of the `admin` administrator to `newpass`. **Note:** When using `set` to change a field containing a space-delimited list, type the whole new list. For example, `set <field> <new-value>` will replace the list with the `<new-value>` rather than appending `<new-value>` to the list.
show	Display changes to the default configuration. Changes are listed in the form of configuration commands.
unset <field>	Reset the table or object's fields to default values. For example, in `config system admin`, after typing `edit admin`, typing `unset password` resets the password of the `admin` administrator account to the default (in this case, no password).

Example of field commands

From within the `admin_1` table, you might enter:

```
set password my1stExamplePassword
```

to assign the value `my1stExamplePassword` to the `password` field. You might then enter the `next` command to save the changes and edit the next administrator's table.

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 “config system accprofile” on page 110.

Table 7: Areas of control in access profiles

Access control area name		**Grants access to** (For each `config` command, there is an equivalent `get`/`show` command, unless otherwise noted. `config` access requires write permission. `get`/`show` access requires just read permission.)
In the web-based manager	**In the CLI**	
Admin Users	`admingrp`	*System* > *Admin* ***except*** *Settings* tab
		`config system admin` `config system accprofile`
Auth Users	`authusergrp`	*User*
		`config user ...`
Autolearn Configuration	`learngrp`	*Auto Learn* and *Web Protection* > *Web Protection Profile* > *Auto Learning Profile* **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` **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 log alertemail ...` `config log ...`
Maintenance	`mntgrp`	*System* > *Maintenance* ***except*** *System Time* tab

		`diagnose system ...`
		`execute backup ...`
		`execute factoryreset`
		`execute reboot`
		`execute restore`
		`execute shutdown`

Network Configuration	`netgrp`	*System* > *Network* > *Interface* *System* > *Network* > *V-zone*
		`config system interface` `config system v-zone`
Router Configuration	`routegrp`	*Router*
		`config router ...`

Table 7: Areas of control in access profiles

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, and interface
		`diagnose network ip ...`
		`diagnose network sniffer ...`
		`execute date ...`
		`execute ping ...`
		`execute ping-options ...`
		`execute traceroute ...`
		`execute time ...`

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*
		`config wvs ...`
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`.

Tips and tricks

Basic features and characteristics of the CLI environment provide support and ease of use for many CLI tasks.

This section includes:

- Help
- Shortcuts and key commands
- Command abbreviation

- Environment variables
- Special characters
- Language support & regular expressions
- Screen paging
- Baud rate
- Editing the configuration file on an external host

Help

To display brief help during command entry, press the question mark (?) key.

- Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each.
- Press the question mark (?) key after a command keyword to display a list of the objects available with that command and a description of each.
- Type a word or part of a word, then press the question mark (?) key to display a list of valid word completions or subsequent words, and to display a description of each.

Shortcuts and key commands

Table 8: Shortcuts and key commands

Action	Keys
List valid word completions or subsequent words. If multiple words could complete your entry, display all possible completions with helpful descriptions of each.	?
Complete the word with the next available match. Press the key multiple times to cycle through available matches.	Tab
Recall the previous command. Command memory is limited to the current session.	Up arrow, or Ctrl + P
Recall the next command.	Down arrow, or Ctrl + N
Move the cursor left or right within the command line.	Left or Right arrow
Move the cursor to the beginning of the command line.	Ctrl + A
Move the cursor to the end of the command line.	Ctrl + E
Move the cursor backwards one word.	Ctrl + B
Move the cursor forwards one word.	Ctrl + F
Delete the current character.	Ctrl + D
Abort current interactive commands, such as when entering multiple lines. If you are not currently within an interactive command such as `config` or `edit`, this closes the CLI connection.	Ctrl + C
Continue typing a command on the next line for a multi-line command. For each line that you want to continue, terminate it with a backslash (\ ). To complete the command line, terminate it by pressing the spacebar and then the Enter key, without an immediately preceding backslash.	\ then Enter

Command abbreviation

You can abbreviate words in the command line to their smallest number of non-ambiguous characters. For example, the command `get system status` could be abbreviated to `g sy st`.

Environment variables

The CLI supports the following environment variables. Variable names are case-sensitive.

$USERFROM	The management access type (`ssh`, `telnet`, `jsconsole` for the *CLI Console* widget in the web-based manager, and so on) and the IP address of the administrator that configured the item.
$USERNAME	The account name of the administrator that configured the item.
$SerialNum	The serial number of the FortiWeb unit.

For example, the FortiWeb unit's host name can be set to its serial number.

```
config system global
  set hostname $SerialNum
end
```

As another example, you could log in as `admin1`, then configure a restricted secondary administrator account for yourself named `admin2`, whose `first-name` is `admin1` to indicate that it is another of your accounts:

```
config system admin
  edit admin2
    set first-name $USERNAME
```

Special characters

Special characters <, >, (,), #, ', and " are usually not permitted in CLI. Some may be enclosed in quotes or preceded with a backslash (\ ) character.

Table 9: Entering special characters

Character	Keys
?	Ctrl + V then ?
Tab	Ctrl + V then Tab
Space (to be interpreted as part of a string value, not to end the string)	Enclose the string in quotation marks: `"Security Administrator"`. Enclose the string in single quotes: `'Security Administrator'`. Precede the space with a backslash: `Security\ Administrator`.
' (to be interpreted as part of a string value, not to end the string)	\'
" (to be interpreted as part of a string value, not to end the string)	\"
\	\\

Language support & regular expressions

Languages currently supported by the CLI interface include:

- English
- Japanese
- simplified Chinese
- traditional Chinese

Characters such as ñ, é, symbols, and ideographs are sometimes acceptable input. Support varies by the nature of the item being configured. CLI commands, objects, field names, and options must use their exact ASCII characters, but some items with arbitrary names or values may be input using your language of choice.

For example, the host name must not contain special characters, and so the web-based manager and CLI will not accept most symbols and other 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 the correct encoding.

The FortiWeb unit stores the input using Unicode UTF-8 encoding, but it is not normalized from other encodings into UTF-8 before 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.

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 or 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 or 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.

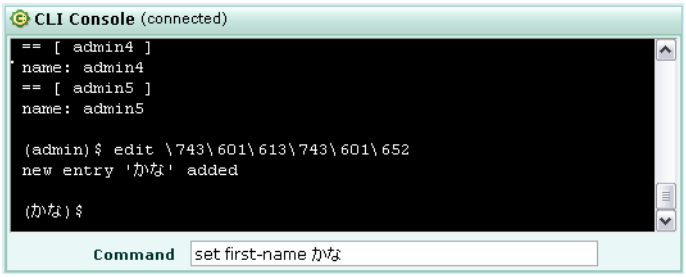
To enter non-ASCII characters in the CLI Console widget

1 On your management computer, start your web browser and go to the URL for the FortiWeb unit's web-based manager.
2 Configure your web browser to interpret the page as UTF-8 encoded.
3 Log in to the FortiWeb unit.
4 Go to *System* > *Status* > *Status*.
5 In title bar of the *CLI Console* widget, click the *Edit* icon.

  The *Console Preferences* dialog appears in a pop-up window.
6 Enable *Use external command input box*.
7 Click *OK*.

  The *Command* field appears below the usual input and display area of the *CLI Console* widget.
8 In *Command*, type a command.

Figure 2: Entering encoded characters (*CLI Console* widget)



9 Press Enter.

  In the display area, the *CLI Console* widget displays your previous command interpreted into its character code equivalent, such as:

  `edit \743\601\613\743\601\652`

  and the command's output.

To enter non-ASCII characters in a Telnet or SSH client

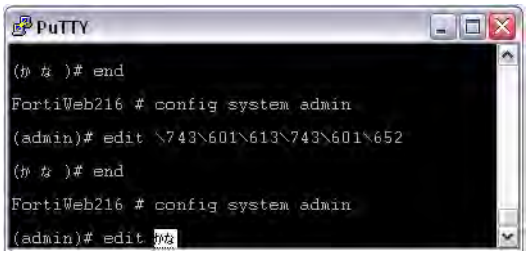
1 On your management computer, start your Telnet or SSH client.
2 Configure your Telnet or SSH client to send and receive characters using UTF-8 encoding the encoding.

  Support for sending and receiving international characters varies by each Telnet or SSH client. Consult the documentation for your Telnet or SSH client.

3 Log in to the FortiWeb unit.

4 At the command prompt, type your command and press Enter.

Figure 3: Entering encoded characters (PuTTY)



You may need to surround words that use encoded characters with single quotes (').

Depending on your Telnet or SSH client's support for your language's input methods and for sending international characters, you may need to interpret them into character codes before pressing Enter.

For example, you might need to enter:

```
edit '\743\601\613\743\601\652'
```

5 The CLI displays your previous command and its output.

Screen paging

When output spans multiple pages, you can configure the CLI to pause after each page. When the display pauses, the last line displays `--More--`. You can then either:

- Press the spacebar to display the next page.
- Type `Q` to truncate the output and return to the command prompt.

This may be useful when displaying lengthy output, such as the list of possible matching commands for command completion, or a long list of settings. Rather than scrolling through or possibly exceeding the buffer of your terminal emulator, you can simply display one page at a time.

To configure the CLI display to pause after each full screen:

```
config system console
  set output more
end
```

For more information, see "config system console" on page 129.

Baud rate

You can change the default baud rate of the local console connection. For more information, see "config system console" on page 129.

Editing the configuration file on an external host

You can edit the FortiWeb configuration on an external host by first backing up the configuration file to a TFTP server. Then edit the configuration file and restore it to the FortiWeb unit.

Editing the configuration on an external host can be time-saving if you have many changes to make, especially if your plain text editor provides advanced features such as batch changes.

To edit the configuration on your computer

1. Use execute backup to download the configuration file to a TFTP server, such as your management computer.
2. Edit the configuration file using a plain text editor that supports Unix-style line endings.

Caution: Do not edit the first line. The first lines of the configuration file (preceded by a # character) contains information about the firmware version and FortiWeb model. If you change the model number, the FortiWeb unit will reject the configuration file when you attempt to restore it.

3. Use execute restore to upload the modified configuration file back to the FortiWeb unit.

   The FortiWeb unit downloads the configuration file and checks that the model information is correct. If it is, the FortiWeb unit loads the configuration file and checks each command for errors. If a command is invalid, the FortiWeb unit ignores the command. If the configuration file is valid, the FortiWeb unit restarts and loads the new configuration.

config

The `config` commands configure your FortiWeb unit's settings. This chapter describes the following commands:

config log alertemail
config log attack-log
config log custom-sensitive-rule
config log disk
config log email-policy
config log event-log
config log forti-analyzer
config log fortianalyzer-policy
config log memory
config log reports
config log sensitive
config log syslogd
config log syslog-policy
config log traffic-log
config log trigger-policy
config router setting
config router static
config server-policy allow-hosts
config server-policy custom-application application-policy
config server-policy custom-application url-replacer
config server-policy health
config server-policy http-content-routing-policy
config server-policy http-conversion-policy
config server-policy custom-application application-policy
config server-policy custom-application url-replacer
config server-policy pattern custom-data-type
config server-policy pattern custom-susp-url
config server-policy pattern custom-susp-url-rule
config server-policy pattern data-type-group
config server-policy pattern suspicious-url-rule
config server-policy policy
config server-policy pserver
config server-policy pservers
config server-policy service custom
config server-policy service predefined
config server-policy vserver
config system accprofile
config system admin
config system autoupdate override
config system autoupdate schedule
config system autoupdate tunneling
config system certificate ca
config system certificate ca-group
config system certificate crl
config system certificate intermediate-certificate
config system certificate intermediate-certificate-group
config system certificate local
config system certificate remote
config system certificate verify
config system conf-sync
config system console
config system dns
config system dos-prevention
config system fail-open
config system global
config system ha
config system interface
config system raidconfig system report-lang
config system settings
config system snmp community
config system snmp sysinfo
config system v-zone
config user ldap-user
config user local-user
config user ntlm-user
config user radius-user
config user user-group
config wad website
config waf allow-method-exceptions
config waf allow-method-policy
config waf brute-force-login
config waf custom-protection-group
config waf custom-protection-rule
config waf file-upload-restriction-policy
config waf file-upload-restriction-rule
config waf hidden-fields-protection
config waf hidden-fields-rule
config waf http-authen http-authen-policy
config waf http-authen http-authen-rule
config waf http-constraints-exceptions

config waf http-protocol-parameter-restriction
config waf input-rule
config waf ip-list
config waf page-access-rule
config waf parameter-validation-ruleconfig waf robot-control
config waf server-protection-exception
config waf server-protection-rule
config waf start-pages
config waf url-access url-access-policy
config waf url-access url-access-rule
config waf url-rewrite url-rewrite-policy
config waf url-rewrite url-rewrite-rule
config waf web-custom-robot
config waf web-protection-profile autolearning-profile
config waf web-protection-profile inline-protection
config waf web-protection-profile offline-protection
config waf web-robotconfig wvs policy
config wvs profile
config wvs schedule
config xml-protection filter-rule
config xml-protection intrusion-prevention-rule
config xml-protection key-file
config xml-protection key-management
config xml-protection period-time onetime
config xml-protection period-time recurring
config xml-protection schema-files
config xml-protection web-service
config xml-protection web-service-group
config xml-protection wsdl-content-routing-table
config xml-protection xml-protection-profile

Note: Although not usually explicitly shown in each config command's "Syntax" section, for all `config` commands, there are related get and show commands which display that part of the configuration, either in the form of a list of settings and values, or commands that are required to achieve that configuration from the firmware's default state, respectively. `get` and `show` commands use the same syntax as their related `config` command, unless otherwise mentioned.

log alertemail

Use this command to enable or disable alert emails, and to choose which email policy to use to issue alert emails, when enabled. Use alert emails to contact administrators or other personnel when an alert condition occurs, such as a system failure or network attack.

The email address information and the alert message intervals are configured separately for each email policy. For information on the severity levels of log messages associated with an email policy, see "config log email-policy" on page 46.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config log alertemail
  set status {enable | disable}
  set email-policy <policy name>
end
```

Variable	Description	Default
`status {enable | disable}`	Enable to generate an alert email when the FortiWeb unit records a log message. The log message must also meet or exceed the severity level configured in "config log email-policy" on page 46.	`enable`
`email-policy <policy name>`	Select the preconfigured email policy, which includes the recipient email address information and the intervals at which alert emails will be sent.	`no default`

Example

This example enables alert email when either a system event or attack log message is logged. The alert email is sent using the recipients configured in `emailpolicy1`.

```
config log alertemail
  set status enable
  set email-policy emailpolicy1
end
```

History

FortiWeb v4.1.1 New

Related topics

- config log email-policy

log attack-log

Use this command to configure recording of attack log messages on the local FortiWeb disk.

Note: You must enable disk log storage and select log severity levels using the config log disk command before any attack logs can be stored on disk.

Also use this command to define specific packet payloads to retain when storing attack logs.

Packet payloads can be retained for specific attack types or validation failures detected by the FortiWeb unit. Packet payloads supplement the log message by providing the actual data that triggered the attack log, which may help you to fine-tune your regular expressions to prevent false positives. You can also 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' of the part of the payload that triggered the log message.

You can view attack log packet payloads from the *Packet Log* column using the web-based manager. For details, see the *FortiWeb Administration Guide*.

Packet payloads can contain sensitive information. You can prevent sensitive data from display in the packet payload by applying sensitivity rules that detect and obscure sensitive information. For details, see "config log sensitive" on page 61.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config log attack-log
  set packet-log {allow-robot | bad-robot | common-exploits | custom-
     protection-rule | hidden-fields-failed | infomation-disclosure |
     parameter-rule-failed | sql-injection | xss-attack}
  set status {enable | disable}
end
```

Variable	Description	Default
`status` `{enable | disable}`	Enable to record attack log messages on the disk. To record attack logs, disk log storage must be enabled, and the severity levels selected using the config log disk command.	`enable`

`packet-log`
`{allow-robot |`
`bad-robot |`
`common-exploits |`
`custom-protection-rule |`
`hidden-fields-failed |`
`infomation-disclosure |`
`parameter-rule-failed |`
`sql-injection |`
`xss-attack}`
	Type the name of the attack types or validation failures, if any, for which packet payloads are to be kept with their associated attack log message.	`none`

Example

This example enables disk log storage, sets `information` as the minimum severity level that a log message must achieve for storage, enables recording of attack logs and retention of specific packet payloads along with the attack logs.

```
config log disk
```

```
    set status enable
    set severity information
  end
  config log attack-log
    set status enable
    set packet-log allow-robot
    set packet-log common-exploits
    set packet-log custom-protection-rule
    set packet-log parameter-rule-failed
  end
```

History

FortiWeb v4.1.1 New. Replaces config log disk filter.

Related topics

- config log sensitive
- config log custom-sensitive-rule
- config log event-log
- config log traffic-log

log custom-sensitive-rule

Use this command to configure custom rules to obscure sensitive information that is not obscured in log message packet payloads by the predefined sensitivity rules.

Use this command in conjunction with “config log sensitive” on page 61.

If enabled to do so, a FortiWeb unit will obscure predefined data types, including user names and passwords in log message packet payloads. If other sensitive data in the packet payload is not obscured by the predefined data types, you can create your own data type sensitivity rules, such as ages or other identifying numbers.

Note: Sensitive data definitions are ***not*** retroactive. They will hide strings in subsequent log messages, but will not affect existing log messages.

This command is relevant only if you have enabled the FortiWeb unit to keep packet payloads along with their associated log messages, and have selected to obscure logs according to custom data types. For details, see “config log attack-log” on page 40 and “config log sensitive” on page 61.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see “Permissions” on page 29.

Syntax

```
config log custom-sensitive-rule
  edit <custom-sensitive-rule-name>
    set expression "<sensitive-type_pattern>
    set field-name "<parameter-name_pattern>"
    set field-value "<parameter-value_pattern>"
    set type {field-mask-rule | general-mask-rule}
  next
end
```

Variable	Description	Default
`<custom-sensitive-rule-name>`	Type the name of a new rule to add or the name of an existing rule to edit.	No default.
`expression "<sensitive-type_pattern>`	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]` Expressions must not start with an asterisk (`*`). The maximum length is 21 characters.	No default.
`type {field-mask-rule | general-mask-rule}`	Select either `general-mask-rule` (a regular expression that will match any substring in the packet payload) or `field-mask-rule` (a regular expression that will match only the value of a specific form input). If you select `general-mask-rule`, configure `expression "<sensitive-type_pattern>`. If you select `field-mask-rule`, configure `field-name "<parameter-name_pattern>"` and `field-value "<parameter-value_pattern>"`.	`general-mask-rule`

Variable	Description	Default
`field-name "<parameter-name_pattern>"`	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-rule` instead.)	No default.

`field-value "<parameter-value_pattern>"`	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 "<parameter-name_pattern>"`, you would enter `age`, and for `field-value "<parameter-value_pattern>"`, 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`
		No default.

Example

This example enables the FortiWeb unit to keep all types of packet payloads with their associated log messages. It also enables and defines a custom sensitive data type (applies to age 13 or less) that will be obscured in logs.

```
config log attack-log
  set status enable
  set packet-log parameter-rule-failed xss-attack sql-injection common-
     exploits bad-robot allow-robot hidden-fields-failed infomation-
     disclosure
end
config log sensitive
  set type custom-rule
end
config log custom-sensitive-rule
  edit rule1
    set type general-mask-rule
    set expression "age\\=[1-13]*$"
  next
end
```

History

FortiWeb v4.0.0	New.
FortiWeb v4.1.1	Modified for packet payload configuration now in config log attack-log and config log traffic-log.

Related topics

- config log sensitive
- config log attack-log
- config log traffic-log

log disk

Use this command to enable and configure recording of log messages to the local hard disk.

Note: Logging must be enabled for each individual log type before log messages are recorded to disk. See `config log attack-log`, `config log event-log`, `config log traffic-log` for details.

You can use SNMP traps to notify you when disk space usage exceeds 80%. For details, see "config system snmp community" on page 150.

You can generate reports based upon log messages that you save to the local hard disk. For details, see "config log reports" on page 53.

Syntax

```
config log disk
  set diskfull {nolog | overwrite}
  set max-log-file-size <filesize_int>
  set severity <severity-level>
  set status {enable | disable}
end
```

Variable	Description	Default
`status {enable | disable}`	Enable to store log messages on the local hard disk. Log messages are stored only if logging is enabled for the individual log types using the config log attack-log, config log event-log and config log traffic-log commands. Also configure `severity`, `diskfull` and `max-log-file-size`.	`disable`
`diskfull {nolog | overwrite}`	Type what the FortiWeb unit will do when the local disk is full and a new log message is caused, either: • `nolog`: Discard the new log message. • `overwrite`: Delete the oldest log file in order to free disk space, and store the new log message. This field is available only if `status` is `enable`.	`overwrite`
`max-log-file-size <filesize_int>`	Enter the maximum size of the current log file in megabytes (MB). When the log file reaches the maximum size the log file is rolled (that is, the current log file is saved to a file with a new name, and a new log file is started). The maximum allowed size is 200 MB. This field is available only if `status` is `enable`.	`100`
`severity <severity-level>`	Type the severity level that a log message must meet or exceed in order to cause the FortiWeb unit to save it to the disk. The severity level is one of: `alert`, `critical`, `debug`, `emergency`, `error`, `information`, `notification`, or `warning`.	`alert`

Example

This example enables logging of event and attack logs and recording of the log messages to the local hard disk. Only the log messages with a severity of `notification` or higher are recorded. If all free space on the hard disk is consumed and a new log message is generated, the `diskfull` option determines that the FortiWeb will overwrite the oldest log message. The log messages are saved to a separated log file for each message type. Once the log file size reaches the 100 MB specified by `max-log-file-size`, the FortiWeb unit saves the log file with a sequentially-numbered name and starts a new log.

```
config log event-log
  set status enable
end
```

```
config log attack-log
   set status enable
end
config log disk
   set status enable
   set severity notification
   set diskfull overwrite
   set max-log-file-size 100
end
```

History

FortiWeb v4.1.1 New. Replaces config log disk setting.

Related topics

- config log attack-log
- config log event-log
- config log traffic-log
- config system snmp community
- config log reports

log email-policy

Use this command to create an email policy. An email policy identifies email recipients, email address, email connection requirements and authentication information, if required.

You can configure multiple email policies and apply those policies as required in different situations. The FortiWeb unit can be configured to send email for different situations, such as to alert administrators when certain system events or rule violations occur, or when log reports are available for distribution.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config log email-policy
  edit <email-policy_name>
    set mailfrom <address_str>
    set mailto1 <recipient_email>
    set mailto2 <recipient_email>
    set mailto3 <recipient_email>
    set smtp-server {ipv4> | <fqdn>}
    set smtp-auth {enable | disable}
    set smtp-username <auth_str>
    set smtp-password <password_str>
    set severity <severity-level>
    set alert-interval <minutes_int>
    set critical-interval <minutes_int>
    set debug-interval <minutes_int>
    set emergency-interval <minutes_int>
    set error-interval <minutes_int>
    set information-interval <minutes_int>
    set notification-interval <minutes_int>
    set warning-interval <minutes_int>
  next
end
```

Variable	Description	Default
`<email-policy_name>`	Type the name of an email policy.	No default
`mailfrom <address_str>`	Type the sender email address that the FortiWeb unit will use when sending email.	No default.
`mailto1 <recipient_email>`	Type the email address of the first recipient to which the FortiWeb unit will send email. You must enter one email address for alert email to function.	No default.
`mailto2 <recipient_email>`	Type the email address of the second recipient, if any, to which the FortiWeb unit will send alert email.	No default.
`mailto3 <recipient_email>`	Type the email address of the third recipient, if any, to which the FortiWeb unit will send alert email.	No default.
`smtp-server {ipv4> | <fqdn>}`	Type the IP address or fully qualified domain name (FQDN) of the SMTP server that the FortiWeb unit can use to send email.	No default.
`smtp-auth {enable | disable}`	Enable if the SMTP server requires authentication. Also enable if authentication is not required but is available and you want the FortiWeb unit to authenticate.	`disable`

Variable	Description	Default
`smtp-username <auth_str>`	If you enable smtp-auth {enable | disable}, type the user name that the FortiWeb unit will use to authenticate itself with the SMTP relay. This field is available only if you enable smtp-auth {enable | disable}.	No default.
`smtp-password <password_str>`	If you enable smtp-auth {enable | disable}, type the password that corresponds with the user name. This field is available only if you enable smtp-auth {enable | disable}.	No default.
`severity <severity-level>`	Select the severity threshold that log messages must meet or exceed in order to cause an email alert. The severity level is one of: alert, critical, debug, emergency, error, information, notification, or warning.	`alert`
`emergency-interval <minutes_int>`	Type the interval in minutes between each email message that the FortiWeb unit will send after the initial email, as long as events whose severity level is emergency continue to occur, triggering additional email.	`1`
`alert-interval <minutes_int>`	Type the interval in minutes between each email message that the FortiWeb unit will send after the initial email, as long as events whose severity level is alert continue to occur, triggering additional email.	`2`
`critical-interval <minutes_int>`	Type the interval in minutes between each email message that the FortiWeb unit will send after the initial email, as long as events whose severity level is critical continue to occur, triggering additional email.	`3`
`error-interval <minutes_int>`	Type the interval in minutes between each email message that the FortiWeb unit will send after the initial email, as long as events whose severity level is error continue to occur, triggering additional email.	`5`
`notification-interval <minutes_int>`	Type the interval in minutes between each message that the FortiWeb unit will send after the initial email, as long as events whose severity level is notification continue to occur, triggering additional email.	`20`
`warning-interval <minutes_int>`	Type the interval in minutes between each email message that the FortiWeb unit will send after the initial email, as long as events whose severity level is warning continue to occur, triggering additional email.	`10`
`information-interval <minutes_int>`	Type the interval in minutes between each email message that the FortiWeb unit will send after the initial email, as long as events whose severity level is information continue to occur, triggering additional email.	`30`
`debug-interval <minutes_int>`	Type the interval in minutes between each email message that the FortiWeb unit will send after the initial email, as long as events whose severity level is debug continue to occur, triggering additional email.	`60`

Example

This example creates email policy for use in multiple situations. When the email policy is attached to rule violations or log reports, an email will be sent from `fortiweb@example.com,` to `admin@example.com` and `analysis@example.com`, using an SMTP server `mail.example.com`. The SMTP server requires authentication. The FortiWeb unit will authenticate as `fortiweb` when connecting to the SMTP server.

Log messages more severe than a notification are logged. As long as events continue to trigger notification-level log messages, the FortiWeb unit will send an alert email every 10 minutes. (Log messages of other severity levels will trigger alert email at their default intervals.)

When the configuration is complete, the administrator should log in to the web-based manager to send a sample alert email to test the configuration and the email system, verifying the complete path between the FortiWeb unit and the inbox for the email account `admin@example.com`.

```
config log email-policy
  edit Email_Policy1
    set mailfrom fortiweb@example.com
    set mailto1 admin@example.com
    set mailto2 analysis@example.com
    set smtp-server mail.example.com
    set smtp-auth enable
```

```
    set smtp-username fortiweb
    set smtp-password fortiWebPasswordD2
    set severity notification
    set notification-interval 10
  next
end
```

History

FortiWeb v4.1.1 New. Replaces config log syslogd setting.

Related topics

- config log alertemail
- config log trigger-policy
- config system dns
- config router static

log event-log

Use this command to configure recording of event log messages, and then use other commands to store those messages on the local FortiWeb disk, in local FortiWeb memory, or both. Use other commands to configure a traffic log and attack log.

Note: You must enable disk and/or memory log storage and select log severity levels before FortiWeb will store any event logs.

Syntax

```
config log event-log
  set status {enable | disable}
  set threshold <percentage>
end
```

Variable	Description	Default
`status {enable | disable}`	Enable to record event log messages. The actual destination of the stored messages and the severity threshold for storing messages must be set using the config log disk and config log memory commands.	`disable`
`threshold <percentage>`	Set a threshold level as a percentage that will trigger an event log when the actual number of persistent server sessions reaches the defined percentage of the total number of persistent server sessions allowed for the FortiWeb unit. Allowed values are: `50, 60, 70, 80, 90`.	`80`

Example

This example enables recording of event logs, enables disk log storage and memory log storage, and sets `alert` as the minimum severity level that a log message must achieve for storage.

```
config log disk
  set status enable
  set severity alert
end
config log memory
  set status enable
  set severity alert
end
config log event-log
  set status enable
end
```

History

FortiWeb v4.1.1 New. Replaces config log disk filter.

Related topics

- config log disk
- config log memory
- config log attack-log
- config log traffic-log

log forti-analyzer

Use this command to configure the local FortiWeb unit to send log messages to a remote FortiAnalyzer unit. You must first define one or more FortiAnalyzer policies using the config log fortianalyzer-policy command.

FortiAnalyzer entries are controlled by FortiAnalyzer policies and trigger actions associated with various types of violations. If you enable the `forti-analyzer` log command but do not set a trigger action for a specific type of violation, FortiWeb will record every occurrence of that violation in FortiAnalyzer.

Caution: Enabling FortiAnalyzer could result in excessive log messages being recorded in FortiAnalyzer.

Note: Logs stored remotely cannot be viewed from the FortiWeb web-based manager.

Syntax

```
config log forti-analyzer
  set fortianalyzer-policy <policy-name-str>
  set severity <severity-level>
  set status {enable | disable}
end
```

Variable	Description	Default
`fortianalyzer-policy <policy-name-str>`	Type the name of an existing FortiAnalyzer policy to use when storing log information remotely. You set the policy using the config log fortianalyzer-policy command.	No default.
`status {enable | disable}`	Enable to record event log messages in memory. The log message must also meet or exceed the severity level configured in the `set severity` subcommand.	`disable`
`severity <severity-level>`	Type the severity level that a log message must meet or exceed in order to cause the FortiWeb unit to save it to memory. The severity level is one of: alert, critical, debug, emergency, error, information, notification, or warning.	`alert`

Example

This example enables FortiAnalyzer logging and recording of the log messages. Only the log messages with a severity of `error` or higher are recorded.

```
config log forti-analyzer
  set status enable
  set severity error
end
```

History

FortiWeb v4.2 New.

Related topics

- config log fortianalyzer-policy

log fortianalyzer-policy

Use this command to create policies for use by protection rules to store log messages remotely on a FortiAnalyzer unit. For example, once you create a FortiAnalyzer policy, you can include it in a trigger policy, which in turn can be applied to a trigger action in a protection rule.

You need to create a FortiAnalyzer policy if you also plan to send log messages to a FortiAnalyzer unit.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config log fortianalyzer-policy
  edit <policy-name_str>
    set ip-address <ipv4>
    next
end
```

Variable	Description	Default
`<policy-name_str>`	Type the name of a FortiAnalyzer policy.	No default.
`<ipv4>`	Type the IP address of the remote FortiAnalyzer unit.	No default.

Example

This example creates a policy entry and assigns an IP address, then enables FortiAnalyzer logging for log messages with a severity of `error` or higher

```
config log fortianalyzer-policy
  edit fa-policy1
    set ip-address 192.0.2.0
    next
  end
config log forti-analyzer
  set status enable
  set severity error
end
```

History

FortiWeb v4.2 New.

Related topics

- config log forti-analyzer

log memory

Use this command to enable and configure event logging to memory (RAM). Only event logs can be stored in local memory.

Caution: Do not store important log messages to memory. Memory is not permanent storage. Log messages stored in memory will be lost upon reboot or shutdown.

Note: Event message logging must be enabled before event messages are recorded to memory. See `config log event-log` for details.

Tip: For improved performance, when not necessary, avoid logging highly frequent log types.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config log memory
  set severity <severity-level>
  set status {enable | disable}
end
```

Variable	Description	Default
`status {enable | disable}`	Enable to record event log messages in memory. The log message must also meet or exceed the severity level configured in `severity`.	`disable`
`severity <severity-level>`	Type the severity level that a log message must meet or exceed in order to cause the FortiWeb unit to save it to memory. The severity level is one of: alert, critical, debug, emergency, error, information, notification, or warning.	`alert`

Example

This example enables event logging and recording of the log messages at the `error` level to memory.

```
config log event-log
  set status enable
end
config log memory
  set status enable
  set severity error
end
```

History

FortiWeb v4.1.1 New. Replaces config log memory filter and config log memory setting

Related topics

- config log event-log

log reports

Use this command to configure report profiles.

When generating a report, FortiWeb units collate information collected from their log files and present the information in tabular and graphical format.

In addition to log files, your FortiWeb unit requires a report profile 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 in the web-based manager when you click the *Run now* icon 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.

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 Attack Severity by Hour of Day," the report includes the top ***x*** hours, and their top ***y*** attacks, then groups the remaining results.

- `scope_top1 <topX_int>` is ***x***.
- `scope_top2 <topY_int>` is ***y***.

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 "config log attack-log" on page 40 and "config log disk" on page 44.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see "Permissions" on page 29.

Tip: Creating a report profile is considerably easier in the web-based manager. Go to *Log&Report > Report Config.*

Syntax

```
config log reports
  edit <report_name>
    set custom_company <org_str>
    set custom_footer_options {custom | report-title}
    set custom_footer <footer_str>
    set custom_header <header_str>
    set custom_header logo <filename_hex>
    set custom_title_logo <filename_hex>
    set email_attachment_compress {enable | disable}
    set email_attachment_name <filename_str>
    set email_body <message_str>
    set email_subject <subject_str>
    set filter_string <log-filter_str>
    set include_nodata {yes | no}
    set on_demand {enable | disable}
    set output_email {html mht pdf rtf txt}
    set output_email_policy <policy_str>
    set output_file {html mht pdf rtf txt}
```

```
    set period_end <time_str> <date_str>
    set period_last_n <n_int>
    set period_start <time_str> <date_str>
    set period_type {last-14-days | last-2-weeks | last-30-days | last-7-
       days | lastmonth | last-n-days | last-n-hours | last-nweeks |
       last-quarter | last-week | other | thismonth | this-quarter |
       this-week | this-year | today | yesterday}
    set report_desc <comment_str>
    set report_title <title_str>
    set Report_attack_activity {attacks-type attacks-url attacks-date-type
       attacks-month-type attacks-day-type attacks-hour-type
       attacks-type-dev attacks-dst-type attacks-dst-ip attacks-type-ip
       attacks-method-type attacks-cat attacks-policy attacks-day attacks-ts
       attacks-td attacks-proto attacks-date-severity
       attacks-month-severity attacks-day-severity attacks-hour-severity
       attacks-sessionid}
    set Report_event_activity {ev-all ev-all-cat ev-all-type ev-crit-hour
       ev-crit-day ev-warn-hour ev-warn-day ev-info-hour ev-info-day
       ev-emer-hour ev-emer-day ev-aler-hour ev-aler-day ev-err-hour
       ev-err-day ev-noti-hour ev-noti-day ev-hour ev-hour-cat ev-day
       ev-day-cat ev-stat}
    set Report_traffic_activity {net-pol net-srv net-src net-dst net-src-dst
       net-dst-src net-date-dst net-hour-dst net-day-dst net-month-dst
       net-date-src net-hour-src net-day-src net-month-src}
    set Report_pci_activity {pci-attacks-date-type pci-attacks-day-type pci-
       attacks-hour-type pci-attacks-month-type}
    set schedule_type {daily | dates | days | none}
    set schedule_days {sun | mon | tue | wed | thu | fri | sat}
    set schedule_dates {1 to 31}
    set schedule_time <time_str>
    set scope_include_summary {yes | no}
    set scope_include_table_of_content {yes | no}
    set scope_top1 <topX_int>
    set scope_top2 <topY_int>
      next
    end
  next
end
```

Variable	Description	Default
`<report_name>`	Type the name of a report profile. The profile name will be included in the report header.	No default.
`custom_company <org_str>`	Type the name of your department, company, or other organization, if any, that you want to include in the report summary. If the text is more than one word or contains special characters, enclose it in double quotes ("). For information on enabling the summary, see `scope_include_summary {yes | no}`.	No default.
`custom_footer_options {custom | report-title}`	Select whether to use <report_name> as the footer text or to provide separate footer text in `custom_footer <footer_str>`.	`report-title`

Variable	Description	Default
`custom_footer <footer_str>`	Type the text, if any, that you want to include at the bottom of each report page. If the text is more than one word or contains special characters, enclose it in double quotes (`"`). This setting is available only if `custom_footer_options` is `custom`.	
`custom_header <header_str>`	Type the text, if any, that you want to include at the top of each report page. If the text is more than one word or contains special characters, enclose it in double quotes (`"`).	No default.
`custom_header_logo <filename_hex>`	Type the file name, encoded in hexadecimal values, of a custom logo that you have previously uploaded to the FortiWeb unit. The logo image will be included in the report header.	No default.
`custom_title_logo <filename_hex>`	Type the file name, encoded in hexadecimal values, of a custom logo that you have previously uploaded to the FortiWeb unit. The logo image will be included in the report title.	No default.
`email_attachment_compress {enable | disable}`	Enable to enclose the generated report formats in a compressed archive attached to the email. This field is required if you have enabled email output by enabling one or more of the file formats for email output in output_email {html mht pdf rtf txt}.	`disable`
`email_attachment_name <filename_str>`	Type the file name that will be used for the reports attached to the email. This field is required if you have enabled email output by enabling one or more of the file formats for email output in output_email {html mht pdf rtf txt}.	No default.
`email_body <message_str>`	Type the message body of the email. This field is required if you have enabled email output by enabling one or more of the file formats for email output in output_email {html mht pdf rtf txt}.	No default.
`email_subject <subject_str>`	Type the subject line of the email. This field is required if you have enabled email output by enabling one or more of the file formats for email output in output_email {html mht pdf rtf txt}.	No default.
`filter_string <log-filter_str>`	Type a log message filter string that includes or excludes log messages based upon matching log field values. For example syntax, see “Example” on page 59.	No default.
`include_nodata {yes | no}`	Select whether to include (`yes`) or hide (`no`) reports which are empty because there is no matching log data.	`no`
`on_demand {enable | disable}`	Type `enable` to run the report one time only. After the FortiWeb unit completes the report, it removes the report profile from its hard disk. Type `disable` to schedule a time to run the report, and to keep the report profile for subsequent use.	`disable`
`output_email {html mht pdf rtf txt}`	Select one or more file types for the report when mailing generated reports.	No default.
`output_email_policy <policy_str>`	If you set a value for `output_email`, type the name of the predefined policy to be use to send the report by email. The email policy defines the details for sending the report by email, including: the recipients, email addresses, email servers and authentication. For more information on email policy, see “config log email-policy” on page 46.	No default.
`output_file {html mht pdf rtf txt}`	Select one or more file types for the report when saving to the FortiWeb hard disk.	`html`

Variable	Description	Default
`period_end <time_str> <date_str>`	Enter the time and date that define the ***end*** of the span of time whose log messages you want to use when generating the report. The time format is `hh:mm` and the date format is `yyyy/mm/dd`, where: • `hh` is the hour according to a 24-hour clock • `mm` is the minute • `yyyy` is the year • `mm` is the month • `dd` is the day This setting appears only when you select a `period_type` of `other`.	No default.
`period_last_n <n_int>`	Enter the number that defines ***n*** if the `period_type` contains that variable. This setting appears only when you select a `period_type` of `last-n-days`, `last-n-hours`, or `last-n-weeks`.	No default.
`period_start <time_str> <date_str>`	Enter the time and date that defines the ***beginning*** of the span of time whose log messages you want to use when generating the report. The time format is `hh:mm` and the date format is `yyyy/mm/dd`, where: • `hh` is the hour according to a 24-hour clock • `mm` is the minute • `yyyy` is the year • `mm` is the month • `dd` is the day This setting appears only when you select a `period_type` of `other`.	No default.
`period_type {last-14-days | last-2-weeks | last-30-days | last-7-days | lastmonth | last-n-days | last-n-hours | last-nweeks | last-quarter | last-week | other | thismonth | this-quarter | this-week | this-year | today | yesterday}`	Select the span of time whose log messages you want to use when generating the report. If you select `last-n-days`, `last-n-hours`, or `last-nweeks`, you must also define ***n*** by entering period_last_n <n_int>. If you select other, you must also define the start and end of the report's time range by entering `period_start` and `period_end`. The span of time will be included in the summary, if enabled. For information on enabling the summary, see scope_include_summary {yes | no}.	`last-7-days`
`report_desc <comment_str>`	Type a description of the report, if any, that you want to include in the report summary. If the text is more than one word or contains special characters, enclose it in double quotes ("). For information on enabling the summary, see scope_include_summary {yes | no}.	No default.
`report_title <title_str>`	Type a title, if any, that you want to include in the report summary. If the text is more than one word or contains special characters, enclose it in double quotes ("). For information on enabling the summary, see scope_include_summary {yes | no}.	No default.

Variable	Description	Default
`Report_attack_activity {attacks-type attacks-url attacks-date-type attacks-month-type attacks-day-type attacks-hour-type attacks-type-dev attacks-dst-type attacks-dst-ip attacks-type-ip attacks-method-type attacks-cat attacks-policy attacks-day attacks-ts attacks-td attacks-proto attacks-date-severity attacks-month-severity attacks-day-severity attacks-hour-severity attacks-sessionid}`	Type zero or more options to indicate which charts based upon attack logs to include in the report. For example, to include “Attacks By Policy," enter a list of charts that includes `attacks-policy`. To include “Top Attacked HTTP Methods by Type," enter a list of charts that includes `attacks-method-type`.	No default.
`Report_event_activity {ev-all ev-all-cat ev-all-type ev-crit-hour ev-crit-day ev-warn-hour ev-warn-day ev-info-hour ev-info-day ev-emer-hour ev-emer-day ev-aler-hour ev-aler-day ev-err-hour ev-err-day ev-noti-hour ev-noti-day ev-hour ev-hour-cat ev-day ev-day-cat ev-stat}`	Type zero or more options to indicate which charts based upon event logs to include in the report. For example, to include “Top Event Categories by Status", enter a list of charts that includes `ev-status`.	No default.

Variable	Description	Default
Report_traffic_activity {net-pol net-srv net-src net-dst net-src-dst net-dst-src net-date-dst net-hour-dst net-day-dst net-month-dst net-date-src net-hour-src net-day-src net-month-src}	Type zero or more options to indicate which charts based upon traffic logs to include in the report. For example, to include “Top Sources By Day of Week", enter a list of charts that includes net-day-src.	No default.
Report_pci_activity {pci-attacks-date-type pci-attacks-day-type pci-attacks-hour-type pci-attacks-month-type}	Type zero or more options to indicate which charts based upon PCI attack logs to include in the report.	
schedule_type {daily | dates | days | none}	Select when the FortiWeb unit will automatically run the report. If you reboot the FortiWeb unit while the report is being generated, report generation resumes after the boot process is complete. If schedule_type is daily, dates or days, specify the schedule_time, schedule_days, or schedule_dates when the report will be generated. If schedule_type is none, the report will be generated only when you manually initiate it.	none
schedule_days {sun | mon | tue | wed | thu | fri | sat}	If schedule_type is not days, select the day of the week when the report should be generated.	No default.
schedule_dates {1 to 31}	If schedule_type is dates, select the specific date of the month, from 1 to 31, when the report should be generated.	No default.
schedule_time <time_str>	If schedule_type is not none, select the time of day when the report should be run. The time format is hh:mm, where hh is the hour according to a 24-hour clock and mm is the minute.	00:00
scope_include_summary {yes | no}	Enter yes to include a summary section at the beginning of the report. The summary includes: • custom_company "<org_str>" • <report_name> • report_desc "<comment_str>" • the date and time when the report was generated using this profile • the span of time whose log messages were used to generate the report, according to period_type	yes
scope_include_table_of_content {yes | no}	Enter yes to include a table of contents at the beginning of the report. The table of contents includes links to each chart in the report.	yes

Variable	Description	Default
`scope_top1 <topX_int>`	Enter ***x*** number of items (up to 30) to include in the first cross-section of ranked reports. For some report types, you can set the top ranked items for the report. These reports have “Top" in their name, and will always show only the top ***x*** entries. Reports that do not include “Top" in their name show all information. Changing the values for top field will not affect these reports.	6
`scope_top2 <topY_int>`	Enter ***y*** number of items (up to 30) to include in the second cross-section of ranked reports. For some report types, you can set the number of ranked items to include in the report. These reports have “Top" in their name, and will always show only the top ***x*** entries. Some report types have two levels of ranking: the top ***y*** sub-entries for each top ***x*** entry. Reports that do not include “Top" in their name show all information. Changing the values for top field will not affect these reports.	3

Example

This example configures a report to be generated every Saturday at 1 PM. The report, whose title is “Report 1”, includes all available charts, and covers the last 14 days’ worth of event, traffic, and attack logs. However, it only uses logs where the source IP address was 172.16.1.20. Each time it is generated, it will be saved to the hard disk in both HTML and PDF file formats and will be sent by email in PDF format to recipients defined within the “Log report analysis” email policy.

```
config log reports
  edit "Report_1"
    set Report_attack_activity attacks-type attacks-url attacks-date-type
       attacks-month-type attacks-day-type attacks-hour-type attacks-type-dev
       attacks-dst-type attacks-dst-ip attacks-type-ip attacks-method-type
       attacks-cat attacks-policy attacks-day attacks-ts attacks-td attacks-
       proto attacks-date-severity attacks-month-severity attacks-day-
       severity attacks-hour-severity attacks-sessionid
    set Report_event_activity ev-all ev-all-cat ev-all-type ev-crit-hour ev-
       crit-day ev-warn-hour ev-warn-day ev-info-hour ev-info-day ev-emer-hour
       ev-emer-day ev-aler-hour ev-aler-day ev-err-hour ev-err-day ev-noti-
       hour ev-noti-day ev-hour ev-hour-cat ev-day ev-day-cat ev-stat
    set Report_traffic_activity net-pol net-srv net-src net-dst net-src-dst
       net-dst-src net-date-dst net-hour-dst net-day-dst net-month-dst net-
       date-src net-hour-src net-day-src net-month-src
    set custom_company "Example, Inc."
    set custom_footer_options custom
    set custom_header "A fictitious corporation."
    set custom_title_logo "%74%65%73%74%2e%70%6e%67"
    set filter_string "(and  src==\'172.16.1.10\')"
    set include_nodata yes
    set output_file html pdf
    set output_email html
    set output_email_policy log_report_analysis
    set period_type last-n-days
    set report_desc "A sample report."
    set report_title "Report 1"
    set schedule_type days
    set custom_footer "Weekly report for Example, Inc."
    set period_last_n 14
    set schedule_days sat
    set schedule_time 01:00
```

```
    next
end
```

History

FortiWeb v3.3.0	New.
FortiWeb v4.0.0	Added fields `output_email`, `email_attachment_compress`, `email_attachment_name`, `email_body`, and `email_subject`, and the subcommand `config output_addresses`. Configures email output for generated reports.
FortiWeb v4.0.1	Added field `log_filter`. Configures a log message filter to select the log data upon which a report will be based.
FortiWeb v4.1.1	Added field `output_email_policy`. Selects the email policy, which defines the details for log reports sent by email.

Related topics

- config system report-lang
- config log attack-log
- config log disk
- config log email-policy

log sensitive

Use this command to configure whether the FortiWeb unit will obscure sensitive information, such as user names and passwords, in log messages for which packet payloads are enabled. Each packet payload has predefined sensitivity rules based on the payload data type. If needed, you can also create custom sensitivity rules to obscure other payload data types using “config log custom-sensitive-rule” on page 42.

This command is relevant only if you have enabled the FortiWeb unit to keep packet payloads along with their associated log messages. For details, see “config log attack-log” on page 40 and “config log traffic-log” on page 65.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see “Permissions” on page 29.

Syntax

```
config log sensitive
  set type {custom-rule | pre-defined-rule}
end
```

Variable	Description	Default
`type {custom-rule | pre-defined-rule}`	Select whether the FortiWeb unit will obscure packet payloads according to predefined data types and/or custom data types. See “config log custom-sensitive-rule” on page 42.	No default.

Example

This example enables the FortiWeb unit to use a custom sensitive rule to obscure packet payload information that displays information about users that are age 13 and under.

```
config log sensitive
  set type custom-rule
end
config log custom-sensitive-rule
  edit custom-sensitive-rule1
    set type general-mask-rule
    set expression "age\\=[1-13]*$"
  next
end
```

History

FortiWeb v4.0.0	New.
FortiWeb v4.1.1	Modified. Packet payload configuration now part of config log attack-log and config log traffic-log commands

Related topics

- config log custom-sensitive-rule
- config log attack-log
- config log traffic-log

log syslogd

Use this command to configure the FortiWeb unit to send log messages to a Syslog server defined by the config log syslog-policy command.

Tip: For improved performance, when not necessary, avoid logging highly frequent log types.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config log syslogd
  set status {enable | disable}
  set facility <identifier>
  set severity <severity-level>
  set policy <policy_str>
end
```

Variable	Description	Default
`status {enable | disable}`	Enable to send log messages to the Syslog server defined by the config log syslog-policy. Also configure `facility`, `port` and `severity`.	`disable`
`facility <identifier>`	Enter the facility identifier that the FortiWeb unit will use to identify itself when sending log messages to the first Syslog server. 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. The value of `identifier` is one of: `alert, audit, auth, authpriv, clock, cron, daemon, ftp, kernel, local0, local1, local2, local3, local4, local5, local6, local7, mail, ntp, user.`	`local7`
`severity <severity-level>`	Type the severity level that a log message must meet or exceed in order to cause the FortiWeb unit to send it to the first Syslog server. The severity level is one of: alert, critical, debug, emergency, error, information, notification, or warning.	`alert`
`policy <policy_str>`	If logging to a Syslog server is enabled, type the name of the predefined syslogd policy. The syslogd policy describes the Syslog server to which the log message will be sent. For more information on syslogd policy, see "config log syslog-policy" on page 64.	

Example

This example enables storage of log messages with the `notification` severity level and higher on the Syslog server. The network connections to the Syslog server are defined in `Syslog_Policy1.` The FortiWeb unit uses the facility identifier `local7` when sending log messages to the Syslog server to differentiate its own log messages from those of other network devices using the same Syslog server.

```
config log syslogd
  set status enable
  set severity notification
  set facility local7
  set policy Syslog_Policy1
end
```

History

FortiWeb v4.1.1 New. Replaces config log syslogd filter

Related topics

- config log syslog-policy

log syslog-policy

Use this command to configure a connection to a Syslog server. A unique policy is required for each Syslog server. The policy is used by the `log syslogd` configuration to define the specific Syslog server on which log messages are stored. For more information, see "config log syslogd" on page 62.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config log syslog-policy
  edit <policy name>
  set csv {enable | disable}
  set port <port_number>
  set server <syslog_ipv4>
end
```

Variable	Description	Default
`<policy name>`	Type the name of a Syslog policy. The name of the report profile will be included in the report header.	No default
`csv {enable | disable}`	Enable if the Syslog server requires the FortiWeb unit to send log messages in comma-separated value (CSV) format, instead of the standard Syslog format.	`disable`
`port <port_number>`	Type the TCP port number on which the Syslog server listens.	`514`
`server <syslog_ipv4>`	Type the IP address of the Syslog server, in IPv4 format.	No default.

Example

This example creates `Syslog_Policy1`. The Syslog server is contacted by its IP address, `192.168.1.10`. Communications occur over the standard TCP port number for Syslog, UDP port `514`. The FortiWeb unit sends log messages to the Syslog server in CSV format.

```
config log syslog-policy
  edit Syslog_Policy1
    set server 192.168.1.10
    set port 514
    set csv enable
  next
end
```

History

FortiWeb v4.1.1 New. Replaces config log syslogd setting.

Related topics

- config log syslogd
- config system dns
- config router static

log traffic-log

Use this command to have the FortiWeb unit record traffic log messages on its local disk. This command also lets you save packet payloads with the traffic logs.

Note: You must enable disk log storage and select log severity levels using the config log disk command before any traffic logs can be stored on disk.

Packet payloads supplement the log message by providing the actual data associated with the traffic log, which may help you to analyze traffic patterns.

You can view packet payloads in the *Packet Log* column when viewing a traffic logs using the web-based manager. For details, see the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config log traffic-log
  set packet-log {enable | disable}
  set status {enable | disable}
end
```

Variable	Description	Default
`status {enable | disable}`	Enable to record traffic log messages on the disk. To record traffic logs, disk log storage must be enabled, and the severity levels selected using the config log disk command.	`enable`
`packet-log {enable | disable}`	Enable to keep packet payloads stored with their associated traffic log message.	`disable`

Example

This example enables disk log storage, sets `information` as the minimum severity level that a log message must achieve for storage, enables recording of traffic logs and retention of all packet payloads along with the traffic logs.

```
config log disk
   set status enable
   set severity information
end
config log traffic-log
   set status enable
   set packet-log enable
end
```

History

FortiWeb v4.1.1 New. Replaces config log disk filter.

Related topics

- config log attack-log
- config log event-log
- config log disk

log trigger-policy

Use this command to configure a trigger policy for use in the notification process.

Trigger policies are applied to individual conditions that have an associated action and severity, such as attacks and rule violations. A trigger policy has two components: an email policy and a Syslog policy. The trigger policy determines whether an email is sent to administrators when a certain condition occurs and whether the log messages associated with the condition are stored on a Syslog server. The email policy contains the details associated with the recipient email account, and the Syslog policy contains details required to communicate with the Syslog server.

You must define the email and Syslog policies before you can apply the trigger policy to an individual condition. For more information, see “config log email-policy” on page 46 and “config log syslog-policy” on page 64.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see “Permissions” on page 29.

Syntax

```
config log trigger-policy
  edit <trigger-policy_name>
    set <email-policy_name>
    set <syslog-policy_name>
    set analyzer-policy <fortianalyzer-policy>
    next
  end
```

Variable	Description	Default
`<trigger-policy_name>`	Type the name of a trigger policy.	no default
`<email-policy_name>`	Select the name of the email policy to be used with the trigger policy. If the conditions associated with the trigger policy occur, the email policy determines the recipients of the notification email messages associated with the condition. For more information, see “config log email-policy” on page 46.	no default
`<syslog-policy_name>`	Select the name of the Syslog policy to be used with the trigger policy. If the conditions associated with the trigger policy occur, the Syslog policy determines which Syslog server the messages are sent to. For more information, see “config log syslog-policy” on page 64.	no default
`analyzer-policy <fortianalyzer-policy>`	Enter the name of an existing FortiAnalyzer policy. See “config log fortianalyzer-policy” on page 51.	

Example

This example creates `Trigger_policy1`, which uses `emailpolicy1` to send email notifications about the condition to specific recipients, and `Syslog_Policy1` to submit the log messages to a specific Syslog server.

```
config log trigger-policy
  edit Trigger_policy1
    set syslog-policy Syslog_Policy1
    set email-policy emailpolicy1
    next
end
```

History

FortiWeb v4.1.1 New

Related topics

- config log email-policy
- config log syslog-policy
- config waf http-protocol-parameter-restriction
- config waf server-protection-rule

router setting

Use this command to enable or disable IP-based forwarding. FortiWeb units are designed to provide in-depth protection ***specifically*** for the HTTP and HTTPS protocols. Because of this, they do ***not*** forward other protocols to your protected physical servers. This provides a secure default configuration by blocking traffic to ports that were unintentionally left open and should not be accessible to the general public. .

Note: This command has no equivalent in the web-based manager.

In some cases, however, you may have a physical server that must provide more services than just HTTP or HTTPS. A typical exception is a server that hosts both HTTP and FTP daemons.

For those deployments, you may need to forward non-web traffic destined for your physical servers' subnet by enabling `ip-forward {enable | disable}`.

Caution: Install a general purpose firewall in addition to the FortiWeb unit. Failure to do so could leave your web servers vulnerable to attacks that are not HTTP/HTTPS-based. FortiWeb units are ***not*** general-purpose firewalls, and, if you enable `ip-forward {enable | disable}`, will allow non-HTTP/HTTPS traffic to pass through uninspected. Ideally, control and protection measures should ***only*** allow web traffic, or other properly firewalled protocols, to reach the FortiWeb unit and your web servers.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `routegrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config router setting
  set ip-forward {enable | disable}
end
```

Variable	Description	Default
`ip-forward {enable | disable}`	Enable to forward non-HTTP/HTTPS traffic, if its IP address matches a static route. **Caution:** Do not enable this option unless the non-HTTP/HTTPS servers on the subnet behind the FortiWeb unit are protected by a general purpose firewall, or an application-specific firewall. Failure to provide appropriate freewheels for other protocols, such as FTP, could expose servers to security risks via those other protocols.	`disable`

Example

This example enables forwarding of non-HTTP/HTTPS traffic, based upon whether the IP address matches a route for the physical servers' subnet, and regardless of HTTP proxy pickup.

```
config router static
  set ip-forward enable
end
```

History

FortiWeb v3.2.2 New.

Related topics

- config router static

router static

Use this command to configure static routes, including the default gateway.

Static routes direct traffic existing 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 more specific static route is defined for the packet's destination IP address.

During installation and setup, you should have configured at least one static route, a default route, that points to your gateway. You may configure additional 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.

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.

Note: By default, the FortiWeb unit will forward only HTTP/HTTPS traffic. For information on routing other protocols such as FTP, see "config router setting" on page 68.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `routegrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config router static
  edit <route_index>
    set device <port_name>
    set dst <destination_ipv4mask>
    set gateway <router_ipv4>
  next
end
```

Variable	Description	Default
`<route_index>`	Type the index number of the static route. If multiple routes match a packet, the one with the smallest index number is applied.	No default.
`device <port_name>`	Type the name of the network interface device, such as `port1`, through which traffic subject to this route will be outbound.	No default.
`dst <destination_ipv4mask>`	Enter the destination IP address and netmask of traffic that will be subject to this route, separated with a space. To indicate all traffic regardless of IP address and netmask (that is, to configure a route to the default gateway), enter `0.0.0.0 0.0.0.0`.	`0.0.0.0 0.0.0.0`
`gateway <router_ipv4>`	Enter the IP address of a next-hop router. ***Warning***: The gateway IP address must be in the same subnet as the interface's IP address. When you change the interface's IP address later on, the new IP address must also be in the same subnet as the interface's default gateway address. Otherwise, all the static routes and the default gateway information will be lost.	`0.0.0.0`

Example

This example configures a default route that forwards all packets to the gateway router `192.168.1.1`, through the network interface named `port1`.

```
config router static
  edit 0
    set dst 0.0.0.0 0.0.0.0
    set gateway 192.168.1.1
    set device port1
  next
end
```

History

FortiWeb v3.2.0 New.

Related topics

- config router setting
- config system interface
- config log syslog-policy
- config server-policy policy
- config system admin
- config system dns
- config system global
- config system snmp community
- config wad website

server-policy allow-hosts

Use this command to configure protected host groups.

A protected host group contains one or more IP addresses and/or fully qualified domain names (FQDNs). Each entry 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, a 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, therefore, is often a ***private*** network address (unless the FortiWeb unit operates in offline protection or either of the transparent modes).

Protected host groups can be used by:

- policies
- input rules
- server protection exceptions
- start page rules
- page access rules
- URL access rules
- allowed method exceptions
- HTTP authentication rules
- hidden fields rules

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 use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config server-policy allow-hosts
  edit <protected-hosts_name>
    set default-action {allow | deny}
```

```
    config host-list
      edit <protected-host_index>
        set action {allow | deny}
        set host {<host_ipv4> | <host_fqdn>}
      next
    end
  next
end
```

Variable	Description	Default
<protected-hosts_name>	Type the name of a group of protected hosts.	No default.
default-action {allow | deny}	Select whether to accept or deny HTTP requests whose Host: field does ***not*** match any of the host definitions that you will add to this protected hosts group.	allow
<protected-host_index>	Type the index number of a protected host within its group.	No default.
action {allow | deny}	Select whether to accept or deny HTTP requests whose Host: field matches the host definition in host {<host_ipv4> | <host_fqdn>}.	allow
host {<host_ipv4> | <host_fqdn>}	Type the IP address or FQDN of a virtual or real web host, as it appears in the Host: field of HTTP headers, such as www.example.com. 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. 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: • 10.0.0.1, the address of the virtual server • www.example.com, the domain name that resolves to the virtual server	No default.

Example

This example configures a protected hosts group named example_com_hosts that contains a web site's domain names and its IP address in order to match HTTP requests regardless of which form they use to identify the host.

```
config server-policy allow-hosts
  set default-action deny
  edit example_com_hosts
    config host-list
      edit 0
        set host example.com
    next
      edit 1
        set host www.example.com
    next
      edit 2
        set host 10.0.0.1
      next
  next
end
```

History

FortiWeb v3.2.0	New.
FortiWeb v3.3.2	Added field `default-action`. Selects whether to allow or deny HTTP requests whose `Host:` field does ***not*** match any of the host entries in the group. Previously, non-matching requests were denied. Added field `action`. Selects whether to accept or deny HTTP requests whose `Host:` field matches a specific host's definition in the protected hosts group.

Related topics

- config server-policy policy
- config waf allow-method-exceptions
- config waf allow-method-policy
- config waf input-rule
- config waf server-protection-exception
- config waf start-pages
- config waf page-access-rule
- config waf hidden-fields-rule

server-policy custom-application application-policy

Some web applications build URLs differently than expected by FortiWeb, which causes FortiWeb to create incorrect auto-learning profiles.

To solve this kind of problem, FortiWeb uses application policy plug-ins that recognize the non-standard, customized applications and modify the URL information so that the auto-learning profile can work properly.

First create a URL replacer (see config server-policy custom-application url-replacer) to create the plug-ins, and then use this command to create an application policy to use the replacer.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config server-policy custom-application application-policy
  edit <policy-name>
    config rule-list
      edit <entry_index>
        set plugin-name <plugin-name>
        set priority <int>
        set type <plugin-type>
      next
    end
  next
end
```

Variable	Description	Default
`<policy-name>`	Type the name of a new or existing application policy.	No default.
`<entry_index>`	Enter an integer corresponding to a new or existing rule.	No default.
`plugin-name <plugin-name>`	Type the name of an existing URL-replacer plug-in.	No default.
`priority <int>`	Enter an integer to set the priority level of the rule where 0 is the highest priority level. Priority numbers must be unique within the rule list.	No default.
`type <plugin-type>`	Type the name of the plug-in type. (Only `URL_Replacer` is available at present.)	`URL_Replacer`

Note: Rule order affects URL replacer plug-in 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.

Example

This example adds two existing URL replacer plug-ins to a application policy.

```
config server-policy custom-application application-policy
  edit replacer-policy1
    config rule-list
      edit 1
        set plugin-name url-replacer1
        set priority 1
      next
```

```
        edit 2
          set plugin-name url-replacer2
          set priority 2
        next
      end
    next
  end
```

History

FortiWeb v4.2 New.

Related topics

- config server-policy custom-application url-replacerr

server-policy custom-application url-replacer

Some web applications build URLs differently than expected by FortiWeb. This can cause FortiWeb to create incorrect auto-learning profiles. Use this command and config server-policy custom-application application-policy to fix problems caused by “non-standard” URLs.

This command creates application policy plug-ins that recognize the non-standard, customized applications and modify the URL information so that the auto-learning profile can work properly.

Follow these steps to apply custom application policies:

1. Create the custom application URL replacers.
2. Apply the custom application policy.
3. Apply the application policies in the auto-learning profiles (see “config waf web-protection-profile autolearning-profile” on page 232).
4. Finally, apply the auto-learning profiles in the server policies (see “config server-policy policy” on page 92).

A URL replacer defines how you’re going to modify the non-standard request URLs.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see “Permissions” on page 29.

Syntax

```
config server-policy custom-application url-replacer
  edit <plugin-name-str>
    set type {pre-defined | custom-defined}
    set url <original-url>
    set new-url <new-url>
    set param <param-value-str>
    set new-param <replaced-param-name>
  next
end
```

Variable	Description	Default
`<plugin-name-str>`	Type the name of a new or existing URL replacer.	No default.
`type {pre-defined | custom-defined}`	Enter either `pre-defined` or `custom-defined`. The `pre-defined` type supports the JSP application type only. For any other type, use `custom-defined`.	`pre-defined`
`url <original-url>`	Type a regular expression that matches the request URL in the HTTP header. Only applies with `custom-defined`..	No default.
`new-url <new-url>`	Type the new URL string to be sent to the auto-learning module that uses the plug-in. Only applies with `custom-defined`.	No default.
`param <param-value-str>`	Type the new parameter’s value string. Only applies with `custom-defined`.	No default.
`new-param <replaced-param-name>`	Type the new parameter’s name string. Only applies with `custom-defined`.	No default.

Example

This example assumes the HTTP request URL from a client is `/tom/login.asp`. The following URL replacer changes the URL to `/login.asp` with an extra parameter: `username=tom`.

```
config server-policy custom-application url-replacer
  edit url-replacer1
```

```
    set type custom-defined
    set url ^/(.*)/(.*)$
    set new-url /$1
    set param $0
    set new-param username
  next
end
```

History

FortiWeb v4.2 New.

Related topics

- config server-policy custom-application application-policy

server-policy health

Use this command to configure server health checks.

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 regularly as 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 unavailable for a lengthy period, such as when it is undergoing hardware repair or when you have removed a server from the server farm, you may 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 "config server-policy pserver" on page 101.

To apply server health checks, select them in a policy for use with a server farm. For details, see "config server-policy policy" on page 92.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config server-policy health
  edit <health-check_name>
    set type {disable | http | icmp | tcp}
    set interval <seconds_int>
    set retry-times <retries_int>
    set time-out <seconds_int>
    set url-path <request_str>
  next
end
```

Variable	Description	Default
`<health-check_name>`	Type the name of the server health check.	No default.
`type {disable | http | icmp | tcp}`	Type either: • `disable`: Do not perform server health checks. • `http`: Use an HTTP request to determine server availability. Also configure `url-path <request_str>`. • `icmp`: Use an ICMP ping to determine server availability. • `tcp`: Use a TCP connection to determine server availability.	`disable`
`interval <seconds_int>`	Type the number of seconds between each server health check.	`5`
`retry-times <retries_int>`	Type the number of times, if any, a failed health check will be retried before the server is determined to be unresponsive.	`5`
`time-out <seconds_int>`	Type the number of seconds which must pass after the server health check to indicate a failed health check.	`10`
`url-path <request_str>`	Type 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. This setting is available when `type` is `http`.	No default.

Example

This example configures a server health check that periodically requests the main page of the web site, `/index`. If a physical server does not successfully return that page every five seconds (the default), and fails the check at least three times in a row, it will be deemed unresponsive and the FortiWeb unit will forward subsequent HTTP requests to other physical servers in the server farm.

```
config server-policy health
  edit status_check1
    set retry-times 3
    set type http
    set url-path "/index"
  next
end
```

History

FortiWeb v3.2.0 New.

Related topics

- config server-policy policy
- config server-policy pservers

server-policy http-content-routing-policy

Use this command when you want to route connections to a specific physical server in a server farm.

HTTP content routing is beneficial in cases where one virtual server provides the interface for many physical web servers. Content routing enables routing to be done according to URL or Host.

In some cases, HTTP requests must be converted before HTTP content routing can occur. For more information, see "config server-policy http-conversion-policy" on page 82.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config server-policy http-content-routing-policy
  edit <routing-policy_name>
    set host-status {enable | disable}
    set host <host_str>
    set url-type {regular-expression | simple-string}
    set request-url <request_str>
  next
end
```

Variable	Description	Default
`<routing-policy_name>`	Type the name of the HTTP content routing policy.	No default.
`host-status {enable | disable}`	Select to enable host name routing.	`disable`
`host <host_str>`	Enter the IP address or host name for the physical server in the server farm to route HTTP requests to. This setting is available only if `host-status` is enabled.	No default.
`url-type {regular-expression | simple-string}`	Select the method used to match the URL upon which routing will take place. If matching is done according to `host`, use `regular-expression`.	`simple-string`
`request-url <request_str>`	Enter the specific request file to be routed. If matching by host, add "\/" (a back slash and forward slash with no space between) in the URL pattern, such as `\/example`	No default.

Example

This example configures an HTTP content routing policy to route URL requests for www.example.com/school to a physical server in the server farm with IP address 10.5.5.12. The content routing is based on a matching a regular expression.

```
config server-policy http-content-routing-policy
  edit content_routing_policy1
    set host-status enable
    set host 10.5.5.12
    set request-url \/example
  next
end
```

History

FortiWeb v4.1.1 New.

Related topics

- config server-policy policy
- config server-policy pservers
- config server-policy http-conversion-policy

server-policy http-conversion-policy

Use this command in situations where HTTP requests received by the FortiWeb unit include a host name or URL, which must be converted to a destination address before the request is routed to a physical server (forward conversion), or where the "Location" field in an HTTP response needs to be converted to the original host name or URL (reverse conversion).

This enables bidirectional conversion of URLs and host names for HTTP content routing. For more information, see “config server-policy http-content-routing-policy” on page 80.

The HTTP conversion policy is used as part of configuring a server farm, which is in turn used as part of an overall server policy. For more information on server farm configuration, see “config server-policy pservers” on page 102.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see “Permissions” on page 29.

Syntax

```
config server-policy http-conversion-policy
  edit <content conversion policy name>
    config members
      edit <member_entry_index>
        set conversion_method {forward-conversion | reverse-conversion
        set host-from <hostname_str>
        set host-to <hostname_str>
        set url-from <url_str>
        set url-to <url_str>
      next
    end
  next
end
```

Variable	Description	Default
`<content conversion policy name>`	Type the name of the HTTP content routing policy.	No default.
`<member_entry_index>`	Type the index number of the conversion policy you want to configure.	No default.
`conversion_method {forward-conversion | reverse-conversion`	Select the HTTP conversion method. The conversion method modifies the HTTP packet header information, depending whether the packet is an HTTP request or an HTTP response. • In forward conversion, the FortiWeb unit converts the `url-from` in the HTTP request packet to a specific `url-to` on a destination host. • In reverse conversion, the FortiWeb unit modifies the HTTP response packet to the original `url-from`.	`forward-conversion`
`host-from <hostname_str>`	Enter the host name from the original HTTP request packet. The host name is contained in the Host field in the HTTP request packet.	No default.
`host-to <hostname_str>`	Enter the name of the destination host. The FortiWeb unit converts the `host-from` to the `host-to`.	No default.
`url-from <url_str>`	Enter the URL from the original HTTP request packet. The URL is part of the HTTP request packet. Depending on the conversion method, the `url-from` is converted to a `url-to` (forward conversion), or inserted as the Location for HTTP response packets (reverse conversion).	No default.
`url-to <url_str>`	Enter the URL to be used as the destination URL. The FortiWeb unit converts the `url-from` to the `url-to`.	No default.

Example

This example configures a forward and reverse HTTP conversion policy from an original URL (`url-from`) to destination URL (`url-to`), and an original host (`host-from`) to a destination host (`host-to`).

```
config server-policy http-conversion-policy
  edit "Terramark"
    config members
      edit 1
        set conversion-method forward-conversion
        set host-from "www.example.com"
        set host-to "10.153.25.102:8443"
        set url-from "/example"
        set url-to "/example"
      next
      edit 2
        set conversion-method reverse-conversion
        set host-from "10.153.25.102:8443"
        set host-to "www.example.com"
        set url-from "/example"
        set url-to "/example"
      next
    end
  next
end
```

History

FortiWeb v4.1.1 New.

Related topics

- config server-policy http-content-routing-policy
- config server-policy policy
- config server-policy pservers

server-policy pattern custom-data-type

Use this command to configure custom data types to augment the predefined data types. You can add custom data types to input rules to define the data type of an input, and to auto-learning profiles to detect valid input parameters.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config server-policy pattern custom-data-type
  edit <custom-data-type_name>
    set expression <string>
  next
end
```

Variable	Description	Default
`<custom-data-type_name>`	Type the name of the custom data.	No default.
`<string>`	Type the custom data.	No default.

Example

This example configures two custom data types.

```
config server-policy pattern custom-data-type
  edit "Level 3 Password-custom"
    set expression "^aaa"
  next
  edit "Custom Data Type 1"
    set expression "^555"
  next
end
```

History

FortiWeb v4.1 New.

Related topics

- config server-policy pattern data-type-group

server-policy pattern custom-susp-url

Use this command to configure custom suspicious URL requests to augment the list of predefined suspicious URL requests. You can add custom suspicious URLs to a custom suspicious URL rule.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config server-policy pattern custom-susp-url
  edit <custom-susp-url_name>
    set expression expression <url>
  next
end
```

Variable	Description	Default
`<custom-susp-url_name>`	Type the name of the custom URL.	No default.
`expression <url>`	Enter a simple string or a regular expression to defines the custom URL request to check for.	No default.

Example

This example configures a custom suspicious URL named `Suspicious-URL 1` and defines the custom expression associated with that suspicious URL.

```
config server-policy pattern custom-susp-url
  edit "Suspicious URL 1"
    set expression "^/schema.xml$"
end
```

History

FortiWeb v4.1 New.

Related topics

- config server-policy pattern suspicious-url-rule

server-policy pattern custom-susp-url-rule

Use this command to add one or more existing custom suspicious URLs to a custom suspicious URL rule.

Custom suspicious URL rules can augment the predefined suspicious URL rules. You can add custom suspicious URL rules to input rules.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config server-policy pattern custom-susp-url-rule
  edit <rule_name>
    config type-list
      edit <url-rule_index>
        set custom-susp-url <susp_name>
      next
    end
  next
end
```

Variable	Description	Default
`<rule_name>`	Type the name of the custom suspicious URL rule.	No default.
`<url-rule_index>`	Type the index number for a member of the group..	No default.
`<susp_name>`	Type the name of an existing custom URL already defined using the config server-policy pattern custom-susp-url command.	No default.

Example

This example configures a custom suspicious URL rule using an existing custom suspicious URL.

```
config server-policy pattern custom-susp-url-rule
  edit "Suspicious Rule 1"
    config type-list
      edit 1
        set custom-susp-url "Suspicious URL 1"
      next
    end
  next
end
```

History

FortiWeb v4.1 New.

Related topics

- config server-policy pattern custom-susp-url

server-policy pattern data-type-group

Use this command to configure data type groups.

A data type group selects a subset of one or more predefined data types. Each of those entries in the data type group defines a type of input that the FortiWeb unit should attempt to recognize and track in HTTP sessions when gathering data for an auto-learning profile.

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.

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 "config server-policy policy" on page 92.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config server-policy pattern data-type-group
  edit <data-type-group_name>
    config type-list
      edit <data-type_index>
        set data-type <type>
      next
    end
  next
end
```

Variable	Description	Default
`<data-type-group_name>`	Type the name of the data type group.	No default.
`<data-type_index>`	Type the index number for a member of the group.	No default.

Variable	Description	Default

`data-type <type>`	For each `data-type` entry, enter one of the following predefined data types exactly as shown:
	• `Address`: Canadian postal codes and United States ZIP code and ZIP + 4 codes.
	• `Canadian_Post_code`: Canadian postal codes such as K2H 7B8.
	• `Canadian_Province_Name`: 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.
	• `Canadian_SIN`: Canadian Social Insurance Numbers (SIN) such as 123-456-789.
	• `China_Post_Code`: Chinese postal codes such as 610000.
	• `Country_Name`: Country names, codes, and abbreviations in English characters, such as CA, Cote d'Ivoire, Brazil, Russian Federation, Brunei, and Dar el Salam.
	• `Credit_Card_Number`: American Express, Carte Blanche, Diners Club, enRoute, Japan Credit Bureau (JCB), Master Card, Novus, and Visa credit card numbers.
	• `Dates_and_Times`: 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.
	• `Email`: Email addresses such as admin@example.com.
	• `L1_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.
	• `L2_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$%.
	• `Markup_or_Code`: HTML comments, wiki code, hexadecimal HTML color codes, quoted strings in VBScript and ANSI SQL, SQL statements, and RTF bookmarks such as:
	  • `#00ccff, <!--A comment.-->`
	  • `[link url="http://example.com/url?var=A&var2=B"]`
	  • `SELECT * FROM TABLE`
	  • `{\*\bkmkstart TagAmountText}`
	Does ***not*** match ANSI escape codes, which are instead detected as strings.
	• `Num`: 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.
	• `Phone`: Australian, United States, and Indian phone numbers in various formats such as (123)456-7890, 1.123.456.7890, 0732105432, and +919847444225.
	• `String`: 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.
	• `Uri`: Uniform resource identifiers (URI) such as http://www.example.com, ftp://ftp.example.com, and mailto:admin@example.com.
	• `US_SSN`: United States Social Security Numbers (SSN) such as 123-45-6789.
	• `US_State_Name`: United States state names and modern postal abbreviations such as HI and Wyoming. Does ***not*** detect older postal abbreviations such as Fl. or Wyo.
	• `US_Zip_Code`: United States ZIP code and ZIP + 4 codes such as 34285-3210.
	Note: You can use the web-based manager to view the regular s that define each predefined data type. For details, see the *FortiWeb Administration Guide*.
		No default.

Example

This example configures a data type group named `data-type-group1` that detects addresses and phone numbers when an auto-learning profile uses it.

```
config server-policy pattern data-type-group
  edit data-type-group1
    config type-list
      edit 1
        set data-type Address
      next
      edit 2
        set data-type Phone
      next
    end
  next
end
```

History

FortiWeb v3.2.1	New.
FortiWeb v3.3.0	Renamed and added redefined data type options to include credit card numbers, United States Social Security Numbers (SSN), and other common formatted strings.

Related topics

- config waf web-protection-profile autolearning-profile
- config server-policy pattern custom-data-type

server-policy pattern suspicious-url-rule

Use this command to add one or more predefined suspicious URL rules to a suspicious URL rule group.

.Each entry in a suspicious URL group defines a type of URL that the FortiWeb unit considers 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.

To see the regular expressions used in the three predefined suspicious URL rules, use the web-based manager. Go To *Server Policy Predefined Pattern Predefined URL Rule*.

Suspicious URL groups are used by auto-learning profiles. For details, see "config server-policy policy" on page 92.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config server-policy pattern suspicious-url-rule
  edit <rule-group_name>
    config type-list
      edit <rule_index>
        set server-type {Apache | IIS | Tomcat}
      next
    end
  next
end
```

Variable	Description	Default
`<rule-group_name>`	Type the name of the suspicious URL rule group.	No default.
`<rule_index>`	Type the index number for a member of the group.	No default.
`server-type {Apache | IIS | Tomcat}`	For each rule index, add one of: • `Apache`: Detect URLs that are usually sensitive for Apache web servers. • `IIS`: Detect URLs that are usually sensitive for Microsoft IIS web servers. • `Tomcat`: Detect URLs that are usually sensitive for Apache Tomcat Java servlet/Java server pages (.jsp) web servers.	No default.

Example

This example configures a suspicious URL rule group named `suspicious-url-group1` that detects HTTP requests for administratively sensitive URLs specific to Apache and Apache Tomcat servers, and could therefore represent attack attempts.

```
config server-policy pattern suspicious-url-rule
  edit suspicious-url-group1
    config type-list
      edit 1
        set server-type Apache
```

```
        next
        edit 2
          set server-type Tomcat
        next
      end
    next
end
```

History

FortiWeb v3.2.1 New.

Related topics

- config waf web-protection-profile autolearning-profile
- config server-policy pattern custom-susp-url

server-policy policy

Use this command to configure server policies.

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

- **Reverse Proxy:** 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.
- **True Transparent Proxy:** Apply the policy whose bridge matches the connection. Do not consider the IP address of the bridge.
- **Transparent Inspection:** Apply the policy whose bridge matches the connection. Do not consider the IP address of the bridge.

The FortiWeb unit will apply only one server policy to each connection.

Policies are not used while they are disabled, as indicated by `status {enable | disable}`.

Policy behavior varies by the operation mode.

Table 10: Policy behavior by operation mode

	Reverse Proxy	Offline Protection	True Transparent Proxy	Transparent Inspection
Matches by	• Service • Virtual server	• Virtual server's network interface, but ***not*** its IP address	• V-zone bridge, but ***not*** its IP address	• V-zone 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	Attempts to block by mimicking the client or server and requesting to reset the connection; does ***not*** modify otherwise
Profile support	• Inline protection profiles • Auto-learning profiles • XML protection profiles	• Offline protection profiles • Auto-learning profiles	• Inline protection profiles • Auto-learning profiles	• Offline protection profiles • 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	Certificate used 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 • 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	Lets the traffic pass through to a member of a server farm, but does ***not*** load-balance

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.

Before you can configure a server policy, you must first configure several policies and profiles:

- Configure a virtual server, a physical server or server farm.
- Configure a health check if needed by the server policy.
- To restrict traffic based upon which hosts you want to protect, configure a group of protected host names.
- If you want the FortiWeb unit to gather auto-learning data, generate or configure an auto-learning profile and its required components.
- If you plan to authenticate users, you need to configure users, user groups, and authentication rules and policy, and include the policy in an inline web protection profile.
- To apply a web protection or XML protection profile to a server policy, you must first configure them.
- 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 either of the transparent modes, 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.

For details, see:

- config server-policy allow-hosts
- config server-policy vserver, config server-policy pserver, config server-policy pservers
- config server-policy health
- config user ldap-user, config user local-user, config user radius-user, config user ntlm-user, config user user-group, config waf http-authen http-authen-rule, config waf http-authen http-authen-policy
- config xml-protection xml-protection-profile (reverse proxy mode), config waf web-protection-profile inline-protection (reverse proxy mode or either of the transparent modes), or config waf web-protection-profile offline-protection (offline protection mode)
- config waf web-protection-profile autolearning-profile
- config system certificate local
- config system certificate verify

Use SNMP traps to notify you of policy status changes, or when a policy enforces your network usage policy. For details, see “config system snmp community” on page 150.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see “Permissions” on page 29.

Syntax

```
config server-policy policy
  edit <policy_name>
    set server-type <type>
    set data-capture-port <interface>
    set monitor-mode {enable | disable}
    set status {enable | disable}
    set type {waf-protection | xml-protection}
    set deployment-mode <method>
    set allow-hosts <protected-hosts_name>
    set case-sensitive {enable | disable}
    set certificate <certificate_name>
    set circulate-url-decode {enable | disable}
    set comment <comment_str>
    set monitor-mode {enable | disable}
```

```
    set block-port <port number>
    set health <health-check_name>
    set intermediate-certificate-group <intermediate-CA-group_name>
    set lb-algo <balance-option>
    set persistence-timeout <timeout_int>
    set persistent-server-sessions <http-sessions_int>
    set pserver <physical-server_name>
    set pserver-port <port_number>
    set pservers <server-farm_name>
    set service <service_name>
    set ssl-client {enable | disable}
    set ssl-client-verify <certificate_verificator_name>
    set ssl-server {enable | disable}
    set vserver <virtual-server_name>
    set v-zone <bridge_name>
    set waf-autolearning-profile <auto-learning-profile_name>
    set web-protection-profile <web-profile_name>
    set xml-protection-profile <xml-protection-profile_name>
  next
end
```

Variable	Description	Default
`<policy_name>`	Type the name of the policy.	No default.
`server-type <type>`	Sets the server type. Only `physical` is available in CLI. To configure a server policy for a domain server, use the web-based manager.	`physical`
`monitor-mode {enable | disable}`	Set `enable` to override deny and redirect actions that have been defined in the server protection rules for the selected policy. This enables FortiWeb to log attacks without performing the deny or redirect action, and to collect more information to build an auto learning profile for the attack. Set `disable` to allow attack deny/redirect actions to be performed as defined by the server protection rules.	`disable`
`data-capture-port <interface>`	Enter a string or port name that identifies the network interface of incoming traffic to which the policy will apply.	No default.
`status {enable | disable}`	Enable to allow the policy to be used when evaluating traffic for a matching policy. **Note:** You can use SNMP traps to notify you of changes to the policy's status. For details, see "config system snmp community" on page 150.	No default.
`type {waf-protection | xml-protection}`	Select whether you will apply an XML protection profile or a web protection/detection profile. Also configure `web-protection-profile <web-profile_name>` or `xml-protection-profile <xml-protection-profile_name>`. Depending on the types of profiles that the current operation mode supports, not all policy types may be available. For details, see Table 10 on page 92.	`xml-protection`

Variable	Description	Default
`deployment-mode <method>`	Select one applicable distribution method that the FortiWeb unit will use when forwarding connections accepted by this policy. • `single-server`: Forward connections to a single physical server. Also configure pserver <physical-server_name>, and pserver-port <port_number>. This option is available only if the FortiWeb unit is operating in reverse proxy mode. • `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 `lb-algo`, and pservers <server-farm_name>. This option is available only if the FortiWeb unit is operating in reverse proxy mode. • `content-routing`: Use content routing rules defined as XPath s 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 health <health-check_name> and pservers <server-farm_name>. This option is available only if the FortiWeb unit is operating in reverse proxy mode and `type` is `xml-protection`. • `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 health <health-check_name> and pservers <server-farm_name>. This option is available only if the FortiWeb unit is operating in reverse proxy mode and `type` is `xml-protection`. • `offline-detection`: Allow connections to pass through the FortiWeb unit, and apply an offline protection profile. Also configure health <health-check_name> and pservers <server-farm_name>. This option is available only if the FortiWeb unit is operating in offline protection mode. • `transparent-servers`: Allow connections to pass through the FortiWeb unit, and apply a protection profile. Also configure pservers <server-farm_name>. This option is available when the FortiWeb unit is operating in either of the transparent modes. Depending on the types of topologies that the current operation mode supports, not all deployment modes may be available. For details, see Table 10 on page 92.	No default.
`allow-hosts <protected-hosts_name>`	Type the name of 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. 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 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.	No default.
`case-sensitive {enable | disable}`	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. For example, when enabled, an HTTP request involving `http://www.`***`E`***`xample.com/` would ***not*** match protection profile features that specify `http://www.`***`e`***`xample.com` (difference highlighted in bold).	No default.
`certificate <certificate_name>`	Type the name of the certificate that the FortiWeb unit will use when encrypting or decrypting SSL-secured connections. This option is used only if `ssl-client` is `enable`.	No default.

Variable	Description	Default
`circulate-url-decode {enable | disable}`	Enable to detect URL-embedded attacks that are obfuscated using recursive URL encoding (that is, multiple levels' worth of URL encoding). Encoded URLs can be legitimately used for non-English URLs, but can also be used to avoid detection of attacks that use special characters. Encoded URLs can now be decoded to scan for these types of attacks. Several encoding types are supported. For example, you could detect the character A that is encoded as either `%41`, `%x41`, `%u0041`, or `\t41`. Disable to decode only one level's worth of the URL, if encoded.	`disable`
`comment <comment_str>`	Type a description or other comment. The description may be up to 35 characters long. If the comment is more than one word, surround the comment with quotes (`'`).	No default.
`monitor-mode {enable | disable}`	Enable to override deny and redirect actions defined in the server protection rules for the selected policy. This enables FortiWeb to log attacks without performing the deny or redirect action, and to collect more information to build an auto learning profile for the attack. Disable to allow attack deny/redirect actions to be performed as defined by the server protection rules	`disable`
`block-port <port number>`	Type the number of the specific interface to send TCP reset packet. This option is available only in offline protection mode.	No default.
`health <health-check_name>`	Type the name of a server health check to use when determining responsiveness of physical servers in the server farm. This option is applicable 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 cannot 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 (see the *FortiWeb Administration Guide*) or an SNMP trap (see "config system snmp community" on page 150).	No default.
`intermediate-certificate-group <intermediate-CA-group_name>`	Select the name of an intermediate certificate authority (CA) group, if any, that will be used to validate the CA signing chain in a client's certificate. This option is applicable only if `ssl-client-verify` is configured and the FortiWeb unit is operating in reverse proxy mode.	No default.
`lb-algo <balance-option>`	Select one of the following load-balancing algorithms 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 `type` is `waf-protection`. This field appears only if `deployment-mode` is `server-balance`.	No default.
`persistence-timeout <timeout_int>`	Enter the timeout for inactive TCP sessions. This field appears only if `deployment-mode` is `server-balance` or `transparent-servers`.	`0`

Variable	Description	Default
`persistent-server-sessions <http-sessions_int>`	Type the maximum number of concurrent TCP client connections that can be accepted by this policy. The maximum number of HTTP sessions for each physical server depends on this field, and whether you have selected a single physical server or a server farm, and `lb-algo`. 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. For more information, see the maximum values matrix in the *FortiWeb Administration Guide*. This option appears only if `deployment-mode` is not `offline-detection`.	`0`
`pserver <physical-server_name>`	Type the name of a single physical server to which to forward connections. This field is applicable only if `deployment-mode` is `single-server`.	No default.
`pserver-port <port_number>`	Type 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. This field is applicable only if `deployment-mode` is `single-server`.	No default.
`pservers <server-farm_name>`	Type the name of the server farm whose physical servers will receive the connections. This option appears only if `deployment-mode` is `server-balance`, `http-content-routing`, `wsdl-content-routing`, `offline-detection`, or `transparent-servers`. **Note:** If `deployment-mode` is `offline-detection` 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.	No default.
`service <service_name>`	Type the custom or predefined service that defines the TCP port number on which the virtual server or bridge receives traffic. This field is applicable only if `deployment-mode` is ***not*** `offline-detection`. **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 {enable | disable}.	No default.
`ssl-client {enable | disable}`	Applies to reverse proxy mode only. Enable if connections from HTTP clients to the FortiWeb unit or protected hosts use SSL. Also configure `certificate <certificate_name>`. FortiWeb units contain specialized hardware to accelerate SSL processing. Offloading SSL processing may improve the performance of secure HTTP (HTTPS) connections. SSL 3.0, TLS 1.0, and TLS 1.1 are supported. SSL 2.0 is supported only in reverse proxy mode. 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 {enable | disable}. This option appears only if the FortiWeb unit is operating in reverse proxy mode or either of the transparent modes. **Note:** If the FortiWeb unit is operating in offline protection mode, you must enable `ssl {enable | disable}` in the server farm instead. **Caution:** You ***must*** enable either this option or ssl-server {enable | disable}, 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.	No default.

Variable	Description	Default
`ssl-client-verify <certificate_verificator_name>`	Select the name of a certificate verifier, 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 the certificate revocation list (CRL) or, if enabled, the online certificate status protocol (OCSP) (see ""config system certificate verify" on page 127) • Be signed by a certificate authority (CA) whose certificate you have imported into the FortiWeb unit (see the *FortiWeb Administration Guide*); if the certificate has been signed by a chain of intermediate CAs, those certificates must be included in an intermediate CA group (see `intermediate-certificate-group <intermediate-CA-group_name>`) • 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 the *FortiWeb Administration Guide*. This option is applicable only if `ssl-client` is `enable`, and only applies if the FortiWeb unit is operating in reverse proxy mode. SSL 3.0 or TLS 1.0 is required. **Note:** If the connection fails when you have selected a certificate verifier, 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 display 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.	No default.
`ssl-server {enable | disable}`	Applies to reverse proxy mode only. Enable to use SSL to encrypt connections from the FortiWeb unit to protected web servers. Disable to pass traffic to protected web servers in clear text. (The FortiWeb unit cannot act as an SSL terminator or initiator in offline protection mode or either of the transparent modes.) **Note:** Enable ***only*** if the protected host supports SSL.	No default.
`vserver <virtual-server_name>`	Type the name of a virtual server. Use of this option varies by operating mode: • reverse proxy: Select the virtual server to indicate the IP address and network interface of incoming traffic that will be routed and to which the policy will apply a profile. • offline protection: Select the virtual server to indicate the network interface of incoming traffic to which the policy will attempt to apply a profile. The IP address of the virtual server will be ignored. This option appears only if the FortiWeb unit is operating in reverse proxy or offline protection mode. Otherwise, configure `v-zone <bridge_name>` instead.	No default.

Variable	Description	Default
`v-zone <bridge_name>`	Select the name of a bridge to whose incoming traffic the policy will apply a profile. This option appears only if the FortiWeb unit is operating in true transparent proxy or transparent inspection mode. Otherwise, configure `vserver <virtual-server_name>` instead.	No default.
`waf-autolearning-profile <auto-learning-profile_name>`	Type the auto-learning profile, if any, to use in order to discover attacks, URLs, and parameters in your web servers' HTTP sessions. Data gathered using an auto-learning profile can be viewed in an auto-learning report, and can be used to generate inline or offline protection profiles. For details, see the *FortiWeb Administration Guide*. This option appears only if `deployment-mode` is `offline-detection`.	No default.
`web-protection-profile <web-profile_name>`	Type the name of the web protection or detection profile to apply to the connections accepted by this policy This field is available only if `type` is `web-protection`.	No default.
`xml-protection-profile <xml-protection-profile_name>`	Type the name of the XML protection profile to apply to the connections accepted by this policy. This field is available only if `type` is `xml-protection`.	No default.

Example

This example configures a web protection server policy. HTTPS connections received by the virtual server named `virtual_ip1` are forwarded to a single physical server named `apache1`. The FortiWeb unit will use the certificate named `certificate1` during SSL negotiations with the client, then forward traffic to the physical server using clear text.

While clients will connect to the virtual server on the FortiWeb unit using TCP port 443, the standard port number for HTTPS connections, the FortiWeb unit will actually forward the connections to TCP port 1443, which is the port number on which the physical server listens.

```
config server-policy policy
  edit "https-policy"
    set type waf-protection
    set deployment-mode single-server
    set vserver "virtual_ip1"
    set service "HTTPS"
    set web-protection-profile "inline-protection1"
    set pserver "apache1"
    set pserver-port 1443
    set persistent-server-sessions 1000
    set ssl-client enable
    set ssl-server disable
    set certificate "certificate1"
    set case-sensitive disable
    set status enable
  next
end
```

History

FortiWeb v3.2.0 New.

FortiWeb v3.2.1 New field `waf-autolearning-profile`.

FortiWeb v3.3.0	New field `circulate-url-decode`. Enables recursive URL decoding in order to scan for URL-embedded attacks. Behavior change. Policies inapplicable to the current operation mode can no longer be created. Inapplicable policies will also be deleted when changing the operation mode.
FortiWeb v3.3.2	Renamed field `ssl` to `ssl-client`. New field `ssl-server`. Enables the FortiWeb unit to connect to protected host(s) using SSL.
FortiWeb v4.0.0	New field `ssl-client-verify`. Enables verification of personal certificates for certificate-based client authentication. New field `v-zone`. Selects which bridge will be used to match connections to the policy. New option `transparent-servers` for field `deployment-mode`. Instead of using a single server, either of the transparent modes now allows connections to pass through to any member of the server farm, similar to offline protection mode. Behavior change. Policies for either of the transparent modes now require server farms and cannot use single servers.
FortiWeb v4.0.1	New field `intermediate-certificate-group`. Selects use of an intermediate CA group in order to verify a signing chain on the client's certificate.
FortiWeb v4.1.1	New field `monitor-mode`. Enables override of deny and redirect actions for the selected policy so attacks can be logged without performing the deny or redirect action to collect more information for an auto learning profile for the attack.
FortiWeb v4.2	Added new set statements `server-type`, `data-capture-port`, and `monitor-mode`.

Related topics

- config server-policy allow-hosts
- config system certificate local
- config server-policy health
- config server-policy pserver
- config server-policy pservers
- config server-policy service custom
- config server-policy vserver
- config system dos-prevention
- config system snmp community
- config system settings
- config system v-zone
- config waf web-protection-profile autolearning-profile
- config waf web-protection-profile inline-protection
- config waf web-protection-profile offline-protection
- config xml-protection xml-protection-profile

server-policy pserver

Use this command to configure 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.

To apply physical servers, select them within a server policy or a server farm that is selected in a policy. For details, see "config server-policy policy" on page 92 or ""config server-policy pserver" on page 101.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config server-policy pserver
  edit <physical-server_name>
    set ip <server_ipv4>
    set status {enable | disable}
  next
end
```

Variable	Description	Default
`<physical-server_name>`	Type the name of a physical server.	No default.
`status {enable | disable}`	Enable to forward connections accepted by the policy to the physical server.	No default.
`ip <server_ipv4>`	Type the IP address of a physical server.	`0.0.0.0`

Example

This example configures a physical server named `soap-server1`.

```
config server-policy pserver
  edit "soap-server1"
    set ip 172.16.1.10
    set status enable
  next
end
```

History

FortiWeb v3.2.0 New.

Related topics

- config server-policy policy
- config server-policy pservers

server-policy pservers

Use this command to configure server farms.

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

- In reverse proxy 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.

  You can assign different weights to each physical server in the server farm, if you are using load-balancing with a weighted algorithm and you want to adjust the proportion of connections that each physical server receives. More connections are forwarded to physical servers with greater weights.

  To prevent traffic from being forwarded to unavailable physical servers, verify the availability of physical servers in a server farm 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 "config server-policy policy" on page 92.
- In offline protection and either of the transparent modes, when the FortiWeb unit receives traffic destined for a virtual server or passing through a bridge, it allows the traffic to pass directly through to members of the server farm.

To apply server farms, select them within a server policy. For details, see "config server-policy policy" on page 92.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config server-policy pservers
  edit <server-farm_name>
    set <comment>
    set type <distribution>
    set http-conversion-policy <policy_name>
    config pserver-list
      edit <entry_index>
        set server-type {physical | domain}
        set pserver <physical-server_name>
        set dserver <domain-server_name>
        set certificate <certificate_name>
        set http-content-routing-policy <policy_name>
        set port <port_number>
        set ssl {enable | disable}
        set weight <weight_int>
        set wsdl-content-routing-table <wsdl-content-routing-group_name>
        set xpath-expression <xpath_str>
      next
    end
  next
end
```

Variable	Description	Default
<server-farm_name>	Type the name of the server farm.	No default.
<comment>	Type a description for the server farm.	No default.
type <distribution>	Select the method of distribution that the FortiWeb unit will use when forwarding connections to the physical servers in this server farm. It is one of: http-content-routing, offline-protection, server-balance, transparent-servers, wsdl-content-routing, xml-content-routing. For details, see "deployment-mode" in "config server-policy policy" on page 92.	server-balance
http-conversion-policy <policy_name>	Optionally, select the http conversion policy if HTTP host names and URLs must be converted before HTTP content can be routed to a specific physical server. For more information, see "config server-policy http-conversion-policy" on page 82.	No default.
<entry_index>	Type the index number of the physical server entry within the server farm. 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. **Note:** 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.***	No default.
server-type {physical | domain}	Set the server type.	physical
certificate <certificate_name>	Type the name of the physical server's certificate that the FortiWeb unit will use when decrypting SSL-secured connections.	No default.
http-content-routing-policy <policy_name>	Select the HTTP content routing policy to route HTTP requests to a specific physical server in a server farm by specifying the host or URL and the request file.	No default.
port <port_number>	Type the TCP port number on which the physical server listens for connections.	0
pserver <physical-server_name>	Type the name of a physical server that will be a member of the server farm. This option appears only when server-type is set to physical.	No default.
dserver <domain-server_name>	Type the name of a domain server that will be a member of the server farm. This option appears only when server-type is set to domain.	No default.

Variable	Description	Default
`ssl {enable | disable}`	Enable if connections to the server use SSL, ***and*** if the FortiWeb unit is operating in offline protection mode or either of the transparent modes. Also configure `certificate <certificate_name>`. Unlike `ssl-client {enable | disable}` in policies, when you select 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. SSL 3.0, TLS 1.0, and TLS 1.1 are supported. **Caution:** You ***must*** enable either this option or `ssl-client {enable | disable}` in the policy 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. **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. **Note:** Ephemeral (temporary key) Diffie-Hellman exchanges are not supported if the FortiWeb unit is operating in offline protection mode.	No default.
`weight <weight_int>`	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.	`0`
`wsdl-content-routing-table <wsdl-content-routing-group_name>`	Type 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 "config xml-protection wsdl-content-routing-table" on page 259. **Note:** You can alternatively or additionally configure `xpath-expression <xpath_str>`.	No default.
`xpath-expression <xpath_str>`	Type an XPath expression. HTTP requests with content matching this expression will be routed to this physical server. **Note:** For web services connections, you can alternatively or additionally configure `wsdl-content-routing-table <wsdl-content-routing-group_name>`.	No default.

Example

This example configures a server farm named `server-farm1`, which consists of two physical servers: `physical-server1` and `physical-server2`.

When both servers are available, SOAP requests matching `wsdl-content-routing-group1` are forwarded to `physical-server2`; all others are forwarded to `physical-server1`. If `physical-server2` is down, all requests are forwarded to `physical-server1`, because it is the first physical server in the server farm.

```
config server-policy pservers
  edit "server-farm1"
    set comment "SOAP servers in rack 2"
    config pserver-list
      edit 1
        set pserver "physical-server1"
        set ssl disable
        set port 8081
      next
      edit 2
        set pserver "physical-server2"
        set ssl disable
        set port 8082
        set "wsdl-content-routing-group1"
      next
    end
```

```
    next
end
```

History

FortiWeb v3.2.0	New.
FortiWeb v4.1.1	Changed. Added new settings for comment, http-conversion-policy, type and http-content-routing-policy.
FortiWeb v4.2	Added new set statements `server-type` and `dserver`.

Related topics

- config server-policy policy
- config server-policy http-content-routing-policy
- config server-policy http-conversion-policy
- config system certificate local
- config server-policy pserver
- config xml-protection wsdl-content-routing-table

server-policy service custom

Use this command to configure a custom service.

You can add a custom services to a policy to define the protocol and listening port of a virtual server. For details, see “config server-policy policy” on page 92.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see “Permissions” on page 29.

Syntax

```
config server-policy service custom
  edit <service_name>
    set port <port_number>
    set protocol TCP
  next
end
```

Variable	Description	Default
`<service_name>`	Type the name of a custom network service, such as `SOAP1`	No default.
`port <port_number>`	Type the TCP port number on which a virtual server will receive HTTP or HTTPS connections.	`0`

Example

This example configures a service definition named `SOAP1`.

```
config server-policy custom
  edit "SOAP1"
    set port 8081
    set protocol TCP
  next
end
```

History

FortiWeb v3.2.0 New.

Related topics

- config server-policy vserver
- config server-policy policy
- config server-policy service predefined

server-policy service predefined

Use this command to view a predefined service. You can edit the port number and protocol but FortiWeb discards your changes.

Predefined Internet services can be selected in a policy in order to define the protocol and listening port of a virtual server. For details, see "config server-policy policy" on page 92.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config server-policy service predefined
  edit <service_name>
    show
  next
end
```

Variable	Description	Default
`<service_name>`	Displays the name of a predefined network service, such as `HTTP` or `HTTPS`.	No default.
`port <port_number>`	Displays the port number on which a virtual server will receive HTTP or HTTPS connections.	No default.
`protocol {TCP | UDP}`	Displays the applicable protocol: `TCP` or `UDP`.	No default.

Example

This examples shows the default settings for the predefined services.

```
config server-policy service predefined
  show

config server-policy service predefined
  edit "HTTP"
    set port 80
    set protocol TCP
  next
  edit "HTTPS"
    set port 443
    set protocol TCP
  next
end
```

History

FortiWeb v4.2. New.

Related topics

- config server-policy vserver
- config server-policy policy
- config server-policy service custom

server-policy vserver

Use this command to configure 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 reverse proxy 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.

To apply virtual servers, select them within a server policy. For details, see "config server-policy policy" on page 92.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config server-policy vserver
  edit <virtual-server_name>
    set status {enable | disable}
    set interface <interface_name>
    set vip <virtual-ip_ipv4mask>
  next
end
```

Variable	Description	Default
`<virtual-server_name>`	Type the name of the virtual server.	`disable`
`status {enable | disable}`	Enable to accept traffic destined for this virtual server.	No default.
`interface <interface_name>`	Type the name of the network interface or bridge, such as `port1` or `bridge1`, to which the virtual server is bound, and on which traffic destined for the virtual server will arrive.	No default.
`vip <virtual-ip_ipv4mask>`	Type the IP address and subnet of the virtual server.	`0.0.0.0 0.0.0.0`

Example

This example configures a virtual server named `inline_vip1` on the network interface named `port1`.

The TCP port number on which the virtual server will receive traffic is defined separately, in the policies that use this virtual server definition.

```
config server-policy vserver
  edit "inline_vip1"
    set vip 10.0.0.1 255.255.255.0
    set interface port1
    set status enable
  next
end
```

History

FortiWeb v3.2.0	New.
FortiWeb v3.3.1	Behavior change to field `interface`. Now accepts the name of a network interface or the name of a bridge, depending on the operation mode.

Related topics

- config system interface
- config server-policy policy
- config server-policy service custom

system accprofile

Use this command to configure access control profiles for administrators.

Access profiles specify which parts of the FortiWeb configuration interface an administrator is permitted to access, and whether that administrator is permitted to view (`r`), modify (`w`), or both (`rw`). The default administrator account, `admin`, uses the preconfigured `prof_admin` access profile, and has full access to all parts of the configuration. That profile cannot be viewed, changed, or deleted.

If you create other administrator accounts, you may want to create other access profiles with different degrees and areas of access.

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.

To view and modify the list of access profiles, you must log in using either the `admin` administrator account, or an administrator account whose access profile contains both `r` and `w` permissions to items in the `admingrp` category.

For information on how each access control area correlates to which CLI commands that administrators can access, see “Permissions” on page 29

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `admingrp` area.

Syntax

```
config system accprofile
  edit <access-profile_name>
    set admingrp {none | r | rw | w}
    set authusergrp {none | r | rw | w}
    set learngrp {none | r | rw | w}
    set loggrp {none | r | rw | w}
    set mntgrp {none | r | rw | w}
    set netgrp {none | r | rw | w}
    set routegrp {none | r | rw | w}
    set sysgrp {none | r | rw | w}
    set traroutegrp {none | r | rw | w}
    set wadgrp {none | r | rw | w}
    set webgrp {none | r | rw | w}
    set wvsgrp {none | r | rw | w}
    set xmlgrp {none | r | rw | w}
  next
end
```

Variable	Description	Default
`<access-profile_name>`	Type the name of the access profile.	No default.
`admingrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the system administrator configuration.	`none`
`authusergrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the HTTP authentication user configuration.	`none`

Variable	Description	Default
`learngrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the auto-learning profiles and their resulting auto-learning reports.	none
`loggrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the logging and alert email configuration.	none
`mntgrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to maintenance commands. Unlike the other rows, whose scope is an area of the configuration, the maintenance access control area does not affect the configuration. Instead, it indicates whether the administrator can perform special system operations such as changing the firmware.	none
`netgrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the network interface configuration.	none
`routegrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the routing configuration.	none
`sysgrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the basic system configuration (except for areas included in other access control areas such as `admingrp`).	none
`traroutegrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the server policy (formerly called traffic routing) configuration.	none
`wadgrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the web anti-defacement configuration.	none
`webgrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the web protection profile configuration.	none
`wvsgrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the web vulnerability scanner.	none
`xmlgrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the XML protection profile configuration.	none

Example

This example configures an administrator access profile named `full_access`, which permits both read and write access to all special operations and parts of the configuration.

Note: Even though this access profile configures full access, administrator accounts using this access profile will ***not*** be fully equivalent to the `admin` administrator. The `admin` administrator has some special privileges that are inherent in that account and cannot be granted through an access profile, such as the ability to reset other administrators' passwords without knowing their current password.

```
config system accprofile
  edit "full_access"
    set admingrp rw
    set authusergrp rw
    set learngrp rw
    set loggrp rw
    set mntgrp rw
    set netgrp rw
    set routegrp rw
    set sysgrp rw
    set traroutegrp rw
    set wadgrp rw
    set webgrp rw
```

```
    set wvsgrp rw
    set xmlgrp rw
  next
end
```

History

FortiWeb v3.2.0	New.
FortiWeb v3.3.2	Added field `wadgrp`. Configures read, write, read-write, or no access to the web site anti-defacement-related CLI commands and tabs in the web-based manager.
FortiWeb v4.0.0	Added field `wvsgrp`. Configures read, write, read-write, or no access to the web vulnerability scanner in the web-based manager. Added field `authusergrp`. Configures read, write, read-write, or no access to HTTP authentication user CLI commands and tabs in the web-based manager. Changed `traroutegrp`. No longer controls certificate access, which is now controlled by `sysgrp`.

Related topics

- config system admin
- “Permissions”

system admin

Use this command to configure FortiWeb administrator accounts. In its factory default configuration, a FortiWeb unit has one administrator account, named `admin`. That 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 can access the web-based manager and 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 "config system interface" on page 142.

To see which administrators are logged in, use the CLI command get system logged-users.

Tip: To prevent multiple administrators from logging in simultaneously, which could allow them to inadvertently overwrite each other's changes, enable `single-admin-mode {enable | disable}`. For details, see "config system global" on page 134.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `adminegrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system admin
  edit <administrator_name>
    set accprofile <access-profile_name>
    set password <password_str>
    set email-address <contact_email>
    set first-name <name_str>
    set last-name <surname_str>
    set mobile-number <cell-phone_str>
    set phone-number <phone_str>
    set trusthost1 <management-computer_ipv4mask>
    set trusthost2 <management-computer_ipv4mask>
    set trusthost3 <management-computer_ipv4mask>
    set is-default-config {yes | no}
  next
end
```

Variable	Description	Default
`<administrator_name>`	Type the name of the administrator account as they will enter it to log in to the web-based manager or CLI, such as `admin1`.	No default.
`accprofile <access-profile_name>`	Type the name of an access profile that gives the permissions for this administrator account. See "config system accprofile" on page 110.	No default.
`password <password_str>`	Type 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.	No default.
`email-address <contact_email>`	Type an email address that can be used to contact this administrator.	No default.
`first-name <name_str>`	Type the first name of the administrator.	No default.
`last-name <surname_str>`	Type the surname of the administrator.	No default.
`mobile-number <cell-phone_str>`	Type a cell phone number that can be used to contact this administrator.	No default.

Variable	Description	Default
`phone-number <phone_str>`	Type a phone number that can be used to contact this administrator.	No default.
`trusthost1 <management-computer_ipv4mask>`	Type the IP address and netmask of a management computer or management LAN from which the administrator is allowed to log in to the FortiWeb unit. You can specify up to three trusted hosts. To allow login attempts from any IP address, enter `0.0.0.0/0.0.0.0`. If you allow logins 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 "config system interface" on page 142. **Note:** For improved security, restrict all three trusted host addresses to the IP addresses of computers from which only this administrator will log in.	`0.0.0.0 0.0.0.0`
`trusthost2 <management-computer_ipv4mask>`	Type a second IP address and netmask of a management computer or management LAN from which the administrator is allowed to log in to the FortiWeb unit. To allow login attempts from any IP address, enter `0.0.0.0/0.0.0.0`.	`0.0.0.0 0.0.0.0`
`trusthost3 <management-computer_ipv4mask>`	Type a third IP address and netmask of a management computer or management LAN from which the administrator is allowed to log in to the FortiWeb unit. To allow login attempts from any IP address, enter `0.0.0.0/0.0.0.0`.	`0.0.0.0 0.0.0.0`
`is-default-config {yes | no}`	Enter yes to set this configuration as the default for all managers without a specific assigned access profile.	`no`

Example

This example configures an administrator account named `log-auditor`, which uses an access profile that grants only permission to read the logs. This account can log in only from an IP address on the management LAN (172.16.2.0/24), or from one of two specific IP addresses (172.16.3.15 and 192.168.1.50).

```
config system admin
  edit "log-auditor"
    set accprofile "log_read_access"
    set password P@ssw0rd
    set email-address log-admin@example.com
    set trusthost1 172.16.2.0 255.255.255.0
    set trusthost2 172.16.3.15 255.255.255.255
    set trusthost3 192.168.1.50 255.255.255.255
  next
end
```

History

FortiWeb v3.2.0 New.

Related topics

- config system accprofile
- config system interface
- config system global
- config system console
- get system logged-users

system autoupdate override

Use this command to override the default Fortiguard Distribution Server (FDS).

If you cannot connect to the FortiGuard Distribution Network (FDN) or if your organization provides updates using their own FortiGuard server, you can override the FDS server setting so that the FortiWeb unit connects to this server instead of the default server on Fortinet's public FDN.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system autoupdate override
  set status {enable | disable}
  set address {<fds_fqdn> | <fds_ipv4>}
  set fail-over {enable | disable}
end
```

Variable	Description	Default
`status {enable | disable}`	Enable to override the default list of FDN servers, and connect to a specific server.	`disable`
`address {<fds_fqdn> | <fds_ipv4>}`	Type the IP address or fully qualified domain name (FQDN) of the override FDS.	No default.
`fail-over {enable | disable}`	Enable to fail over to one of the public FDN servers if FortiWeb cannot reach the specified FDS.	`enable`

History

FortiWeb v4.0.0 New.

Related topics

- config system autoupdate schedule

system autoupdate schedule

Use this command to configure how the FortiWeb unit will access the FortiGuard Distribution Network (FDN) to retrieve updates. The FDN is a world-wide network that updates the FortiWeb unit's repository of predefined robots, data types, suspicious URLS, and attack signatures used to detect attacks such as:

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

Tip: Alternatively, you can manually upload update packages. For details, see the *FortiWeb Administration Guide*.

FortiWeb units connect to the FDN by connecting to the Fortiguard Distribution Server (FDS) nearest to the FortiWeb unit based on its configured time zone.

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

If you want to connect to a specific FDS, you must configureconfig system autoupdate override. If your FortiWeb unit must connect through a web proxy, you must also configure config system autoupdate tunneling.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system autoupdate schedule
  set status {enable | disable}
  set frequency {daily | every | weekly}
  set time <time_str>
  set day {update_day}
end
```

Variable	Description	Default
`status {enable | disable}`	Enable to periodically request signature updates from the FDN.	`disable`
`frequency {daily | every | weekly}`	Type the frequency with which the FortiWeb unit will request signature updates.	`every`
`time <time_str>`	Type the hours and minutes, according to a 24-hour clock, in hh:mm format, which the FortiWeb unit will request signature updates.	`00:00`
`day {update_day}`	Type which day of the week that the FortiWeb unit will request signature updates. This option applies only if `frequency` is `weekly`. Type the full name with an initial capital; for example, `Saturday`.	`Monday`

Example

This example configures weekly signature update requests on Sunday at 2:00 PM.

```
config system autoupdate schedule
  set status enable
  set frequency weekly
  set day Sunday
  set time 14:00
end
```

History

FortiWeb v4.0.0 New.

Related topics

- config system autoupdate override
- config system autoupdate tunneling
- config system global

system autoupdate tunneling

Use this command to configure the FortiWeb unit to use a proxy server to connect to the FortiGuard Distribution Network (FDN).

The FortiWeb unit will connect to the proxy using the HTTP `CONNECT` method, as described in RFC 2616.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system autoupdate tunneling
  set status {enable | disable}
  set address {<proxy_fqdn> | <proxy_ipv4>}
  set port <port_number>
  set username <proxy-user_str>
  set password <proxy-password_str>
end
```

Variable	Description	Default
`status {enable | disable}`	Enable to connect to the FDN through a web proxy.	`disable`
`address {<proxy_fqdn> | <proxy_ipv4>}`	Type the IP address or fully qualified domain name (FQDN) of the web proxy.	No default.
`port <port_number>`	Type the port number on which the web proxy listens for connections.	`0`
`username <proxy-user_str>`	If the proxy requires authentication, type the FortiWeb unit's login name on the web proxy.	No default.
`password <proxy-password_str>`	If the proxy requires authentication, type the password for the FortiWeb unit's login name on the web proxy.	No default.

Example

This example configures the FortiWeb unit to connect through a web proxy that requires authentication.

```
config system autoupdate tunneling
  set status enable
  set address 192.168.1.10
  set port 1443
  set username fortiweb
  set password myPassword1
end
```

History

FortiWeb v4.0.0 New.

Related topics

- config system autoupdate schedule

system certificate ca

Use this command to edit the comment associated with a certificate for a certificate authority (CA).

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

CA certificates are required by connections that use SSL or transport layer security (TLS).CA certificates are not used directly, but must first be grouped in order to be selected in a certificate verification rule. For details, see "config system certificate ca-group" on page 120.

For information on how to upload a certificate file, see the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system certificate ca
  edit <certificate_name>
    set comment <comment_str>
  next
end
```

Variable	Description	Default
`<certificate_name>`	Type the name of a CA certificate file.	No default.
`comment <comment_str>`	Type a description or comment. If the comment is more than one word, surround the words with quotes (`'`).	No default.

History

FortiWeb v4.0.0 New.

FortiWeb v4.1 Access control profile changed from `sysgrp` to `admingrp`.

Related topics

- config system certificate ca-group
- config system certificate verify

system certificate ca-group

Use this command to group certificate authorities (CA).

CAs must belong to a group in order to be selected in a certificate verification rule.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system certificate ca-group
  edit <ca-group_name>
    config members
      edit <ca_index>
        set name <ca_name>
      next
    end
  next
end
```

Variable	Description	Default
`<ca-group_name>`	Type the name of a certificate authority (CA) group.	No default.
`<ca_index>`	Type the index number of a CA within its group.	No default.
`name <ca_name>`	Type the name of a previously uploaded CA certificate.	No default.

Example

This example groups two CA certificates into a CA group named `caVEndors1`.

```
config system certificate ca-group
  edit "caVendors1"
    config members
      edit 1
        set name "CA_Cert_1"
      next
      edit 2
        set name "CA_Cert_2"
      next
    end
  next
end
```

History

FortiWeb v4.0.0 New.

FortiWeb v4.1 Access control profile changed from `sysgrp` to `admingrp`.

Related topics

- config system certificate local
- config system certificate verify

system certificate crl

Use this command to edit the comment or URL associated with a previously uploaded certificate revocation list (CRL).

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 status. For more information, see “config system certificate remote” on page 126.

For information on how to upload a CRL, see the *FortiWeb Administration Guide*.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see “Permissions” on page 29.

Syntax

```
config system certificate crl
  edit <crl_name>
    set comment <comment_str>
    set url <server_url>
  next
end
```

Variable	Description	Default
`<crl_name>`	Type the name of a CRL.	No default.
`comment <comment_str>`	Type a description or other comment. If the comment is more than one word, surround the words with quotes (').	No default.
`url <server_url>`	If you did not upload a CRL file, but instead will query for it from an HTTP or OCSP server, enter the URL of the CRL.	No default.

History

FortiWeb v4.0.0 New.

FortiWeb v4.1 Access control profile changed from `sysgrp` to `admingrp`.

Related topics

- config system certificate local
- config system certificate verify

system certificate intermediate-certificate

Use this command to edit the comment associated with an intermediate CA certificate.

For information on how to upload an intermediate certificate file, see the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system certificate intermediate-certificate
  edit <int-certificate_name>
    set comment <comment_str>
  next
end
```

Variable	Description	Default
`<int-certificate_name>`	Type the name of an intermediate certificate file.	No default.
`comment <comment_str>`	Type a description or other comment. If the comment is more than one word, surround the words with quotes (').	No default.

History

FortiWeb v4.0.1 New.

FortiWeb v4.1 Access control profile changed from `sysgrp` to `admingrp`.

Related topics

- config server-policy pservers
- config server-policy policy

system certificate intermediate-certificate-group

Use this command to group intermediate CA certificates.

Intermediate CAs must belong to a group in order to be selected in a certificate verification rule.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system certificate intermediate-certificate-group
  edit <intermediate-ca-group_name>
    config members
      edit <intermediate-ca_index>
        set name <ca_name>
      next
    end
  next
end
```

Variable	Description	Default
`<intermediate-ca-group_name>`	Type the name of an intermediate certificate authority (CA) group.	No default.
`<intermediate-ca_index>`	Type the index number of an intermediate CA within its group.	No default.
`name <ca_name>`	Type the name of a previously uploaded intermediate CA certificate.	No default.

History

FortiWeb v4.0.1 New.

FortiWeb v4.1 Access control profile changed from `sysgrp` to `admingrp`.

Related topics

- config server-policy pservers
- config server-policy policy

system certificate local

Use this command to edit the comment associated with a server certificate that is 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 reverse proxy mode only)

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

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 hosts. Then, select which one the FortiWeb unit will use when configuring the SSL option in a policy or server farm.

For information on how to upload a certificate file, see the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system certificate local
  edit <certificate_name>
    set comment <comment_str>
    set password <password_str>
    set status {na | ok | pending}
    set type {certificate | csr}
    set flag <integer>
  next
end
```

Variable	Description	Default
`<certificate_name>`	Type the name of a certificate file.	No default.
`comment <comment_str>`	Type a description or other comment. If the comment contains more than one word, enclose the words in quotes (').	No default.
`password <password_str>`	If uploading a certificate, type the password for the certificate.	No default.
`status {na | ok | pending}`	Indicates the status of an imported certificate: • `na` indicates that the certificate was successfully imported, and is currently selected for use by the FortiWeb unit. • `ok` indicates that the certificate was successfully imported but is not selected as the certificate currently in use. To use the certificate, select it in a policy or server farm. • `pending` indicates that the certificate request was generated, but must be downloaded, signed, and imported before it can be used as a local certificate.	No default.

Variable	Description	Default
`type {certificate | csr}`	Indicates whether the file is a certificate or a certificate signing request (CSR).	No default.
`flag <integer>`	Indicates if a password was saved. This is used by FortiWeb for backwards compatibility.	No default

Example

This example adds a comment to the certificate named `certificate1`.

```
config system certificate local
  edit certificate1
    set comment 'This is a certificate for the host www.example.com.'
  next
end
```

History

FortiWeb v3.2.0	New.
FortiWeb v4.0.0	Renamed config server-policy certificate to config system certificate local.
FortiWeb v4.1	Access control profile changed from `sysgrp` to `admingrp`.

Related topics

- config server-policy pservers
- config server-policy policy

system certificate remote

Use this command to edit the comment and URL associated with 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 on how to upload a certificate file, see the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system certificate remote
  edit <ocsp_name>
    set comment <comment_str>
    set ocsp_url <server_url>
  next
end
```

Variable	Description	Default
`<ocsp_name>`	Type the name of an OCSP certificate file.	No default.
`comment <comment_str>`	Type a description or other comment. If the comment is more than one word, surround the comment with quotes (`'`).	No default.
`ocsp_url <server_url>`	If you want to query for the server's certificate from its URL, enter the URL of the server.	No default.

History

FortiWeb v4.0.0 New.

FortiWeb v4.1 Access profile changed from `sysgrp` to `admingrp`.

Related topics

- config system certificate local
- config system certificate verify

system certificate verify

Use this command to configure how the FortiWeb unit will verify certificates presented by HTTP clients.

To apply a certificate verification rule, select it in a policy. For details, see "config server-policy policy" on page 92.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system certificate verify
  edit <certificate_verificator_name>
    set ca <ca-group_name>
    set crl <crl_name>
    set ocsp <remote_name>
  next
end
```

Variable	Description	Default
`<certificate_verificator_name>`	Type the name of a certificate verifier.	No default.
`ca <ca-group_name>`	Type the name of a CA group, if any, that you want to use to authenticate client certificates.	No default.
`crl <crl_name>`	Type the name of a certificate revocation list, if any, to use to verify the revocation status of client certificates.	No default.
`ocsp <remote_name>`	Type 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.	No default.

History

FortiWeb v4.0.0 New.

FortiWeb v4.1 Access profile changed from `sysgrp` to `admingrp`.

Related topics

- config system certificate ca-group
- config system certificate crl
- config system certificate remote
- config server-policy policy

system conf-sync

Use this command to synchronize the configuration information on the local FortiWeb unit with a peer (remote) FortiWeb unit. As a result, the configuration information on the peer FortiWeb unit is updated with that of the local FortiWeb unit. This type of synchronization is used between FortiWeb units that are not part of a high availability (HA) pair.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system conf-sync
  set ip <ipv4>
  set password <password-str>
  set sync-type {full-sync | partial-sync}
  set server-port <port_number>
end
```

Variable	Description	Default
`ip <ipv4>`	Enter the IP address of the remote FortiWeb unit that you want to synchronize with the local FortiWeb unit.	`0.0.0.0`
`password <password-str>`	Type the administrator password for the remote FortiWeb unit.	No default.
`sync-type {full-sync | partial-sync}`	Set the synchronization type. The `full-sync` option has no effect if the operation mode is set to reverse proxy. See "config system settings" on page 148.	`partial-sync`
`server-port <port_number>`	Type the port number of the remote (peer) FortiWeb unit that is used to connect to the local unit for configuration synchronization. ***Warning***: The port number used with this command must be different than the port number used with config system global command or the submitting operation will fail.	`8333`

The `full-sync` command updates all configuration files on the peer FortiWeb unit, except network interfaces and administration configuration data. The `partial-sync` command updates configuration files on the peer FortiWeb unit, with the exception of configurations set using:

- `config system`
- `config router`
- `config server-policy` commands for `policy`, `health`, `dserver`, `pserver`, `pservers`, `vserver`, `service`, `http-content-routing-policy`, and `http-conversion-policy`

To use this command, in your administrator account's access control profile, you must have either `w` or `rw` permission to the `netgrp` area. For more information, see "Permissions" on page 29.

History

FortiWeb v4.2. New.

system console

Use this command to configure the management console settings. Usually this is set during the early stages of installation and needs no adjustment.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system console
  set baudrate {9600 | 19200 | 38400 | 57600 | 115200}
  set mode {batch | line}
  set output {more | standard}
end
```

Variable	Description	Default
`baudrate {9600 | 19200 | 38400 | 57600 | 115200}`	Type the baud rate of the console connection. The rate should conform to the specs for your unit.	`9600`
`mode {batch | line}`	Select console input mode of batch or line.	`line`
`output {more | standard}`	Type either: • `more`: When displaying multiple pages' worth of output, pause after displaying each page's worth of text. When the display pauses, the last line displays `--More--`. You can then either: • Press the spacebar to display the next page. • Type `Q` to truncate the output and return to the command prompt. • `standard`: Do not pause between pages' worth of output, and do not offer to truncate output.	`alert`

Example

This example configures the local console connection to operate at 9,600 baud, and to show long output in a paged format.

```
config system console
  set baudrate 9600
  set output more
end
```

History

FortiWeb v3.2.0 New.

Related topics

- config system admin

system dns

Use this command 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. Use either the DNS servers supplied by your Internet service provider (ISP) or the IP addresses of your own DNS servers.

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system dns
  set primary <dns_ipv4>
  set secondary <dns_ipv4>
  set domain <local-domain_str>
end
```

Variable	Description	Default
`primary <dns_ipv4>`	Type the IP address of the primary DNS server.	`0.0.0.0`
`secondary <dns_ipv4>`	Type the IP address of the secondary DNS server.	`0.0.0.0`
`domain <local-domain_str>`	Type the name of the local domain to which the FortiWeb unit belongs, if any. This field is optional. It will not appear in the `Host:` field of HTTP headers for client connections to protected web servers. **Note:** You can also configure the host name. For details, see "config system global" on page 134.	No default.

Example

This example configures the FortiWeb unit with the name of the local domain to which it belongs, example.com. It also configures its host name, `fortiweb`. Together, this configures the FortiWeb unit with its own fully qualified domain name (FQDN), fortiweb.example.com.

```
config system global
  set hostname "fortiweb"
end
config system dns
  set domain example.com
end
```

History

FortiWeb v3.2.0 New.

Related topics

- config log syslog-policy
- config router static

- config system interface
- config system global
- config server-policy policy

system dos-prevention

Use this command to configure protection from TCP SYN flood-style denial of service (DoS) attacks. Once you configure DoS protection, the FortiWeb unit automatically applies it to connections matching any server policy.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system dos-prevention
  set syncookie {enable | disable}
  set half-open-threshold <syn-rate_int>
  set severity {High | Medium | Low}
  set trigger <trigger-policy_name>
end
```

Variable	Description	Default
`syncookie {enable | disable}`	Enable to detect TCP SYN flood attacks.	`disable`
`half-open-threshold <syn-rate_int>`	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 treats the traffic as a DoS attack and ignores additional traffic from that source address.	`100`
`severity {High | Medium | Low}`	Enter the severity level you want FortiWeb to use in the records and reports generated when a violation of the HTTP request method policy occurs.	`High`
`trigger <trigger-policy_name>`	Type the name of the trigger policy you want FortiWeb to apply when a DoS violation occurs.	No default.

History

FortiWeb v3.2.1 New.

FortiWeb v4.2 Set statements `severity` and `trigger` added.

Related topics

- config server-policy policy

system fail-open

Use this command to configure fail-to-wire behavior if the FortiWeb unit shuts down, reboots, or unexpectedly loses power.

Fail-open applies only for FortiWeb models with a CP7 processor, such as the FortiWeb-1000C and FortiWeb-3000C, and only when operating in either of the transparent modes.

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.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system fail-open
  set type {poweroff-bypass | poweroff-keep}
end
```

Variable	Description	Default
`type {poweroff-bypass | poweroff-keep}`	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.	`poweroff-bypass`

History

FortiWeb v4.0.1 New.

system global

Use this command to configure the language, display refresh rate and listening ports of the web-based manager, the time zone and host name of the FortiWeb unit, and NTP time synchronization.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system global
  set admin-port <port_number>
  set admin-sport <port_number>
  set admintimeout <minutes_int>
  set confsync-port <port-number>
  set dst {enable | disable}
  set hostname <host_name>
  set ie6workaround {enable | disable}
  set language {english | japanese | simch | trach}
  set ntpserver {<ntp_fqdn> | <ntp_ipv4>}
  set ntpsync {enable | disable}
  set refresh <seconds_int>
  set single-admin-mode {enable | disable}
  set ssl-md5 {enable/disable}
  set strong-password {enable | disable}
  set syncinterval <minutes_int>
  set timezone <time-zone-code_str>
  set weak_enc {enable | disable}
end
```

Variable	Description	Default
`admin-port <port_number>`	Type the TCP port number on which the FortiWeb unit will listen for HTTP access to the web-based manager. The valid range is from 1 to 65,535.	`80`
`admin-sport <port_number>`	Type the TCP port number on which the FortiWeb unit will listen for HTTPS (SSL-secured) access to the web-based manager. The valid range is from 1 to 65,535.	`443`
`admintimeout <minutes_int>`	Type the amount of time in minutes after which an idle administrative session with the web-based manager will be automatically logged out. The valid range is from 1 to 480 minutes (8 hours). To improve security, do not increase the idle timeout.	`480`
`confsync-port <port-number>`	Type the port number the local FortiWeb unit uses to listen for a remote (peer) FortiWeb unit. ***Warning***: The port number must be different than the port number set using config system conf-sync.	8333
`dst {enable | disable}`	Enable to adjust the FortiWeb unit's clock for daylight savings time (DST).	`disable`

Variable	Description	Default
`hostname <host_name>`	Type the host name of this FortiWeb unit. Host names may include US-ASCII letters, numbers, hyphens, and underscores, and may be up to 35 characters in length. Spaces and special characters are not allowed. The host name of the FortiWeb unit is used in several places. • It appears in the *System Information* widget on the *Status* tab of the web-based manager, and in the get router all CLI command. • It is used in the command prompt of the CLI. • It is used as the SNMP system name. For information about SNMP, see "config system snmp sysinfo" on page 154. The *System Information* widget and the get router all 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~#`. **Note:** You can also configure the local domain name. For details, see "config system dns" on page 130.	`FortiWeb`
`ie6workaround {enable | disable}`	Enable to use the work around for a navigation bar freeze issue caused by using the web-based manager with Microsoft Internet Explorer 6.	`disable`
`language {english | japanese | simch | trach}`	Select which language to use when displaying the web-based manager. 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. 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. 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. 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. For more information on language support in the web-based manager and CLI, see "Using the CLI Language support & regular expressions" on page 33. **Note:** This setting does ***not*** affect the display of the CLI.	`english`
`ntpserver {<ntp_fqdn> | <ntp_ipv4>}`	Type the IP address or fully qualified domain name (FQDN) of a Network Time Protocol (NTP) server to query in order to synchronize the FortiWeb unit's clock. For more information about NTP and to find the IP address of an NTP server that you can use, see http://www.ntp.org/.	No default.
`ntpsync {enable | disable}`	Enable to automatically update the system date and time by connecting to a NTP server. Also configure `ntpserver {<ntp_fqdn> | <ntp_ipv4>}, syncinterval <minutes_int>` and `timezone <time-zone-code_str>`.	`disable`
`refresh <seconds_int>`	Type the automatic refresh interval, in seconds, for the web-based manager's *System Status Monitor*. To disable automatic refreshes, type `0`.	`0`

Variable	Description	Default
`single-admin-mode {enable | disable}`	Enable to allow only one administrator account to be logged in at any given time. This option may be useful to prevent administrators from inadvertently overwriting each other's changes. 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. If only one administrator may be logged in at a time, this problem cannot occur. 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.	`disable`
`ssl-md5 {enable/disable}`	If you enable an SSL server in policy for use in reverse proxy mode, use this option to enable or disable MD5 support in all such policies. This option is intended to support older servers and enabling it creates weaker protection.	`disable`
`strong-password {enable | disable}`	Enable to enforce strong password rules for administrator accounts. If the password entered is not strong enough when a new administrator account is created, the FortiWeb unit displays an error and prompts to enter a stronger password. Strong passwords have the following characteristics: • are between 8 and 16 characters in length • contain at least one upper case and one lower case letter • contain at least one numeric • contain at least one non-alphanumeric character	`disable`
`syncinterval <minutes_int>`	Type how often, in minutes, the FortiWeb unit should synchronize its time with the Network Time Protocol (NTP) server. The valid range is from 1 to 1440 minutes. To disable time synchronization, type `0`.	`60`
`timezone <time-zone-code_str>`	Type the two-digit code for the time zone in which the FortiWeb unit is located. The valid range is from `00` to `74`. To display a list of time zone codes, their associated the GMT time zone offset, and contained major cities, type `set timezone ?`.	`00`
`weak_enc {enable | disable}`	If you enable an SSL server in policy for use in reverse proxy mode, use this option to enable or disable SSL v2 support in all such policies. This option is intended to support older servers and enabling it creates weaker protection.	`disable`

Example

This example configures time synchronization with a public NTP server pool. The FortiWeb unit is located in the Pacific Time zone (code `04`) and will synchronize its time with the NTP server pool every 60 minutes.

```
config system global
  set timezone 04
  set ntpserver pool.ntp.org
  set syncinterval 60
  set ntpsync enable
end
```

For an example that includes a host name, see "config system dns" on page 130.

History

FortiWeb v3.2.0	New.
FortiWeb v3.3.1	New option `simch` for field `language`. Allows you to switch the display of the web-based manager between English and simplified Chinese.
FortiWeb v4.0.0	New field `single-admin-mode`. When enabled, allows only one administrator account to be logged in at any given time.
FortiWeb v4.1	Added Japanese and traditional Chinese language support for web-based manager. Added refresh system status monitor refresh interval setting. Added strong administrator password setting. Added `weak-enc`.

Related topics

- config system admin
- config system autoupdate schedule
- config system interface
- config system dns
- config router static
- execute date
- execute time

system ha

Use this command to configure a FortiWeb unit to operate as one of two units in an active-passive high availability (HA) pair. FortiWeb units that are joined as an HA pair enhance availability by causing the backup unit to assume the role of the primary unit if the primary unit fails.

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

- There are two FortiWeb units.
- Both units have identical hardware platforms.
- Both units have identical firmware versions.
- One network port is connected (for best results, directly, using a cross-over Ethernet cable) to the same port number on the other FortiWeb unit in order to carry HA heartbeat and synchronization traffic between members of the HA pair.
- The network topology has redundant paths: if the primary unit fails, physical network cabling and routes must be able to redirect traffic to the secondary (backup) unit

You can have more than one HA pair on the same network as long as pair has a different `group-id`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system ha
  set mode {master | slave | standalone}
  set device <interface_name>
  set device-backup <interface_name>
  set arps <arp_int>
  set arp-interval <seconds_int>
  set group-id <group_int>
  set hb-interval <seconds_int>
  set hb-lost-threshold <seconds_int>
  set monitor {<interface_name> ...}
end
```

Variable	Description	Default
`mode {master | slave | standalone}`	Type one of the following: • `master`: Operate as the primary unit in an HA pair. The FortiWeb unit will form an HA pair with another FortiWeb unit whose `group-id <group_int>` matches, and which is connected to its `device <interface_name>`. • `slave`: Operate as the backup unit in an HA pair. The FortiWeb unit will form an HA pair with another FortiWeb unit whose `group-id <group_int>` matches, and which is connected to its `device-backup <interface_name>`. 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. • `standalone`: Do not operate as a member of an HA pair. Instead, operate as a single, independent FortiWeb unit. When this is the mode, none of the following set statements are available.	`standalone`

Variable	Description	Default
`device <interface_name>`	Type the name of the network interface that the primary unit (master) will use to send HA heartbeat packets to the secondary unit (backup). 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. This setting is available only if `mode` is not `standalone`.	No default.
`device-backup <interface_name>`	Type the name of the network interface that the secondary unit (backup) will use to send HA heartbeat packets to the primary unit (master). It must ***not*** be the same network interface as `device <interface_name>.` This setting is available only if `mode` is not `standalone`.	No default.
`arps <arp_int>`	Type 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-interval <seconds_int>`. The valid range is 1 to 16. 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. This setting is available only if `mode` is not `standalone`.	3
`arp-interval <seconds_int>`	Type the number of seconds to wait between each time that the FortiWeb unit broadcasts ARP packets. The valid range is from 1 to 20. 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. This setting is available only if `mode` is not `standalone`.	1
`group-id <group_int>`	Type 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. Changing the group ID changes the cluster's virtual MAC address. The title bar of your browser window will include the group ID when you are connected to the web-based manager and the FortiWeb unit is operating in HA mode. The valid range is from 0 to 63. This setting is available only if `mode` is not `standalone`.	`0`

Variable	Description	Default
`hb-interval <seconds_int>`	Type 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 valid range is 1 to 20 (that is, between 100 and 2,000 milliseconds). This setting is available only if `mode` is not `standalone`.	1
`hb-lost-threshold <seconds_int>`	Type the number of heartbeat intervals that one of the HA units waits to receive HA heartbeat packets from the other HA unit before assuming that the other unit is no longer responsive, causing a failover. 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 valid range is from 1 to 60 seconds. This setting is available only if `mode` is not `standalone`. **Note:** You can use SNMP traps to notify you when a failover is occurring. For details, see "config system snmp community" on page 150.	1
`monitor {<interface_name> ...}`	Type the name of one or more network interfaces that directly correlates with a physical link in order to monitor for link failure. Separate the name of each network interface with a space. To remove from or add to the list of monitored network interfaces, retype the entire list. 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 occurs. This setting is available only if `mode` is not `standalone`. **Note:** To prevent unintentional failover, do not configure port monitoring ***until*** you have configured HA on both members of the HA pair, and have connected the physical ports to be monitored to the network.	No default.

Example

This example configures a primary unit in an HA cluster. Both the backup and primary unit will send HA heartbeat and synchronization traffic to each other through their port3 network interfaces.

Because in this example the connections that the FortiWeb cluster protects occur through port1 and port2, link failure monitoring is configured for those physical network ports.

Other HA settings use their default values.

```
config system ha
  set mode master
  set group-id 0
  set device port3
  set device-backup port3
  set arps 3
  set arp-interval 1
  set hb-interval 1
  set hb-lost-threshold 1
  set monitor port1 port2
```

```
end
```

History

FortiWeb v3.2.0	New.
FortiWeb v4.0.0	Behavior change. You can now use HA while operating in either of the transparent modes. Additionally, a second failover will no longer be triggered when the failed primary unit is returned to service in the group. Instead, the original primary unit will wait until the current primary unit (originally configured as the backup unit) fails.

Related topics

- config system interface
- config system global

system interface

Use this command to configure:

- the network interfaces associated with the physical network ports of the FortiWeb unit, including administrative access
- VLAN subinterfaces associated with physical network interfaces

Note: You can restrict which IP addresses are permitted to log in as a FortiWeb administrator through the network interfaces. For details, see "config system admin" on page 113.

Note: When the FortiWeb unit is operating in either of the transparent modes, VLANs do not support Cisco discovery protocol (CDP).

You can use SNMP traps to notify you when a network interface's configuration changes. For details, see "config system snmp community" on page 150.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `netgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system interface
  edit <interface_name>
    set status {enable | disable}
    set allowaccess {http https ping snmp ssh telnet}
    set description <comment_str>
    set interface <interface_name>
    set ip <interface_ipv4mask>
    set mode static
    set type {physical | vlan}
    set vlanid <vlan-id_int>
  next
end
```

Variable	Description	Default
`<interface_name>`	Type the name of a network interface.	No default.
`status {enable | disable}`	Enable to bring up the network interface so that it is permitted to receive or transmit traffic.	`enable`

Variable	Description	Default
`allowaccess {http https ping snmp ssh telnet}`	Type the protocols that will be permitted for administrative connections to the network interface. Separate each protocol with a space. To remove from or add to the list of permitted administrative access protocols, retype the entire list. • `ping`: Allow ICMP ping responses from this network interface. • `http`: Allow HTTP access to the web-based manager. **Caution:** HTTP connections are ***not*** secure and can be intercepted by a third party. To reduce risk to the security of your FortiMail unit, enable this option only on network interfaces connected directly to your management computer. • `https`: Allow secure HTTP (HTTPS) access to the web-based manager. • `snmp`: Allow SNMP access. For more information, see "config system snmp community" on page 150. **Note:** This setting only configures which network interface will ***receive*** SNMP queries. To configure which network interface will ***send*** traffic, see "config system snmp community" on page 150. • `ssh`: Allow SSH access to the CLI. • `telnet`: Allow Telnet access to the CLI. **Caution:** Telnet connections are ***not*** secure and can be intercepted by a third party. To reduce risk to the security of your FortiMail unit, enable this option only on network interfaces connected directly to your management computer. **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. Consider allowing ping only when troubleshooting.	`ping https ssh`
`description <comment_str>`	Type a description or other comment. The comment may be up to 63 characters long. If the comment is more than one word, surround the words with quotes (`'`).	No default.
`interface <interface_name>`	Type the name of the network interface with which the VLAN subinterface will be associated. This field is available only if `type` is `vlan`.	No default.
`ip <interface_ipv4mask>`	Type the IP address and netmask of the network interface, 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. The default setting for port1 is `192.168.`***`1`***`.99` with a netmask of 255.255.255.0: other ports have no default.	Varies

Variable	Description	Default
`type {physical | vlan}`	Indicates whether the interface is directly associated with a physical network port, or is instead a VLAN subinterface. This option is set by the system automatically, and cannot be changed. The default varies by whether you are editing a network interface associated with a physical port (`physical`) or creating a new subinterface (`vlan`).	Varies
`vlanid <vlan-id_int>`	Type the VLAN ID of 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 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, 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 either of the transparent modes 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 reverse proxy 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. For the maximum number of interfaces, including VLAN subinterfaces, see Appendix B in the *FortiWeb Administration Guide*. 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. **Note:** Inter-VLAN routing is not supported if the FortiWeb unit is operating in either of the transparent modes. In that case, you must configure the same VLAN IDs on each physical network port.	`0`

Example

This example configures the network interface named port1, associated with the first physical network port, with the IP address and subnet mask 10.0.0.1/24. It also enables ICMP ECHO (ping) and HTTPS administrative access to that network interface, and enables it.

```
config system interface
  edit "port1"
    set ip 10.0.0.1 255.255.255.0
    set allowaccess ping https
    set status up
  next
end
```

Example

This example configures the network subinterface named vlan_100, associated with the physical network interface port1, with the IP address and subnet mask 10.0.1.1/24. It does not allow administrative access.

```
config system interface
  edit "vlan_100"
    set type vlan
```

```
    set ip 10.0.1.1 255.255.255.0
    set status up
    set vlanid 100
    set interface port1
  next
end
```

History

FortiWeb v3.2.0	New.
FortiWeb v4.0.0	New field `interface`. Selects the physical network interface with which a VLAN subinterface is associated. New option `vlan` for field `type`. Selects whether an interface is directly associated with a physical network port, or is a VLAN subinterface associated with a network interface. New field `vlanid`. Configures the ID part of the VLAN tag. New field `speed`. Configures the speed of a physical network link.

Related topics

- config system v-zone
- config router static
- config server-policy vserver
- config system snmp community
- config system admin
- config system ha

system raid

Use this command to configure RAID status. Currently, only RAID level 1 is supported, and only on FortiWeb models 1000B, 1000C,and 3000C shipped with version 4.1 or later. On older units that have been upgrade to version 4.1, the RAID status cannot be activated.

Note: Rebuilding RAID after a disk failure will result in some loss of data in packet logs.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system raid
  set level <raid-level>
end
```

Variable	Description	Default
`<raid-level>`	Type the RAID level. Currently only raid1 is supported.	No default.

Example

This example sets the RAID status to level 1.

```
config system raid
  set level raid1
end
```

History

FortiWeb v4.1 New.

system report-lang

Use this command to modify the name or description of a report language.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system report-lang
  edit <report-language_name>
    set description <comment_str>
  next
end
```

Variable	Description	Default
`<report-language_name>`	Type the name of an existing report language. If no report languages exist, you can download, customize, and upload one using the web-based manager. For details, see the *FortiWeb Administration Guide*.	No default.
`description <comment_str>`	Type a description or other comment. If the comment is more than one word, surround the words with quotes (').	No default.

History

FortiWeb v3.3.0 New.

Related topics

- config log reports

system settings

Use this command to configure the operation mode and gateway of the FortiWeb unit.

The default operation mode is reverse proxy 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 reverse proxy mode and actively begin filtering traffic. Backup your configuration before changing modes. Changing the mode causes the FortiWeb unit to remove policies that are not applicable in the current mode.

FortiWeb units can operate in one of these modes:

- **Reverse Proxy:** Reverse proxy traffic destined for a virtual server's network interface and IP address, forward it to a physical server, and apply the first applicable server policy. The FortiWeb unit logs, blocks, or modifies traffic according to the matching server policy and its protection profile.
- **Offline Protection:** Monitor traffic received on the virtual server's network interface (regardless of the IP address), and apply the first applicable server policy. The FortiWeb unit logs or blocks traffic according to the matching server 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 reverse proxy 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.

- **True Transparent Proxy**: Proxy traffic destined for a physical server's IP address, and apply the first applicable server 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.
- **Transparent Inspection**: Inspect traffic destined for a physical server's IP address, asynchronously capture traffic, and apply the first applicable server 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.) Similar to offline protection mode, actions other than alert cannot be guaranteed to be successful. It is easy to switch between transparent inspection and true transparent proxy without changing your network topology.

Note: 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 network interfaces and virtual servers on the FortiWeb unit, reconfigure policies, and enable or disable SSL on your web servers.

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

You can use SNMP traps to notify you if the operation mode changes. For details, see "config system snmp community" on page 150.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system settings
  set opmode {offline-protection | reverse-proxy | transparent |
     transparent-inspection}
  set stop-monitor {enable | disable}
```

```
  set gateway <gateway_ipv4>
end
```

Variable	Description	Default
`opmode {offline-protection | reverse-proxy | transparent | transparent-inspection}`	Select the operation mode of the FortiWeb unit, either offline-protection, reverse-proxy, transparent or transparent-inspection. If you have not yet adjusted the physical topology to suit the new operation mode, see the *FortiWeb Installation Guide*. You may also need to reconfigure IP addresses, static routes, bridges, policies, and virtual servers, and on your web servers, enable or disable SSL.	`reverse-proxy`
`gateway <gateway_ipv4>`	Set the default gateway. This command applies to either of the transparent modes.	`none`
`stop-monitor {enable | disable}`	Set `enable` to override deny and redirect actions defined in the server protection rules for the selected policy. This enables FortiWeb to log attacks without performing the deny or redirect action, and to collect more information to build an auto learning profile for the attack. Set `disable` to allow attack deny/redirect actions to be performed as defined by the server protection rules.	`disable`

History

FortiWeb v3.2.0	New.
FortiWeb v3.3.0	Behavior change. Changing the operation mode now deletes policies that are not applicable in the current mode. Previously, inapplicable policies were merely ignored.
FortiWeb v3.3.1	New option `transparent`. Enables transparent mode.
FortiWeb v4.0.2	New command `gateway`. Sets the default gateway for transparent mode.
FortiWeb v4.1	Operating mode names changed: • Inline is now reverse proxy • Offline is now offline protection • Transparent is now true transparent proxy New transparent inspection mode added.

Related topics

- config server-policy policy
- config server-policy vserver

system snmp community

Use this command to configure the FortiWeb unit's SNMP agent to belong to an SNMP community, and to select which events will cause the FortiWeb unit to generate SNMP traps.

The FortiWeb unit's simple network management protocol (SNMP) agent allows queries for system information can 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. You can 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.

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 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. Use SNMP traps to notify the SNMP manager of a wide variety of types of events. Event types range from basic system events, such as high usage of resources, to when an attack type is detected or a specific rule is enforced by a policy.

Before you can use SNMP, you must activate the FortiWeb unit's SNMP agent (see "config system snmp sysinfo" on page 154) 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 "config system interface" on page 142.)

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 in the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system snmp community
  edit <community_index>
    set status {enable | disable}
    set name <community_name>
    set events {event_names}
    set query-v1-port <port_number>
    set query-v1-status {enable | disable}
    set query-v2c-port <port_number>
    set query-v2c-status {enable | disable}
    set trap-v1-lport <port_number>
    set trap-v1-rport <port_number>
    set trap-v1-status {enable | disable}
    set trap-v2c-lport <port_number>
    set trap-v2c-rport <port_number>
    set trap-v2c-status {enable | disable}
    config hosts
      edit <snmp-manager_index>
        set interface <interface_name>
        set ip <manager_ipv4>
      next
    end
  next
end
```

Variable	Description	Default
`<community_index>`	Type the index number of a community to which the FortiWeb unit belongs.	No default.
`status {enable | disable}`	Enable to activate the community. This setting takes effect only if the SNMP agent is enabled. For details, see “config system snmp sysinfo” on page 154.	`disable`
`name <community_name>`	Type the name of the SNMP community to which the FortiWeb unit and at least one SNMP manager belongs. 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.	No default.

Variable	Description	Default
`events {event_names}`	Type one or more of the following SNMP event names in order to cause the FortiWeb unit to send traps when those events occur. Traps will be sent to the SNMP managers in this community. Also enable traps. • `cpu-high`: CPU usage has exceeded 80%. • `intf-ip`: A network interface's IP address has changed. See "config system interface" on page 142. • `log-full`: Local log disk space usage has exceeded 80%. If the space is consumed and a new log message is triggered, the FortiWeb unit will either drop it or overwrite the oldest log message, depending on your configuration. See "config log disk" on page 44. • `mem-low`: Memory (RAM) usage has exceeded 80%. • `policy-start`: A policy was enabled. See "config server-policy policy" on page 92. • `policy-stop`: A policy was disabled. See "config server-policy policy" on page 92. • `pserver-failed`: A server health check has determined that a physical server that is a member of a server farm is now unavailable. See "config server-policy policy" on page 92. • `sys-ha-hbfail`: An HA failover is occurring. See "config system ha" on page 138. • `sys-mode-change`: The operation mode was changed. See "config system settings" on page 148. • `waf-access-attack`: FortiWeb enforced a page access rule. See "config waf page-access-rule" on page 200. • `waf-amethod-attack`: FortiWeb enforced an allowed methods restriction. See "config waf web-protection-profile inline-protection" on page 234, "config waf web-protection-profile offline-protection" on page 239, and "config waf allow-method-exceptions" on page 167. • `waf-blogin-attack`: FortiWeb detected a brute force login attack. See "config waf brute-force-login" on page 170. • `waf-disclosure-attack`: FortiWeb prevented a server error or version information disclosure. See "config waf server-protection-rule" on page 212. • `waf-exploit-attack`: FortiWeb detected a common exploit attack. See "config waf server-protection-rule" on page 212. • `waf-hidden-fields`: FortiWeb detected a hidden fields attack. • `waf-pvalid-attack`: FortiWeb enforced an input/parameter validation rule See "config waf parameter-validation-rule" on page 203. • `waf-robot-attack`: FortiWeb enforced a robot control rule See "config waf robot-control" on page 205. • `waf-spage-attack`: FortiWeb enforced a start page rule. See "config waf start-pages" on page 220. • `waf-sql-attack`: FortiWeb detected an SQL injection attack. See "config waf server-protection-rule" on page 212. • `waf-xss-attack`: FortiWeb detected a cross-site scripting (XSS) attack. See "config waf server-protection-rule" on page 212. • `xml-filter-attack`: FortiWeb enforced a filter rule. See "config xml-protection filter-rule" on page 247. • `xml-intrusion-attack`: FortiWeb enforced an intrusion prevention rule. See "config xml-protection intrusion-prevention-rule" on page 250. • `xml-schema-attack`: FortiWeb detected a W3C schema poisoning attack. See ""config xml-protection xml-protection-profile" on page 260. • `xml-sigenc-attack`: XML signature verification or decryption failed. See ""config xml-protection xml-protection-profile" on page 260. • `xml-sql-attack`: FortiWeb detected an SQL injection attack. See "config xml-protection xml-protection-profile" on page 260. • `xml-wsdl-attack`: FortiWeb detected a WSDL scanning attack. See "config xml-protection xml-protection-profile" on page 260.	No default.

Variable	Description	Default
`query-v1-port <port_number>`	Type the TCP port number on which the FortiWeb unit will listen for SNMP v1 queries from the SNMP managers of the community.	`161`
`query-v1-status {enable | disable}`	Enable to respond to queries using the SNMP v1 version of the SNMP protocol.	`enable`
`query-v2c-port <port_number>`	Type the TCP port number on which the FortiWeb unit will listen for SNMP v2c queries from the SNMP managers of the community.	`161`
`query-v2c-status {enable | disable}`	Enable to respond to queries using the SNMP v2c version of the SNMP protocol.	`enable`
`trap-v1-lport <port_number>`	Type the TCP port number that will be the source (also called “local") port number for SNMP v1 trap packets.	`162`
`trap-v1-rport <port_number>`	Type the TCP port number that will be the destination (also called “remote") port number for SNMP v1 trap packets.	`162`
`trap-v1-status {enable | disable}`	Enable to send traps using the SNMP v1 version of the SNMP protocol.	`enable`
`trap-v2c-lport <port_number>`	Type the TCP port number that will be the source (also called “local") port number for SNMP v2c trap packets.	`162`
`trap-v2c-rport <port_number>`	Type the TCP port number that will be the destination (also called “remote") port number for SNMP v2c trap packets.	`162`
`trap-v2c-status {enable | disable}`	Enable to send traps using the SNMP v2c version of the SNMP protocol.	`enable`
`<snmp-manager_index>`	Type the index number of an SNMP manager for the community.	No default.
`interface <interface_name>`	Type the name of the network interface from which the FortiWeb unit will send traps and reply to queries. **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. **Note:** This setting only applies to the interface ***sending*** SNMP traffic. To configure the receiving interface, see config system interface.	No default.
`ip <manager_ipv4>`	Type the IP address of the SNMP manager that, if traps and/or queries are enabled in this community: • will receive traps from the FortiWeb unit • will be permitted to query the FortiWeb unit SNMP managers have read-only access. To allow any IP address using this SNMP community name to query the FortiWeb unit, enter `0.0.0.0`. **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.	No default.

Example

For an example, see “config system snmp sysinfo” on page 154.

History

FortiWeb v3.2.0 New.

Related topics

- config system snmp sysinfo
- config system interface
- config server-policy policy

system snmp sysinfo

Use this command to enable and configure basic information for the FortiWeb unit's SNMP agent.

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 (see "config system snmp community" on page 150). You must also enable SNMP access on the network interface through which the SNMP manager will connect. (See ""config system interface" on page 142.)

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 in the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system snmp sysinfo
  set contact-info <contact_str>
  set description <description_str>
  set location <location_str>
  set status {enable | disable}
end
```

Variable	Description	Default
`contact-info <contact_str>`	Type 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 (_).	No default.
`description <description_str>`	Type a description of the FortiWeb unit up to 35 characters long. The string can contain only letters (a-z, A-Z), numbers, hyphens (-) and underscores (_).	No default.
`location <location_str>`	Type the physical location of the FortiWeb unit up to 35 characters long. The string can contain only letters (a-z, A-Z), numbers, hyphens (-) and underscores (_).	No default.
`status {enable | disable}`	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. This setting enables queries only if SNMP administrative access is enabled on one or more network interfaces. For details, see "config system interface" on page 142.	`disable`

Example

This example enables the SNMP agent, configures it to belong to a community named public whose SNMP manager is 172.168.1.20. The SNMP manager is not directly attached, but can be reached through the network interface named port3.

This example also configures the SNMP agent to send traps using SNMP v2c for high CPU or memory usage, and when the primary unit fails; it also enables responses to SNMP v2c queries through the network interface named port3 (along with the previously enabled administrative access protocols, ICMP ping, HTTPS, and SSH).

```
config system snmp sysinfo
  set contact-info 'admin_example_com'
  set description 'FortiWeb-1000B'
  set location 'Rack_2'
```

```
    set status enable
  end
  config system snmp community
    edit 1
      set status enable
      set name public
      set events {cpu-high mem-low sys-ha-hbfail}
      set query-v1-status disable
      set query-v2c-port 161
      set query-v2c-status enable
      set trap-v1-status disable
      set trap-v2c-lport 162
      set trap-v2c-rport 162
      set trap-v2c-status enable
      config hosts
        edit 1
          set interface port3
          set ip 172.168.1.20
        next
      end
    next
  end
  config system interface
    edit port3
      set allowaccess ping https ssh snmp
    next
  end
```

History

FortiWeb v3.2.0 New.

Related topics

- config system snmp community
- config system interface
- config router static

system v-zone

Use this command to configure bridged network interfaces.

Bridges are used when the FortiWeb unit is operating in true transparent proxy or transparent inspection mode and you want to deploy FortiWeb 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. Bridges 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. If you prefer to do so manually, disable STP using `stp <enable | disable>`.

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 perform network switching at Layer 2 of the OSI model. However, if you require the ability to use an IP address for ICMP ECHO requests (ping) to test connectivity with the physical ports comprising the bridge, you can assign an IP address to the bridge using `ip <ping_ipv4mask>` and thereby create a virtual network interface that will respond.

Note: Depending on the status, such as *forwarding* or *blocked,* each port in the bridge may or may not be immediately functional. To view the status of each port, use the web-based manager. For details, see the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `netgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config system v-zone
  edit <bridge_name>
    set interfaces <interface_list>
    set ip <ping_ipv4mask>
    set stp <enable | disable>
  next
end
```

Variable	Description	Default
`<bridge_name>`	Type the IP address or fully qualified domain name (FQDN) of an SMTP relay that the FortiWeb unit can use to send alert email.	No default.
`interfaces <interface_list>`	Type the names of two or more 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. Separate each name with a space.	No default.
`ip <ping_ipv4mask>`	Create a virtual network interface that can respond to ICMP ECHO (ping) requests, enter an IP address/subnet mask for the virtual network interface.	No default.
`stp <enable | disable>`	Enable to use spanning-tree protocol (STP) so that the bridge can automatically prevent Layer 2 loops and enable or disable redundant interfaces in the event of switch failover.	`enable`

Example

This example configures a true bridge between port3 and port4. Spanning-tree protocol is enabled by default. The bridge has no virtual network interface, and so it cannot respond to pings.

```
config system v-zone
  edit bridge1
    set interfaces port3 port4
  next
end
```

History

FortiWeb v3.3.1	New.
FortiWeb v3.3.2	Added field `stp`. Enables or disables spanning-tree protocol (STP) for the bridge.
FortiWeb v4.0.0	Renamed command from `config system bridge` to `config system v-zone`.

Related topics

- config system interface
- config system settings

user ldap-user

Use this command to configure user accounts that will authenticate with the FortiWeb unit via an LDAP server.

LDAP user queries are used by the HTTP authentication feature to authorize HTTP requests. For details, see the *FortiWeb Administration Guide*.

To incorporate LDAP user accounts, select 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 used for web protection. For details, see "config user user-group" on page 163.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config user ldap-user
  edit <ldap-query_name>
    set bind-type {anonymous | simple | regular}
    set common-name-id <cn-attribute_str>
    set distinguished-name <search-dn_str>
    set password <bind-password_str>
    set port <port_number>
    set protocol {ldaps | starttls}
    set server <ldap_ipv4>
    set ssl-connection {enable | disable}
    set username <bind-dn_str>
  next
end
```

Variable	Description	Default
`<ldap-query_name>`	Type the name of the LDAP user query.	No default.
`bind-type {anonymous | simple | regular}`	Select one of the following LDAP query binding styles: • `simple`: Bind using the client-supplied password and a bind DN assembled from the `common-name-id <cn-attribute_str>`, `distinguished-name <search-dn_str>`, and the client-supplied user name. • `regular`: Bind using a bind DN and password that you configure in `username <bind-dn_str>` and `password <bind-password_str>`. • `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.	`simple`
`common-name-id <cn-attribute_str>`	Type the identifier, often `cn`, for the common name (CN) attribute whose value is the user name. Identifiers may vary by your LDAP directory's schema.	`cn`
`distinguished-name <search-dn_str>`	Type the distinguished name (DN) that, when prefixed with the common name, forms the full path in the directory to user account objects.	No default.
`password <bind-password_str>`	Type the password of the `username <bind-dn_str>`. 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`.	No default.
`port <port_number>`	Type the port number where the LDAP server listens. The default port number varies by your selection in `ssl-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.	`0`

Variable	Description	Default
`protocol {ldaps | starttls}`	Select whether to secure the LDAP query using LDAPS or STARTTLS. You may need to reconfigure `port <port_number>` to correspond to the change in protocol. This field is applicable only if `ssl-connection` is `enable`.	`ldaps`
`server <ldap_ipv4>`	Type the IP address of the LDAP server.	No default.
`ssl-connection {enable | disable}`	Enable to connect to the LDAP server(s) using an encrypted connection, then select the style of the encryption in `protocol`.	`disable`
`username <bind-dn_str>`	Type the bind DN, such as `cn=FortiWebA,dc=example,dc=com`, of an LDAP user account with permissions to query the `distinguished-name <search-dn_str>`. 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`.	No default.

Example

This example configures an LDAP user query to the server at 172.16.1.100 on port 389. SSL and TLS are disabled. To bind the query, the FortiWeb unit will use the bind DN `cn=Manager,dc=example,dc=com`, whose password is `mySecretPassword`. Once connected and bound, the query for search for user objects in `ou=People,dc=example,dc=com`, comparing the user name supplied by the HTTP client to the value of each object's `cn` attribute.

```
config user ldap-user
  edit "ldap-user1"
    set server "172.16.1.100"
    set ssl-connection disable
    set port 389
    set common-name-id "cn"
    set distinguished-name "ou=People,dc=example,dc=com"
    set bind-type regular
    set username "cn=Manager,dc=example,dc=com"
    set password "mySecretPassword"
  next
end
```

History

FortiWeb v4.0.0	New.
FortiWeb v4.1	Removed certificate `<ca-certificate_name>`

Related topics

- config user user-group

user local-user

Use this command to configure locally defined user accounts.

Local user accounts are used by the HTTP authentication feature to authorize HTTP requests. For details, see the *FortiWeb Administration Guide*.

To incorporate local user accounts, add them to a user group that is selected within an authentication rule, which is in turn selected within an authentication policy. For details, see "config user user-group" on page 163.

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 use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config user local-user
  edit <local-user_name>
    set username <user_str>
    set password <password_str>
  next
end
```

Variable	Description	Default
`<local-user_name>`	Type the name of the local user account.	No default.
`username <user_str>`	Type the name that the user must provide when authenticating.	No default.
`password <password_str>`	Type the password for the local user account. The maximum length is 63 characters.	No default.

Example

This example configures a local user account that can be used for HTTP authentication.

```
config user local-user
  edit "local-user1"
    set username "user1"
    set password "myPassword"
  next
end
```

History

FortiWeb v4.0.0 New.

Related topics

- config user user-group

user ntlm-user

Use this command to configure user accounts that will authenticate with the FortiWeb unit via an NT LAN Manager (NTLM) server.

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 details, see the *FortiWeb Administration Guide*.

To incorporate NTLM user account queries, add them to a user group that is selected within an authentication rule, which is in turn selected within an authentication policy. For details, see "config user user-group" on page 163.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config user ntlm-user
  edit <ntlm-query_name>
    set port <port_number>
    set server <ntlm_ipv4>
  next
end
```

Variable	Description	Default
`<ntlm-query_name>`	Type the name of the NTLM user query.	No default.
`port <port_number>`	Type the port number where the NTLM server listens.	`0`
`server <ntlm_ipv4>`	Type the IP address of the NTLM server.	No default.

Example

This example configures an NTLM query connection to a server at 172.16.1.101 on port 445.

```
config user ntlm-user
  edit "ntlm-user1"
    set server "172.16.1.101"
    set port 445
  next
end
```

History

FortiWeb v4.0.0 New.

Related topics

- config user user-group

user radius-user

Use this command to modify RADIUS queries used to authenticate users.

To authenticate a user, the FortiWeb unit sends the user's credentials to RADIUS for authentication. If RADIUS authentication succeeds, the user is successfully authenticated with the unit. If RADIUS authentication fails, the unit refuses the connection. To override the default authentication scheme, select a specific authentication protocol or change the default RADIUS port.

To incorporate RADIUS users, theymust be in a user group selected within an authentication rule, which is in turn selected within an authentication policy. For details, see "config user user-group" on page 163.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config user radius-user
  edit <radius-query_name>
    set secret <password_str>
    set server <radius-ipv4>
    set server-port <port_number>
    set auth-type {default | chap | ms_chap | ms_chap_v2 | pap}
    set nas-ip <ipv4>
    set secondary-secret <password_str>
    set secondary-server <radius2-ipv4>
    set secondary-server-port <port_number>
  next
end
```

Variable	Description	Default
`<radius-query_name>`	Type the name of the RADIUS user query.	No default.
`secret <password_str>`	Enter the RADIUS server secret key for the primary RADIUS server. The primary server secret key should be a maximum of 16 characters in length	No default.
`server <radius-ipv4>`	Type the IP address of the RADIUS server to query for users.	`0.0.0.0`
`server-port <port_number>`	Type the port number where the RADIUS server listens.	`1812`
`auth-type {default | chap | ms_chap | ms_chap_v2 | pap}`	Type the authentication method. The `default` option uses PAP, MS-CHAP-V2, and CHAP, in that order.	`default`
`nas-ip <ipv4>`	Enter the NAS IP address and called station ID (see RFC 2548 Microsoft Vendor-specific RADIUS Attributes). If you do not enter an IP address, the IP address that the Fortinet interface uses to communicate with the RADIUS server is applied.	`0.0.0.0`
`secondary-secret <password_str>`	Enter the RADIUS server secret key for the secondary RADIUS server. The secondary server secret key should be a maximum of 16 characters in length.	No default.
`secondary-server <radius2-ipv4>`	Type the IP address of the secondary RADIUS server.	No default.
`secondary-server-port <port_number>`	Type the port number where the secondary RADIUS server listens.	`1812`

History

FortiWeb v4.2 New.

user user-group

Use this command to configure user groups.

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

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 "config user local-user" on page 160, "config user ldap-user" on page 158, "config user radius-user" on page 162 and "config user ntlm-user" on page 161.

To apply user groups, select them in within an authentication rule, which is in turn selected within an authentication policy, which is ultimately selected within an inline protection profile used for web protection. For details, see "config waf http-authen http-authen-rule" on page 185.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config user user-group
  edit <user-group_name>
    config members
      edit <entry_index>
        set name <user_name>
        set type {ldap | local | ntlm | radius}
      next
    end
  next
end
```

Variable	Description	Default
`<user-group_name>`	Type the name of the user group.	No default.
`<entry_index>`	Type the index number of the individual entry in the list.	No default.
`name <user_name>`	Select the name of a local user account, LDAP user query, RADIUS user query, or NTLM user query.	No default.
`type {ldap | local | ntlm | radius}`	Select which type of user or user query that you want to add to the group. **Note:** You can mix all user types in the group. However, if the authentication rule's `authen-type` does not support a given user type, all user accounts of that type will be ignored, effectively disabling them.	`local`

Example

For an example, see "config waf http-authen http-authen-policy" on page 183.

History

FortiWeb v4.0.0 New.

Related topics

- config user ldap-user
- config user local-user
- config user ntlm-user
- config waf http-authen http-authen-rule

wad website

Use this command to enable and configure web site defacement attack detection and automatic repair.

The FortiWeb unit monitors the web site's files for any changes and folder modifications at specified time intervals. If it detects a change that could indicate a defacement attack, the FortiWeb unit will notify you, and can quickly react by automatically restoring the web site contents to the previous backup revision.

Web site files will be backed up automatically and a revision will be created on the FortiWeb unit 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.
- If the FortiWeb unit could not successfully connect during a monitor interval, it will create a new revision the next time it re-establishes the connection.

Caution: When you intentionally modify the web site, you must disable the `monitor` option; otherwise, the FortiWeb unit sees your changes as a defacement attempt and undoes them.

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 `backup-max-fsize <limit_int>` and `backup-skip-ftype <extensions_str>`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wadgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config wad website
  edit <entry_index>
    set alert-email <recipient_email>
    set auto-restore {enable | disable}
    set backup-max-fsize <limit_int>
    set backup-skip-ftype <extensions_str>
    set connect-type {ftp | smb | ssh}
    set description <comment_str>
    set hostname-ip {<host_ipv4> | <host_fqdn>}
    set interval-other <seconds_int>
    set interval-root <seconds_int>
    set monitor {enable | disable}
    set monitor-depth <folders_int>
    set name <name_str>
    set password <password_str>
    set port <port_number>
    set share-name <share_str>
    set user <username_str>
    set web-folder <path_str>
  next
end
```

Variable	Description	Default
`<entry_index>`	Type the index number of the individual entry in the list.	No default.
`alert-email <recipient_email>`	Type the recipient email address (`MAIL TO:`) to which the FortiWeb unit will send an email when it detects that the web site changed.	No default.

Variable	Description	Default
`auto-restore {enable | disable}`	Enable to automatically restore the web site to the previous revision number when it detects that the web site changed. 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. **Note**: When you intentionally modify the web site, you must turn off this option; otherwise, the FortiWeb unit will detect your changes as a defacement attempt, and undo them.	`disable`
`backup-max-fsize <limit_int>`	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. **Note:** Backing up large files can impact performance.	`10240`
`backup-skip-ftype <extensions_str>`	Type zero or more file extensions, such as `iso, avi`, to exclude from the web site backup. Separate each file extension with a comma. **Note:** Backing up large files, such as video and audio, can impact performance.	No default.
`connect-type {ftp | smb | ssh}`	Select which protocol to use when connecting to the web site in order to monitor its contents and download web site backups. For Microsoft Windows-style shares, enter `smb`.	`ftp`
`description <comment_str>`	Type a description or other comment. If the comment is more than one word, surround the comment with quotes (`'`).	No default.
`hostname-ip {<host_ipv4> | <host_fqdn>}`	Type the IP address or fully qualified domain name (FQDN) of the physical server on which the web site is hosted. 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.	No default.
`interval-other <seconds_int>`	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 the web site's subfolders to see if any files have been changed by comparing the files with the latest backup. If any file change is detected, the FortiWeb unit will download a new backup revision. If you have enabled `auto-restore {enable | disable}`, the FortiWeb unit will revert the files to their previous version.	`600`
`interval-root <seconds_int>`	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 `web-folder <path_str>` (but ***not*** its subfolders) to see if any files have been changed by comparing the files with the latest backup. If any file change is detected, the FortiWeb unit will download a new backup revision. If you have enabled `auto-restore {enable | disable}`, the FortiWeb unit will revert the files to their previous version.	`60`
`monitor {enable | disable}`	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.	`disable`
`monitor-depth <folders_int>`	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.	`5`
`name <name_str>`	Type a name for the web site. 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.	No default.
`password <password_str>`	Enter the password for the user name you entered in `user <username_str>`	No default.

Variable	Description	Default
`port <port_number>`	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. This is applicable only if `connect-type` is `ftp` or `ssh`.	21
`share-name <share_str>`	Type the name of the shared folder on the web server. This variable appears only if `connect-type` is `smb`.	No default.
`user <username_str>`	Enter the user name that the FortiWeb unit will use to log in to the web site's physical server.	No default.
`web-folder <path_str>`	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 <username_str>`.	No default.

```
config wad website
    edit 1
        set alert-email "admin@example.com"
        set connect-type ssh
        set hostname-ip "192.168.1.10"
        set monitor enable
        set name "www.example.com"
        set password ENC
0MuYCabMHHnEZNUklkz5I0sfqa6HXW421Ne7TbA0zMSB31/4jp/zvuBWSlMZlm776cKrDKpR15wO1K
dkJojSFN0dXKXrZmKwpG53QvkGRtXdf+xc
        set port 22
        set user "fortiweb"
        set web-folder "public_html"
    next
end
```

History

FortiWeb v3.3.2 New.

Related topics

- config system interface
- config router static

waf allow-method-exceptions

Use this command to configure the FortiWeb unit with combinations of URLs and host names, which are exceptions to HTTP request methods that are generally allowed or denied according to the inline or offline protection profile.

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 configure allowed method exceptions. They allow you to specify exceptions to the generally allowed request methods.

To apply allowed method exceptions, select them within an inline or offline protection profile. For details, see "config waf web-protection-profile inline-protection" on page 234 or "config waf web-protection-profile offline-protection" on page 239.

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 "config server-policy allow-hosts" on page 71.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config waf allow-method-exceptions
  edit <method-exception_name>
    config allow-method-exception-list
      edit <entry_index>
        set allow-request <request-methods>
        set host <allowed-hosts_name>
        set host-status {enable | disable}
        set request-file <url_str>
        set request-type {plain | regular}
      next
    end
  next
end
```

Variable	Description	Default
`<method-exception_name>`	Type the name of the exception to allowed HTTP request methods.	No default.
`<entry_index>`	Type the index number of the individual entry in the list.	No default.
`allow-request <request-methods>`	Type one or more of the allowed HTTP request methods that are an exception for that combination of URL and host. Choices include: `connect`, `delete`, `get`, `head`, `options`, `others`, `post`, `put`, and `trace`.	No default.
`host <allowed-hosts_name>`	Type the name of 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. This setting is used only if `host-status` is `enable`.	No default.
`host-status {enable | disable}`	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 <allowed-hosts_name>`.	`disable`

Variable	Description	Default
`request-file <url_str>`	Depending on your selection in `request-type {plain | regular}`, either: • Type 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 (/). • Type 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`. 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. Do not include the name of the web host, such as `www.example.com`, which is configured separately in `host <allowed-hosts_name>`. **Note:** Regular expressions beginning with an exclamation point (`!`) are not supported. For information on language and regular expression matching, see the *FortiWeb Administration Guide*.	No default.
`request-type {plain | regular}`	Select whether `request-file <url_str>` is a literal URL (`plain`) or a regular expression (`regular`).	`plain`

Example

This example adds an exception to the list of allowed methods (`post`) that can be used in HTTP requests. In addition to the allowed methods already specified in protection profiles that use this exception, web hosts included in the protected hosts group named `example_com_hosts` (such as example.com, www.example.com, and 192.168.1.10) are allowed to receive POST requests to the Perl file that handles the guestbook.

```
config waf allow-method-exceptions
  edit "auto-learn-profile2"
    config allow-method-exception-list
      edit 1
        set allow-request post
        set host "example_com_hosts"
        set host-status enable
        set request-file "/perl/guesbook.pl"
        set request-type plain
      next
    end
  next
end
```

History

FortiWeb v3.2.0 New.

FortiWeb v3.3.0 Renamed the `allow-request` option `track` to `trace`. New option `put`. Field `request-file` now accepts regular expressions that do not begin with a slash (/) character.

Related topics

- config server-policy allow-hosts
- config waf web-protection-profile inline-protection
- config waf web-protection-profile offline-protection

waf allow-method-policy

Use this command to build specific combinations of allowed HTTP request methods.

Too define specific exceptions to those combinations use config waf allow-method-exceptions.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config waf allow-method-policy
  edit <method-allow_name>
    set allow-method <request-methods>
    set severity {High | Medium | Low}
    set triggered-action <trigger-policy_name>
    set allow-method-exception <method-exception_name>
  next
end
```

Variable	Description	Default
`<method-allow_name>`	Type the name of a new or existing allow method policy. 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.	No default.
`allow-method <request-methods>`	Type one or more HTTP request methods that you want to allow for this specific policy: `connect`, `delete`, `get`, `head`, `options`, `others`, `post`, `put`, and `trace`.	No default.
`severity {High | Medium | Low}`	Enter the severity level you want FortiWeb to use in the records and reports generated when a violation of the HTTP request method policy occurs.	`Low`
`triggered-action <trigger-policy_name>`	Type the name of the trigger policy you want FortiWeb to apply when a violation of the HTTP request method policy occurs. Trigger policies determine who will be notified by email when the policy violation occurs, and whether the log message associated with the violation are recorded.	No default.
`allow-method-exception <method-exception_name>`	Enter the name of an existing HTTP request method exception to apply to the policy.	No default.

Example

```
config waf allow-method-policy
  edit "allowpolicy1"
    set allow-method get post
    set triggered-action "TriggerActionPolicy1"
    set allow-method-exception "MethodExceptions1"
  next
end
```

History

FortiWeb v4.2. New.

Related topics

- config waf allow-method-exceptions

waf brute-force-login

Use this command to configure 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.

To apply a brute force login attack sensor, select it within an inline protection profile. For details, see "config waf web-protection-profile inline-protection" on page 234.

You can use SNMP traps to notify you when a brute force login attack is detected. For details, see "config system snmp community" on page 150.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config waf brute-force-login
  edit <brute-force-login_name>
    set severity {High | Medium | Low}
    set trigger <trigger-policy_name>
    config login-page-list
      edit <entry_index>
        set access-limit-standalone-ip <rate_int>
        set access-limit-share-ip <rate_int>
        set block-period <seconds_int>
        set host <allowed-hosts_name>
        set host-status {enable | disable}
        set request-file <url_str>
      next
    end
  next
end
```

Variable	Description	Default
`<brute-force-login_name>`	Type the name of the brute force login attack sensor.	No default.
`severity {High | Medium | Low}`	Type the severity level you want FortiWeb to use in the records and reports generated when a violation of the brute force login profile occurs.	`High`
`trigger <trigger-policy_name>`	Type the name of the policy you want FortiWeb to apply when a violation occurs. Trigger policies determine who will be notified by email when the policy violation occurs, and whether the log message associated with the violation are recorded.	No default.
`access-limit-standalone-ip <rate_int>`	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 `block-period <seconds_int>`. To disable the rate limit, type `0`.	No default.

Variable	Description	Default
access-limit-share-ip <rate_int>	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 <seconds_int>. To disable the rate limit, type 0. **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 access-limit-share-ip <rate_int>.	No default.
block-period <seconds_int>	Type the length of time for which the FortiWeb unit will block additional requests after a source IP address exceeds a rate threshold. The block period is shared by all clients whose traffic originate from the source IP address.	No default.
<entry_index>	Type the index number of the individual entry in the list.	No default.
host <allowed-hosts_name>	Type the name of 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. This setting is applied only if host-status is enable.	No default.
host-status {enable | disable}	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 <allowed-hosts_name>.	disable
request-file <url_str>	Type the URL that the HTTP request must match to be included in the brute force login attack sensor's rate calculations. 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 host <allowed-hosts_name>.	No default.

Example

This example limits IP addresses of individual HTTP clients to 3 requests per second, and NAT IP addresses to 20 requests per second, when they request the file login.php on the host www.example.com on TCP port 8080.

```
config waf brute-force-login
  edit "brute_force_attack_sensor"
    set access-limit-share-ip 20
    set access-limit-standalone-ip 3
    set block-period 5
    config login-page-list
      edit 1
        set host "www.example.com:8080"
        set host-status enable
        set request-file "/login.php"
      next
    end
  next
end
```

History

FortiWeb v3.2.0 New.

FortiWeb v4.2 Set statements severity and trigger added.

Related topics

- config waf web-protection-profile inline-protection
- config system snmp community

waf custom-protection-group

Use this command to configure custom protection groups.

Custom protection groups let you associate custom protection rules with a server protection rule.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config waf custom-protection-group
  edit <custom-protection group_name>
    config type-list
      edit <entry_index>
        set custom-protection-rule <rule_name>
      next
    end
  next
end
```

Variable	Description	Default
`<custom-protection group_name>`	Type the name of the custom protection group.	No default.
`<entry_index>`	Type the index number of a protection group to configure.	No default.
`custom-protection-rule <rule_name>`	Enter the name of the custom protection rule to associate with the custom protection group	No default.

Example

This example associates `custom protection rule 1` and `custom protection rule 3` with `Custom Protection group 1`.

```
config waf custom-protection-group
  edit "Custom Protection group 1"
    config type-list
      edit 1
          set custom-protection-rule "custom protection rule 3"
        next
        edit 3
          set custom-protection-rule "custom protection rule 1"
        next
      end
  next
end
```

History

FortiWeb v4.1 New.

Related topics

- config waf server-protection-rule
- config waf custom-protection-rule

waf custom-protection-rule

Use this command to configure custom protection rules.

Custom protection rules let you create custom signatures and custom data leakage expressions, which you can associate with custom protection groups and server protection rules.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config waf custom-protection-rule
  edit <custom-protection rule_name>
    set type {data-leakage | signature-creation}
    set action {alert | alert_deny | redirect}
    set check-count <count_int>
    set case-sensitive {enable | disable}
    set expression <exp_string>
    set severity {High | Medium | Low}
    set trigger <trigger-policy_name>
      next
    end
  next
end
```

Variable	Description	Default
`<custom-protection rule_name>`	Type the name of the custom protection rule.	No default.
`type {data-leakage | signature-creation}`	Select the type of data that the rule applies to: signature creation or data leakage.	No default.
`action {alert | alert_deny | redirect}`	Select the specific action to be taken in situations where data matches the criteria established by this rule.	`alert`
`check-count <count_int>`	Displayed only if the data leakage rule is selected. Type the threshold for the number of data leakage reports before triggering the action specified for this rule.	0
`case-sensitive {enable | disable}`	Select to specify that case sensitivity is used for rule checking.	`disable`
`expression <exp_string>`	Enter the string of text that defines the type of data the rule will check.	No default
`severity {High | Medium | Low}`	Type the severity level you want FortiWeb to use in the records and reports generated when a violation of the rule occurs.	`Medium`
`trigger <trigger-policy_name>`	Type the name of the policy you want FortiWeb to apply when a violation occurs. Trigger policies determine who will be notified by email when the policy violation occurs, and whether the log message associated with the violation are recorded.	No default.

Example

This example

```
config waf custom-protection-rule
  edit "Custom protection rule 1"
    set type data-leakage
```

```
    set expression "myURL"
    set action alert
  next
end
```

History

FortiWeb v4.1	New.
FortiWeb v4.2	Set statements `severity` and `trigger` added.

Related topics

- config waf custom-protection-group

waf file-upload-restriction-policy

Use this command to set the file upload restriction policies that the FortiWeb unit uses to limit the types of files that can be uploaded to your web servers.

The policies are composed of individual rules set using the config waf file-upload-restriction-rule command. Each rule identifies the host and/or URL to which the restriction applies and the types of files allowed. To apply a file upload restriction policy, select it within an inline or offline protection profile.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config waf file-upload-restriction-policy
  edit <file_upload_restriction_policy_name>
    set action {alert | alert_deny}
    set severity {High | Medium | Low}
    set trigger <trigger_policy_name>
      config rule
        edit <entry_index>
          set file-upload-restriction rule <rule_name>
          next
        end
  next
end
```

Variable	Description	Default
`<file_upload_restriction_policy_name>`	Type the name of an existing or new file upload restriction policy.	No default.
`action {alert | alert_deny}`	Type the action you want FortiWeb to perform when the policy is violated: • `alert`: Accept the file upload and generate an alert and/or log message. • `alert_deny`: Block the file upload and generate an alert and/or log message.	`alert`
`severity {High | Medium | Low}`	Type the severity level you want FortiWeb to use in the records and reports generated when the specified policy is violated: one of: `Low`, `Medium`, or `High`.	`Low`
`trigger <trigger_policy_name>`	Select the trigger policy you want FortiWeb to apply when the specified policy is violated. Trigger policies determine who will be notified by email when the policy is violated, and whether the log message associated with the violation is recorded in Syslog or FortiAnalyzer.	No default.
`<entry_index>`	Type the index number of the individual entry in the list.	No default.
`file-upload-restriction rule <rule_name>`	Type the name of an existing file upload restriction rule.	No default.

History

FortiWeb v4.2 New.

Related topics

- waf file-upload-restriction-rule

waf file-upload-restriction-rule

Use this command to define the specific host and request URL for which file upload restrictions apply, and define the specific file types that can be uploaded to that host or URL. These rules are used by a file upload restriction policy. Set the policy using the waf file-upload-restriction-policy command.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config waf file-upload-restriction-rule
  edit <file_upload_restriction_rule_name>
    set host-status {enable | disable}
    set host {ipv4> | <fqdn>}
    set request-file <request_url>
      config file-types
        edit <entry_index>
          set file-type-id <file_id>
          set file-type_name <file_name>
        next
      end
    next
  end
```

Variable	Description	Default
`<file_upload_restriction_rule_name>`	Type the name of an existing or new file upload restriction rule.	No default.
`host-status {enable | disable}`	Enter `enable` to apply this file upload restriction rule only to HTTP requests for specific web hosts, as configured by `host`. Enter `disable` to match the file upload restriction rule based upon the other criteria, such as the URL, but regardless of the `host` setting.	`disable`
`host {ipv4> | <fqdn>}`	Enter the IP address or fully qualified domain name (FQDN) of a protected host.	No default.
`request-file <request_url>`	Enter the literal URL, such as `/fileupload`, to which the file upload restriction applies. The URL must begin with a slash (/). Do not include the name of the host, such as `www.example.com`, which is configured separately using `host`.	No default.
`<entry_index>`	Type the index number of the individual entry in the list. Each entry in the list can define one file type.	No default.

Variable	Description	Default
`file-type-id <file_id>`	Type one numeric type ID that corresponds to the file type: • 00001 (GIF) • 00002 (JPG) • 00003 (PDF) • 00004 (XML) • 00005 (MP3) • 00006 (MIDI) • 00007 (WAVE • 00008 (FLV for a Macromedia Flash Video) • 00009 (RAR) • 00010 (ZIP) • 00011 (BMP) • 00012 (RM for RealMedia) • 00013 (MPEG for MPEG v) • 00014 (3GPP)	No default.
`file-type_name <file_name>`	Enter one file type to be allowed for uploading: GIF, JPG, PDF, XML, MP3, MIDI ,WAVE, FLV, RAR, ZIP, BMP, RM, MPEG, 3GPP.	No default.

Example

```
config waf file-upload-restriction-rule
  edit file-upload-rule1
    set host-status enable
    set host 172.20.120.48
    set request-file /file-uploads
    config file-types
      edit 1
        set file-type-id 00013
        set file-type-name MPEG
      next
      edit 2
        set file-type-id 00008
        set file-type-name FLV
      next
    end
  next
end
```

History

FortiWeb v4.2 New.

Related topics

- waf file-upload-restriction-policy

waf hidden-fields-protection

Use this command to configure groups of hidden field rules.

To apply hidden field rule groups, select them within an inline protection profile. For details, see “config waf web-protection-profile inline-protection” on page 234.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see “Permissions” on page 29.

Syntax

```
config waf hidden-fields-protection
  edit <hidden-field-group_name>
    config hidden_fields_list
      edit <entry_index>
        set hidden-field-rule <hidden-field-rule_name>
      next
    end
  next
end
```

Variable	Description	Default
`<hidden-field-group_name>`	Type the name of the hidden field rule group.	No default.
`<entry_index>`	Type the index number of the individual entry in the list.	No default.
`hidden-field-rule <hidden-field-rule_name>`	Type the name of an existing hidden field rule to add to the group.	No default.

History

FortiWeb v3.3.0 New.

Related topics

- config waf hidden-fields-rule
- config waf web-protection-profile inline-protection

waf hidden-fields-rule

Use this command to configure 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 for users to unintentionally modify, and are often incorrectly perceived as relatively safe by web site owners.

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. The FortiWeb unit caches the values of a session's hidden inputs as they pass to the HTTP client, and verifies that they remain unchanged when the HTTP client submits a form.

You apply hidden field constraints by first grouping them into a hidden field group. For details, see "config waf hidden-fields-protection" on page 179.

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 "config server-policy allow-hosts" on page 71.

Tip: Alternatively, you could use the web-based manager to fetch the request URL from the server and scan it for hidden inputs, using the results to configure the hidden input rule. For details, see the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config waf hidden-field-rule
  edit <hidden-field-rule_name>
    set action {alert | alert_deny | redirect | send_403_forbidden}
    set host <allowed-hosts_name>
    set host-status {enable | disable}
    set request-file <url_str>
    set action-url0 <url_str>
    set action-url1 <url_str>
    set action-url2 <url_str>
    set action-url3 <url_str>
    set action-url4 <url_str>
    set action-url5 <url_str>
    set action-url6 <url_str>
    set action-url7 <url_str>
    set action-url8 <url_str>
    set action-url9 <url_str>
    set severity {High | Medium | Low}
    set trigger <trigger_policy_name>
    config hidden-field-name
      edit <entry_index>
        set argument <hidden-field_name>
      next
    end
  next
```

```
end
```

Variable	Description	Default
`<hidden-field-rule_name>`	Type the name of the hidden field rule.	No default.
`action {alert | alert_deny | redirect | send_403_forbidden}`	Select one of the following actions that the FortiWeb unit will perform when an HTTP request violates one of the hidden field rules in the entry: • `alert`: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "config log disk" on page 44. • `alert_deny`: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "config log disk" on page 44. • `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 "config log disk" on page 44 and `redirect-url <redirect_fqdn>` • `send_403_forbidden`: Reply with an HTTP 403 (Access Forbidden) error message and generate an alert and/or log message. For details, see "config log disk" on page 44. **Note:** If you select an auto-learning profile used by an offline protection profiles that use this hidden file 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. For more information on auto-learning requirements, see "config waf web-protection-profile autolearning-profile" on page 232.	`alert`
`host <allowed-hosts_name>`	Type the IP address or fully qualified domain name (FQDN) of a protected host. This setting applies only if `host-status` is `enable`.	No default.
`host-status {enable | disable}`	Enable to apply this hidden field rule only to HTTP requests for specific web hosts. Also configure `host <allowed-hosts_name>`. Disable to match the input rule based upon the other criteria, such as the URL, but regardless of the `Host:` field.	`disable`
`request-file <url_str>`	Type the exact URL that contains the hidden form for which you want to create a hidden field rule. 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 `host <allowed-hosts_name>`. Regular expressions are not supported.	No default.
`action-url0 <url_str>`	You can add up to 10 one post URLs that are valid to use when the client submits the form containing the hidden fields in this rule.	No default.
`action-url1 <url_str>`		
`action-url2 <url_str>`		
`action-url3 <url_str>`		
`action-url4 <url_str>`		
`action-url5 <url_str>`		
`action-url6 <url_str>`		
`action-url7 <url_str>`		
`action-url8 <url_str>`		
`action-url9 <url_str>`		
`severity {High | Medium | Low}`	Type the severity level you want FortiWeb to use in the records and reports generated when the specified policy is violated: one of: `Low`, `Medium`, or `High`.	`High`

Variable	Description	Default
`trigger <trigger_policy_name>`	Select the trigger policy you want FortiWeb to apply when the specified policy is violated. Trigger policies determine who will be notified by email when the policy is violated, and whether the log message associated with the violation is recorded in Syslog or FortiAnalyzer.	No default.
`<entry_index>`	Type the index number of the individual entry in the list.	No default.
`argument <hidden-field_name>`	Type the name of the hidden input, such as `languagepref`.	No default.

Example

This example blocks and logs requests from search.jsp if its hidden form input, whose name is “languagepref”, is posted to any URL other than query.do.

```
config waf hidden-fields-rule
  edit "hidden_fields_rule1"
    set action alert_deny
    set request-file "/search.jsp"
    set action-url0 "/query.do"
    config rule-list
      edit 1
        set argument "languagepref"
      next
    end
  next
end
```

History

FortiWeb v3.3.0	New.
FortiWeb v4.0.0	Added options `redirect` and `send_403_forbidden` to `action` field.
FortiWeb v4.2	Set statements `severity` and `trigger` added.

Related topics

- config server-policy allow-hosts
- config waf hidden-fields-protection

waf http-authen http-authen-policy

Use this command to group HTTP authentication rules into HTTP authentication policies.

The FortiWeb unit uses authentication policies with the HTTP authentication feature to authorize HTTP requests. For details, see the *FortiWeb Administration Guide*.

To apply HTTP authentication policies, select them in an inline protection profile. For details, see "config waf web-protection-profile inline-protection" on page 234.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config waf http-authen http-authen-policy
  edit <auth-policy_name>
    set cache {enable | disable}
    set alert-type {none | fail | success | all}
    set cache-timeout <timeout_int>
    config rule
      edit <entry_index>
        set http-authen-rule <http-auth-rule_name>
      next
    end
  next
end
```

Variable	Description	Default
`<auth-policy_name>`	Type the name of the HTTP authentication policy.	No default.
`cache {enable | disable}`	Enable or disable LDAP query caching. If enabled, client usernames and passwords are cached for the timeout duration, which can reduce frequent LDAP queries.	No default
`alert-type {none | fail | success | all}`	Type the instances when alerts will be issued for HTTP authentication attempts: • `none`: No alerts are issued for HTTP authentication. • `fail`: Alerts are issued only for HTTP authentication failures. • `success`: Alerts are issued for successful HTTP authentication. • `all`: Alerts are issued for all failed and successful HTTP authentication.	`none`
`cache-timeout <timeout_int>`	The amount of time LDAP query results are cached, in seconds. This option is available only when `cache` is enabled.	300
`<entry_index>`	Type the index number of the individual entry in the list.	No default.
`http-authen-rule <http-auth-rule_name>`	Type the name of an existing HTTP authentication rule.	No default.

Example

This example first configures a user group that contains both a local user account and an LDAP query.

```
config user user-group
  edit "user-group1"
    config members
      edit 1
        set type local
        set name "local-user1"
```

```
      next
      edit 2
        set name "ldap-user1"
        set type ldap
      next
    end
  next
end
```

Second, it configures a rule that requires basic HTTP authentication when requesting the URL `/employees/holidays.html` on the host `www.example.com`. This URL will be identified as belonging to the realm named “Restricted Area”. Users belonging to `user-group1` can authenticate.

```
config waf http-authen http-authen-rule
  edit "auth-rule1"
    set host-status enable
    set host "www.example.com"
    config rule
      edit 1
        set request-url "/employees/holidays.html"
        set authen-type basic
        set user-group "user-group1"
        set user-realm "Restricted Area"
      next
    end
  next
end
```

Third, it groups two HTTP authentication rules into an HTTP authentication policy that can be applied in a profile.

```
config waf http-authen http-authen-policy
  edit "http-auth-policy1"
    config rule
      edit 1
        set http-authen-rule "http-auth-rule1"
      next
      edit 2
        set http-authen-rule "http-auth-rule2"
      next
    end
  next
end
```

History

FortiWeb v4.0.0	New.
FortiWeb v4.0.1	New field `cache`. Enables caching of LDAP query results.
FortiWeb v4.2	New field `alert-type`. Sets when alerts occur.

Related topics

- config waf http-authen http-authen-rule
- config waf web-protection-profile inline-protection

waf http-authen http-authen-rule

Use this command to configure HTTP 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.

You apply authentication rules by adding them to an authentication policy, which is ultimately selected within an inline protection profile for use in web protection. For details, see "config waf http-authen http-authen-policy" on page 183.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config waf http-authen http-authen-rule
  edit <auth-rule_name>
    set host <allowed-hosts_name>
    set host-status {enable | disable}
    config rule
      edit <entry_index>
        set authen-type {basic | digest | ntlm}
        set request-url <path_str>
        set user-group <user-group_name>
        set user-realm <realm_str>
      next
    end
  next
end
```

Variable	Description	Default
`<auth-rule_name>`	Type the name of the HTTP authentication rule.	No default.
`host <allowed-hosts_name>`	Type the IP address or fully qualified domain name (FQDN) of a protected host. This setting applies only if `host-status` is `enable`.	No default.
`host-status {enable | disable}`	Enable to apply this HTTP authentication rule only to HTTP requests for specific web hosts. Also configure `host <allowed-hosts_name>`. Disable to match the HTTP authentication rule based upon the other criteria, such as the URL, but regardless of the `Host:` field.	`disable`
`<entry_index>`	Type the index number of the individual user group specification.	No default.
`authen-type {basic | digest | ntlm}`	Select which type of HTTP authentication to use, either: • `basic`: Clear text, Base64-encoded user nameand password. Supports local user accounts and LDAP user queries. NTLM user queries are not supported, and will be ignored if any are in the user group. • `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. • `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.	`basic`
`request-url <path_str>`	Type the literal URL, such as `/employees/holidays.html`, that a request must match in order to trigger HTTP authentication.	No default.

Variable	Description	Default
`user-group <user-group_name>`	Type the name of a user group that is authorized to use the URL in `request-url <path_str>`.	No default.
`user-realm <realm_str>`	Type the realm, such as `Restricted Area`, to which the `request-url <path_str>` belongs. The realm is often used by users' browsers. • 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. • 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. The realm may be the same for multiple authentication rules, if all of those URLs permit the same user group to authenticate. For example, the user group `All_Employees` could have access to the `request-url <path_str>` 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. This field does not appear if `authen-type` is `ntlm`, which does not support HTTP-style realms.	No default.

Example

For an example, see "config waf http-authen http-authen-policy" on page 183.

History

FortiWeb v4.0.0 New.

Related topics

- config user user-group
- config waf http-authen http-authen-policy

waf http-constraints-exceptions

Use set statements under this command to configure exceptions to existing HTTP protocol parameter constraints for specific hosts.

Exceptions may be useful if you know that some HTTP protocol constraints, during normal use, will cause false positives by matching an attack signature. Exceptions define HTTP constraints that will ***not*** be subject to HTTP protocol constraint policy.

For example, if you enable `max-http-header-length` in a HTTP protocol constraint exception for a specific host, FortiWeb ignores the HTTP header length check when executing the web protection profile for that host.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config waf http-constraints-exceptions
  edit <http-exception-name>
    config http_constraints-exception-list
      edit <entry_index>
        set request-file <url-pattern>
        set request-type {plain | regular}
        set host {ipv4> | <fqdn>}
        set host-status {enable | disable}
        set Illegal-host-name-check {enable | disable}
        set Illegal-http-request-method-check {enable | disable}
        set max-cookie-in-request {enable | disable}
        set max-header-line-request {enable | disable}
        set max-http-body-length {enable | disable}
        set max-http-content-length {enable | disable}
        set max-http-header-length {enable | disable}
        set max-http-header-line-length {enable | disable}
        set max-http-parameter-length {enable | disable}
        set max-http-request-length {enable | disable}
        set max-url-parameter {enable | disable}
        set max-url-parameter-length {enable | disable}
      next
    end
  next
end
```

Variable	Description	Default
`<http-exception-name>`	Type the name of the HTTP protocol constraint exception.	No default.
`<entry_index>`	Type the index number of the individual constraint definition.	No default.
`request-file <url-pattern>`	Type either: • 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 (/). • 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`. Do not include the name of the web host, such as `www.example.com`, which is configured separately in `host`.	No default.

Variable	Description	Default
`request-type {plain | regular}`	Type either `plain` or `regular` (for a regular expression) to match the string entered in `request-file`.	No default.
`host {ipv4> | <fqdn>}`	Type the IP address or fully qualified domain name (FQDN) of the protected host to which this exception applies.	No default.
`host-status {enable | disable}`	Enter `enable` to apply this HTTP constraint exception only to HTTP requests for specific web hosts, as set using `host`. Enter `disable` to apply the exceptions to all web hosts.	`disable`
`Illegal-host-name-check {enable | disable}`	Type `enable` to create an exception to this constraint. Change `enable` to `disable` to reapply the constraint.	`disable`
`Illegal-http-request-method-check {enable | disable}`	Type `enable` to create an exception to this constraint. Change `enable` to `disable` to reapply the constraint.	`disable`
`max-cookie-in-request {enable | disable}`	Type `enable` to create an exception to this constraint. Change `enable` to `disable` to reapply the constraint.	`disable`
`max-header-line-request {enable | disable}`	Type `enable` to create an exception to this constraint. Change `enable` to `disable` to reapply the constraint.	`disable`
`max-http-body-length {enable | disable}`	Type `enable` to create an exception to this constraint. Change `enable` to `disable` to reapply the constraint.	`disable`
`max-http-content-length {enable | disable}`	Type `enable` to create an exception to this constraint. Change `enable` to `disable` to reapply the constraint.	`disable`
`max-http-header-length {enable | disable}`	Type `enable` to create an exception to this constraint. Change `enable` to `disable` to reapply the constraint.	`disable`
`max-http-header-line-length {enable | disable}`	Type `enable` to create an exception to this constraint. Change `enable` to `disable` to reapply the constraint.	`disable`
`max-http-parameter-length {enable | disable}`	Type `enable` to create an exception to this constraint. Change `enable` to `disable` to reapply the constraint.	`disable`
`max-http-request-length {enable | disable}`	Type `enable` to create an exception to this constraint. Change `enable` to `disable` to reapply the constraint.	`disable`
`max-url-parameter {enable | disable}`	Type `enable` to create an exception to this constraint. Change `enable` to `disable` to reapply the constraint.	`disable`
`max-url-parameter-length {enable | disable}`	Type `enable` to create an exception to this constraint. Change `enable` to `disable` to reapply the constraint.	`disable`

Example

```
config waf http-constraints-exceptions
  edit "exception1"
    config http_constraints-exception-list
      edit 1
        set host "172.20.120.48"
        set host-status enable
        set max-http-header-length enable
        set request-file "/login.asp"
        next
      edit 2
        set host "172.20.120.27"
        set host-status enable
        set max-http-body-length enable
        set request-file "/login.asp"
        next
      end
```

```
    next
  end
```

History

FortiWeb v4.2 New.

Related topics

- config waf web-protection-profile inline-protection
- config waf web-protection-profile offline-protection
- config log trigger-policy
- config waf http-protocol-parameter-restriction

waf http-protocol-parameter-restriction

Use this command to configure HTTP protocol parameter 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.

Each protocol parameter can be uniquely configured with an action, severity and trigger that determines how an attack on that parameter is handled. For example, `HTTP_HEADER_LEN_OVERFLOW` and `HTTP_HEADER_LINE_LEN_OVERFLOW` constraints could have the action set to alert, the severity set to high, and a trigger set to deliver an email each time these protocol parameters are violated.

When the FortiWeb unit detects an HTTP request that violates these protocol parameters, it creates an alert log message and sends an email to predefined users to notify them of the violation.

To apply HTTP protocol constraints, select them in an inline or offline protection profile. For details, see “config waf web-protection-profile inline-protection” on page 234 or “config waf web-protection-profile offline-protection” on page 239.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see “Permissions” on page 29.

Syntax

Note: Each http protocol parameter has settings for -action, -severity and -trigger associated with a violation of the parameter. For more information, see ““config HTTP protocol parameter violations” on page 191.

```
config waf http-protocol-parameter-restriction
  edit <http-constraint_name>
    set Illegal-host-name-check {enable | disable}
    set Illegal-http-request-method-check {enable | disable}
    set Illegal-http-version-check {enable | disable}
    set max-cookie-in-request <limit_int>
    set max-header-line-request <limit_int>
    set max-http-body-length <limit_int>
    set max-http-content-length <limit_int>
    set max-http-header-length <limit_int>
    set max-http-header-line-length <limit_int>
    set max-http-parameter-length <limit_int>
    set max-http-request-length <limit_int>
    set max-url-parameter <limit_int>
    set max-url-parameter-length <limit_int>
    set is-default-config {yes | no}
```

Variable	Description	Default
`<http-constraint_name>`	Type the name of the HTTP protocol constraint.	No default.
`Illegal-host-name-check {enable | disable}`	Enable to check for illegal characters in the Host: line of the HTTP header, such as NULL characters or encoded characters. For example, characters such as "0x0" or "%00*" are considered illegal.	`enable`
`Illegal-http-request-method-check {enable | disable}`	Enable to check for illegal HTTP version numbers.	`enable`
`Illegal-http-version-check {enable | disable}`	Enable to check for illegal HTTP version numbers. If the HTTP version is not "HTTP/1.0" or "HTTP/1.1", it is considered illegal.	`enable`

Variable	Description	Default
`max-cookie-in-request <limit_int>`	Type the maximum acceptable number of cookies in an HTTP request. The allowed range is 1 to 32.	`16`
`max-header-line-request <limit_int>`	Type the maximum acceptable number of lines in the HTTP header. The allowed range is 0 to 64.	`32`
`max-http-body-length <limit_int>`	Type the maximum acceptable length in bytes of the HTTP body. To disable the limit, type `0`.	`0`
`max-http-content-length <limit_int>`	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. To disable the limit, type `0`.	`0`
`max-http-header-length <limit_int>`	Type the maximum acceptable length in bytes of the HTTP header. To disable the limit, type `0`.	`4096`
`max-http-header-line-length <limit_int>`	Type the maximum acceptable length in bytes of each line in the HTTP header. To disable the limit, type `0`.	`1024`
`max-http-parameter-length <limit_int>`	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. To disable the limit, type `0`.	`6144`
`max-http-request-length <limit_int>`	Type the maximum acceptable length in bytes of the HTTP request. The allowed range is 0 to 67108864.	`67108864`
`max-url-parameter <limit_int>`	Type the maximum number of URL parameters. The allowed range is 1 to 64.	`16`
`max-url-parameter-length <limit_int>`	Type the maximum acceptable length of an URL parameter (including the name and value). The allowed range is 1 to 2048.	`2048`
`is-default-config {yes | no}`	Enter yes to set this configuration as the default.	`no`

HTTP protocol parameter violations

Each HTTP protocol parameter constraint has settings to define an action, severity and trigger associated with a violation of the constraint. The action, severity and trigger settings can be applied as required to ensure the violation is clearly identified and communicated.

The syntax for setting HTTP protocol parameter constraint violation action, severity and trigger is as follows:

```
config waf http-protocol-parameter-restriction
  edit <http-constraint_name>
    set <parameter>-action
       {alert | deny&alert | redirect | send_403_forbidden | altert&erase}
    set <parameter>-severity {High | Medium | Low}
    set <parameter>-trigger <trigger-policy-name>
  next
end
```

Variable	Description	Default
`<parameter>-action {alert | deny&alert | redirect | send_403_forbidden | altert&erase}`	Each protocol parameter has a configurable "action" command (i.e. `max-http-header-length-action`), which is used to define the action taken if the HTTP protocol parameter is violated. Select the appropriate action. The available action vary depending on operating mode and protocol parameter.	`alert`

`<parameter>-severity {High | Medium | Low}`	Each violation type has a configurable "severity" command (i.e. `max-http-header-length-severity`). You can configure each violation type to be recorded and reported as either low, medium or high severity.	`High`
`<parameter>-trigger <trigger-policy-name>`	Each violation type has a configurable "trigger" command (i.e. `max-http-header-length-trigger`. When a violation occurs, the FortiWeb unit invokes the specified trigger. The trigger determines whether an alert is created and an email sent to predefined users and/or whether the violation log message is recorded in Syslog. For more information, see "config log trigger-policy" on page 66.	No default.

Example

This example limits the total size of the HTTP header, including all lines, to 2,048 bytes. If the HTTP header length exceeds 2,048 bytes, the FortiWeb unit takes an action to create an `alert` log message, identifies the violation as `medium` severity, and sends an email to the administrators defined within the trigger policy `email-admin`.

```
config waf http-protocol-parameter-restriction
  edit "http-constraint1"
    set max-http-header-length 2048
    set max-http-header-length-action alert
    set max-http-header-length-severity Medium
    set max-http-header-length-trigger email-admin
  next
end
```

History

FortiWeb v4.0.0	New.
FortiWeb v4.1	Added variables for: • max-http-request-length • max-url-parameter-length • Illegal-http-version-check • max-cookie-in-request • max-header-line-request • Illegal-http-request-method-check • max-url-parameter • Illegal-host-name-check
FortiWeb v4.1.1	Added new settings for action, severity and trigger for each parameter.

Related topics

- config waf web-protection-profile inline-protection
- config waf web-protection-profile offline-protection
- config log trigger-policy
- config waf http-constraints-exceptions

waf input-rule

Use this command to configure input rules.

Input rules define whether or not parameters are required, and sets their maximum allowed length, for HTTP requests matching the host and URL defined in the input rule.

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.

To apply input rules, select them within a parameter validation rule. For details, see “config waf parameter-validation-rule” on page 203.

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 ““config server-policy allow-hosts” on page 71.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see “Permissions” on page 29.

Syntax

```
config waf input-rule
  edit <input-rule_name>
    set action {alert | alert_deny | redirect | send_403_forbidden}
    set host <allowed-hosts_name>
    set host-status {enable | disable}
    set request-file <url_str>
    set request-type {plain | regular}
    set severity {High | Medium | Low}
    set trigger <trigger_policy_name>
    config rule-list
      edit <entry_index>
        set argument-expression <regex_str>
        set argument-name <input_name>
        set data-type {<type>}
        set custom-data-type {custom data type}
        set is-essential {yes | no}
        set max-length <limit_int>
        set type-checked (enable | disable}
      next
    end
  next
end
```

Variable	Description	Default
<input-rule_name>	Type the name of the input rule.	No default.
action {alert | alert_deny | redirect | send_403_forbidden}	Select one of the following actions that the FortiWeb unit will perform when an HTTP request violates one of the input rules in the entry: • alert: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see ""config log disk" on page 44. • alert_deny: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "config log disk" on page 44. • 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 "config log disk" on page 44 and redirect-url <redirect_fqdn>. • send_403_forbidden: Reply with an HTTP 403 (Access Forbidden) error message and generate an alert and/or log message. For details, see ""config log disk" on page 44. **Note:** If an auto-learning profile will be selected in the policy with offline protection 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. For more information on auto-learning requirements, see "config waf web-protection-profile autolearning-profile" on page 232.	alert
host <allowed-hosts_name>	Type the IP address or fully qualified domain name (FQDN) of a protected host. This setting applies only if host-status is enable.	No default.
host-status {enable | disable}	Enable to apply this input rule only to HTTP requests for specific web hosts. Also configure host <allowed-hosts_name>. Disable to match the input rule based upon the other criteria, such as the URL, but regardless of the Host: field.	disable
request-file <url_str>	Depending on your selection in request-type {plain | regular}, type either: • 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 (/). • 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. Do not include the name of the web host, such as www.example.com, which is configured separately in host <allowed-hosts_name>. **Note:** Regular expressions beginning with an exclamation point (!) are not supported. For information on language and regular expression matching, see the *FortiWeb Administration Guide*.	No default.
request-type {plain | regular}	Select whether request-file <url_str> will contain a literal URL (plain), or a regular expression designed to match multiple URLs (regular).	plain
severity {High | Medium | Low}	Type the severity level you want FortiWeb to use in the records and reports generated when the specified policy is violated: one of: Low, Medium, or High.	High
trigger <trigger_policy_name>	Select the trigger policy you want FortiWeb to apply when the specified policy is violated. Trigger policies determine who will be notified by email when the policy is violated, and whether the log message associated with the violation is recorded in Syslog or FortiAnalyzer.	No default.
<entry_index>	Type the index number of the individual entry in the list.	No default.

Variable	Description	Default
`type-checked {enable | disable}`	If set to disable, FortiWEB ignores all `data-type` and `custom-data-type` settings	enable
`argument-expression <regex_str>`	Type a regular expression that matches all valid values, and no invalid values, for this input. Alternatively, configure `data-type`. **Note:** Regular expressions beginning with an exclamation point (`!`) are not supported.	No default.
`argument-name <input_name>`	Type the name of the input as it appears in the HTTP content, such as `username`.	No default.
`custom-data-type {custom data type}`	Select one of the custom data types, if the input matches one of them .	No default.
`is-essential {yes | no}`	Select `yes` if the parameter is required for HTTP requests to this combination of `Host:` field and URL. Otherwise, select `no`.	`no`
`max-length <limit_int>`	Type the maximum allowed length of the parameter value. To disable the length limit, type `0`.	`0`
`type-checked (enable | disable}`	Type enable to instruct the FortiWeb unit to ignore all data-type-check related settings even if these settings have values.	disable

Variable	Description	Default

`data-type {<type>}`	Select one of the predefined data types, if the input matches one of them. Alternatively, configure `argument-expression <regex_str>`. This option is ignored if you configure `argument-expression <regex_str>`, which also defines parameters to which the input rule applies, but supersedes this option.
	• `Address`: Canadian postal codes and United States ZIP code and ZIP + 4 codes.
	• `Canadian_Post_code`: Canadian postal codes such as K2H 7B8.
	• `Canadian_Province_Name`: 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.
	• `Canadian_SIN`: Canadian Social Insurance Numbers (SIN) such as 123-456-789.
	• `China_Post_Code`: Chinese postal codes such as 610000.
	• `Country_Name`: Country names, codes, and abbreviations in English characters, such as CA, Cote d'Ivoire, Brazil, Russian Federation, Brunei, and Dar el Salam.
	• `Credit_Card_Number`: American Express, Carte Blanche, Diners Club, enRoute, Japan Credit Bureau (JCB), Master Card, Novus, and Visa credit card numbers.
	• `Dates_and_Times`: 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.
	• `Email`: Email addresses such as admin@example.com.
	• `Markup_or_Code`: HTML comments, wiki code, hexadecimal HTML color codes, quoted strings in VBScript and ANSI SQL, SQL statements, and RTF bookmarks such as:
	`• #00ccff, <!--A comment.-->`
	`• [link url="http://example.com/url?var=A&var2=B"]`
	`• SELECT * FROM TABLE`
	`• {\*\bkmkstart TagAmountText}`
	Does ***not*** match ANSI escape codes, which are instead detected as strings.
	• `Num`: 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.
	• `Phone`: Australian, United States, and Indian phone numbers in various formats such as (123)456-7890, 1.123.456.7890, 0732105432, and +919847444225.
	• `String`: 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.
	• `Uri`: Uniform resource identifiers (URI) such as http://www.example.com, ftp://ftp.example.com, and mailto:admin@example.com.
	• `US_SSN`: United States Social Security Numbers (SSN) such as 123-45-6789.
	• `US_State_Name`: United States state names and modern postal abbreviations such as HI and Wyoming. Does ***not*** detect older postal abbreviations such as Fl. or Wyo.
	• `US_Zip_Code`: United States ZIP code and ZIP + 4 codes such as 34285-3210.
		No default.

Example

This example blocks and logs requests for the file named login.php that do not include a user name and password, both of which are required, or whose user name and password exceed the 64-character limit.

```
config waf input-rule
  edit "input_rule1"
    set action alert_deny
    set request-file "/login.php?*"
    request-type regular
    config rule-list
      edit 1
        set argument-name "username"
        set data-type Email
        set is-essential yes
        set max-length 64
      next
      edit 2
        set argument-name "password"
        set data-type String
        set is-essential yes
        set max-length 64
      next
    end
  next
end
```

History

FortiWeb v3.2.0	New.
FortiWeb v3.3.0	Field `request-file` now accepts regular expressions that do not begin with a slash (/) character.
FortiWeb v4.0.0	Added option `send_403_forbidden` to `action` field.
FortiWeb v4.2	Set statements `type-checked`, `severity`, and `trigger` added.

Related topics

- config server-policy allow-hosts
- config waf parameter-validation-rule

waf ip-list

Use this command to define whether specific source IP addresses are trusted or not trusted:

- Trusted IPs are source IP addresses that you explicitly allow access to your web servers because they are trusted.
- Black-listed IPs are source IP addresses that you explicitly disallow and block access to your web servers because they have failed web protection policy scans.

If a source IP address is not explicitly identified in an IP list policy as a black IP, the source IP has access to your web servers, pending additional web protection scan techniques.

If a source IP addresses is explicitly designated as a trusted IP, that IP address is permitted to connect to your web servers and is exempt from many of the restrictions that would otherwise be applied by the web protection profile used by a server policy.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config waf ip-list
  edit <ip-list-policy_name>
    config members
      edit <entry_index>
        set type {trust-ip | black-ip}
        set <ipv4>
        set severity {Low | Medium | High}
        set trigger-policy <trigger-policy_name>
        next
    end
  next
end
```

Variable	Description	Default
`<ip-list-policy_name>`	Type the name of the IP list policy.	No default.
`<entry_index>`	Type the index number of the individual entry in the list.	No default.
`<ipv4>`	Enter an IP address to be added to the trusted or black list.	No default.
`type {trust-ip | black-ip}`	Enter the type of list to create: either a trusted list or a black list. The type defaults to trust-ip .	`trust-ip`
`severity {Low | Medium | High}`	For a black list only, enter the severity level you want FortiWeb to use in the records and reports generated when the specified IP address attempts to access your web servers. You can configure each violation type to be either `Low`, `Medium` or `High` severity.	No default.
`trigger-policy <trigger-policy_name>`	For a black list only, type the name of the trigger policy you want FortiWeb to apply when the specified IP address attempts to access your web servers. Trigger policies determine who will be notified by email when the source IP address attempts to access your web servers, and whether the log message associated with the attempt is recorded in Syslog or FortiAnalyzer.	No default.

Example

The following shows the configuration for a simple trust list followed by a black list.

```
config waf ip-list
  edit "IP-List-Policy1"
    config members
      edit 1
        set ip 192.0.2.0
        next
      edit 2
        set type black-ip
        set ip 192.0.2.1
        set severity Medium
        set trigger-policy "TriggerActionPolicy1"
      next
    end
  next
end
```

History

FortiWeb v4.2 New.
Replaces waf `black-ipaddress-list` and `waf trust-ipaddress list`.

waf page-access-rule

Use this command to configure page access rules.

Page access rules define URLs that can 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 attack log message (see "config log disk" on page 44).

To apply page access rules, select them within an inline protection profile. For details, see "config waf web-protection-profile inline-protection" on page 234.

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 "config server-policy allow-hosts" on page 71.

Use SNMP traps to notify you when a page access rule is enforced. For details, see "config system snmp community" on page 150.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see "Permissions" on page 29.

Note: In order for page access rules to be enforced, you must also enable `http-session-management {enable | disable}` in the inline protection profile.

Syntax

```
config waf page-access-rule
  edit <page-access-rule_name>
    config page-access-list
      edit <entry_index>
        set host <allowed-hosts_name>
        set host-status {enable | disable}
        set request-file <url_str>
        set request-type {plain | regular}
      next
    end
```

```
    next
  end
```

Variable	Description	Default
<page-access-rule_name>	Type the name of the page access rule.	No default.
<entry_index>	Type the index number of the individual entry in the list. Page access rules should be added to the set in the order which clients will be permitted to access them. For example, if a client must access /login.asp before /account.asp, add the rule for /login.asp first.	No default.
host <allowed-hosts_name>	Type the name of a protected host that the Host: field of an HTTP request must be in order to match the page access rule. This setting applies only if host-status is enable.	No default.
host-status {enable | disable}	Enable to apply this page access rule only to HTTP requests for specific web hosts. Also configure host <allowed-hosts_name>. Disable to match the page access rule based upon the other criteria, such as the URL, but regardless of the Host: field.	disable
request-file <url_str>	Depending on your selection in request-type {plain | regular}, type either: • 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 (/). • 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. Do not include the name of the web host, such as www.example.com, which is configured separately in host <allowed-hosts_name>. **Note:** Regular expressions beginning with an exclamation point (!) are not supported. For information on language and regular expression matching, see the *FortiWeb Administration Guide*.	No default.
request-type {plain | regular}	Select whether request-file <url_str> will contain a literal URL (plain), or a regular expression designed to match multiple URLs (regular).	plain

Example

This example allows any request to www.example.com, as long as it follows the expected sequence within a session for the four key shopping cart URLs (/addToCart.do, /checkout.do, /shipment.do, then /payment.do).

```
config waf page-access-rule
  edit "page-access-rule1"
    config page-access-list
      edit 1
        set host "www.example.com"
        set host-status enable
        set request-file "/addToCart.do?item=*"
        set request-type regular
      next
      edit 2
        set host "www.example.com"
        set host-status enable
        set request-file "/checkout.do?login=*"
        set request-type regular
      next
      edit 3
```

```
        set host "www.example.com"
        set host-status enable
        set request-file "/shipment.do"
        set request-type plain
      next
      edit 4
        set host "www.example.com"
        set host-status enable
        set request-file "/payment.do"
        set request-type plain
      next
    end
  next
end
```

History

FortiWeb v3.2.0	New.
FortiWeb v3.3.0	Field `request-file` now accepts regular expressions that do not begin with a slash (/) character.

Related topics

- config server-policy allow-hosts
- config system snmp community
- config waf web-protection-profile inline-protection

waf parameter-validation-rule

Use this command to configure parameter validation rules, each of which is a group of input rule entries.

To apply parameter validation rules, select them within an inline or offline protection profile. For details, see “config waf web-protection-profile inline-protection” on page 234 or “config waf web-protection-profile offline-protection” on page 239.

Before you can configure parameter validation rules, you must first configure one or more input rules. For details, see “config waf input-rule” on page 193.

Use SNMP traps to notify you when a parameter validation rule is enforced. For details, see “config system snmp community” on page 150.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see “Permissions” on page 29.

Syntax

```
config waf parameter-validation-rule
  edit <rule_name>
    config input-rule-list
      edit <entry_index>
        set input-rule <input-rule_name>
      next
    end
  next
end
```

Variable	Description	Default
`<rule_name>`	Type the name of the parameter validation rule.	No default.
`<entry_index>`	Type the index number of the individual entry in the list.	No default.
`input-rule <input-rule_name>`	Type the name of an input rule.	No default.

Example

This example configures a parameter validation rule named parameter_validator1, which applies two input rules, input_rule1 and input_rule2.

```
config waf parameter-validation-rule
  edit "parameter_validator1"
    config input-rule-list
      edit 1
        set input-rule "input_rule1"
    next
      edit 2
        set input-rule "input_rule2"
      next
    end
  next
end
```

History

FortiWeb v3.2.0 New.

Related topics

- config waf input-rule
- config waf web-protection-profile inline-protection
- config waf web-protection-profile offline-protection
- config system snmp community

waf robot-control

Use this command to configure 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 known legitimate robots, and to block known misbehaving robots.

Before you can configure a robot control sensor, you must first configure any custom or predefined robot groups that you want to include. For details, see "config waf web-robot" on page 242 and "config waf web-custom-robot" on page 231.

To apply robot control sensors, select them within an inline or offline protection profile. For details, see "config waf web-protection-profile inline-protection" on page 234 or "config waf web-protection-profile offline-protection" on page 239.

Use SNMP traps to notify you when a robot control rule is enforced. For details, see "config system snmp community" on page 150.

Tip: Alternatively, you can automatically configure a robot control sensor that allows all search engine types by generating a default auto-learning profile. For details, see the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config waf robot-control
  edit <robot-control_name>
    set access-limit-share-ip <rate_int>
    set access-limit-standalone-ip <rate_int>
    set allow-custom-robot <custom-robot_name>
    set allow-robot <robot-group_name>
    set bad-robot {enable | disable}
    set bad-robot-action {alert | alert_deny | redirect |
       send_403_forbidden}
    set bad-robot-severity {Low | Medium | High}
    set bad-robot-trigger <trigger-policy_name>
    set block-period <duration_int>
    set is-default-config {yes | no}
  next
end
```

Variable	Description	Default
<robot-control_name>	Type the name of the robot control sensor.	No default.
access-limit-share-ip <rate_int>	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 block-period <duration_int>. To disable the rate limit, type 0. **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 access-limit-standalone-ip <rate_int>.	0
access-limit-standalone-ip <rate_int>	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 block-period <duration_int>. To disable the rate limit, type 0.	0
allow-custom-robot <custom-robot_name>	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 "config waf web-custom-robot" on page 231. The FortiWeb unit will omit any subsequent intrusion detection features, including parameter validation rules, server protection rules, or bad-robot {enable | disable} detection. 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.	No default.
allow-robot <robot-group_name>	Select the name of a robot group that defines which, if any, well-known search engines' web crawlers will be exempt from the rate limit of this robot control sensor. In addition to omitting the rate limit, the FortiWeb unit will omit any subsequent intrusion detection features, including parameter validation rules, server protection rules, or bad-robot detection. 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.	No default.
bad-robot {enable | disable}	Select whether to enable or disable detection of web crawlers known to misbehave. Also configure bad-robot-action {alert | alert_deny | redirect | send_403_forbidden}.	disable
bad-robot-action {alert | alert_deny | redirect | send_403_forbidden}	Select the action that the FortiWeb unit will perform when it detects a web crawler known to misbehave. • alert: Accept the connection and generate an alert and/or log message. • alert_deny: Block the connection and generate an alert and/or log message. • 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 "config log disk" on page 441 and redirect-url <redirect_fqdn>. • send_403_forbidden: Reply with an HTTP 403 (Access Forbidden) error message and generate an alert and/or log message. For details, see "config log disk" on page 44. For more information on logging and alerts, see "config log disk" on page 44. **Note:** If you select an auto-learning profile in the server policy with offline protection 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. For more information on auto-learning requirements, see "config waf web-protection-profile autolearning-profile" on page 232.	No default.

Variable	Description	Default
`bad-robot-severity {Low | Medium | High}`	Enter the severity level you want FortiWeb to use in the records and reports generated when the specified IP address attempts to access your web servers. You can configure each violation type to be either `Low`, `Medium` or `High` severity.	`Low`
`bad-robot-trigger <trigger-policy_name>`	Type the name of the trigger policy you want FortiWeb to apply when the specified IP address attempts to access your web servers. Trigger policies determine who will be notified by email when the source IP address attempts to access your web servers, and whether the log message associated with the attempt is recorded in Syslog or FortiAnalyzer.	No default.
`block-period <duration_int>`	Type the length of time for which the FortiWeb unit will block additional requests after a source IP address exceeds its rate threshold in either `access-limit-share-ip <rate_int>` or `access-limit-standalone-ip <rate_int>`.	`0`
`is-default-config {yes | no}`	Enter yes to set this configuration as the default.	`no`

Example

This example allows the Yahoo! and Baidu search engines' robots, forming the group named `robot-group1`, to crawl the protected web site, and blocks known misbehaving robots. For all other robots, it limits the rate to 3 requests per second for each individual client's IP address, and 20 requests per second for each NAT client's IP address; robots exceeding the rate limit are blocked from making further requests for the next 60 seconds.

```
config waf web-robot
  edit "robot_group1"
    config list
      edit 1
        set robot yahoo
      next
      edit 2
        set robot baidu
      next
    end
  next
end
config waf robot-control
  edit "robot_control_sensor"
    set access-limit-share-ip 20
    set access-limit-standalone-ip 3
    set allow-robot robot-group1
    set bad-robot enable
    set bad-robot-action alert_deny
    set block-period 60
  next
end
```

History

FortiWeb v3.2.0 New.

FortiWeb v3.3.2 Field `allow-robot` now takes a reference to a robot control group. Previously, it took an option set.

FortiWeb v4.0.0	New field `allow-custom-robot`. Configures use of a custom robot group. New options `redirect` and `send_403_forbidden` added to `bad-robot-action`.
FortiWeb v4.2	Set statements `bad-robot-severity` and `bad-robot-trigger` were added.

Related topics

- config waf web-custom-robot
- config waf web-robot
- config waf web-protection-profile inline-protection
- config waf web-protection-profile offline-protection
- config system snmp community

waf server-protection-exception

Use this command to configure 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.

To apply server protection exceptions, select them within a server protection rule. For details, see "config waf server-protection-rule" on page 212.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config waf server-protection-exception
  edit <server-protection-exception_name>
    config exception-list
      edit <entry_index>
        set common-exploits {enable | disable}
        set common-exploits-subtype {<exploit_subtypes>}{
        set credit-card-detection {enable | disable}
        set cross-site-scripting {enable | disable}
        set cross-site-scripting-subtype {<xss_subtype>}
        set host {<protected-host_ipv4> | <protected-host_fqdn>}
        set host-status {enable | disable}
        set information-disclosure {enable | disable}
        set information-disclosure-subtype {<info_subtypes>}
        set remote-file-inclusion {enable | disable}
        set remote-file-inclusion-subtype {<inclusion_subtype>}
        set request-file <url_str>
        set request-type {plain | regular}
        set sql-injection {enable | disable}
        set sql-injection-subtype {<injection_subtypes>}
      next
    end
  next
end
```

Variable	Description	Default
`<server-protection-exception_name>`	Type the name of the server protection exception.	No default.
`<entry_index>`	Type the index number of the individual entry in the list.	No default.
`common-exploits {enable | disable}`	Enable to omit detection of common exploits, such as an injection attack in a language other than SQL. Also configure `common-exploits-subtype {<exploit_subtypes>}{`.	`disable`
`credit-card-detection {enable | disable}`	Enable to omit detection of credit card numbers in the response from the server.	`disable`

Variable	Description	Default
common-exploits-subtype {<exploit_subtypes>}{	Leave this field blank to omit all subtypes, or enter the names of one or more specific subtypes that you want to omit: • file-injection • command-access • command-injection • coldfusion-injection • ldap-injection • ssi-injection • php-injection • email-injection • response-splitting • injection-flaw • src-disclosure • trojans	No default.
cross-site-scripting {enable | disable}	Enable to omit detection of cross-site scripting (XSS) attacks. Also configure cross-site-scripting-subtype {<xss_subtype>}}.	disable
cross-site-scripting-subtype {<xss_subtype>}	Leave this field blank to omit all subtypes, or enter the name of a specific subtypes that you want to omit; one of: • xss-signature-1 • xss-signature-2 • xss-signature-3 • xss-signature-4 • xss-signature-5 • xss-signature-6 • xss-signature-7 • xss-signature-8 • xss-signature-9	No default.
host {<protected-host_ipv4> | <protected-host_fqdn>}	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. This option is available only if host-status is enable.	No default.
host-status {enable | disable}	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 {<protected-host_ipv4> | <protected-host_fqdn>}.	disable
request-type {plain | regular}	Select whether request-file <url_str> is plain (that is, a literal URL) or regular (that is, a regular expression).	plain
request-file <url_str>	Depending on your selection in request-type {plain | regular}, type either: • 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 (/). • 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. Do not include the name of the web host, such as www.example.com, which is configured separately in host {<protected-host_ipv4> | <protected-host_fqdn>}.	No default.
information-disclosure {enable | disable}	Enable to omit detection of server errors and other sensitive messages in the requested document and HTTP headers. Also configure information-disclosure-subtype {<info_subtypes>}.	disable

Variable	Description	Default
information-disclosure-subtype {<info_subtypes>}	Leave this field blank to omit all subtypes, or enter the names of one or more specific subtypes that you want to omit: • application-not-available • asp-jsp-source-code-leakage • cf-information-leakage • cf-source-code-leakage • directory-listing • file-or-dir-names-leakage • iis-errors-leakage • iis-default-location • isa-server-existence-revealed • ms-doc-properties-leakage • php-information-leakage • php-source-code-leakage • statistics-pages-revealed • sql-errors-leakage • weblogic-info-disclosure • zope-information-leakage • http-retcode-4xx • http-retcode-5xx	No default.
sql-injection {enable | disable}	Enable to omit detection of SQL injection attacks. Also configure sql-injection-subtype {<injection_subtypes>}	disable
sql-injection-subtype {<injection_subtypes>}	Leave this field blank to omit all subtypes, or enter the name of a specific subtypes that you want to omit; one of • sql-injection-1 • sql-injection-2 • sql-injection-3 • sql-injection-4 • sql-injection-5 • sql-injection-6 • sql-injection-7 • sql-injection-8 • sql-injection-9 • sql-injection-10	No default.
remote-file-inclusion {enable | disable}	Type enable to omit detection of remote file inclusion, then disable individual remote file inclusion signatures that you do ***not*** want to omit, if any.	
remote-file-inclusion-subtype {<inclusion_subtype>}	Leave this field blank to omit all subtypes, or enter the names of one or more specific subtypes that you want to omit: • rfi-signature-1 • rfi-signature-2 • rfi-signature-3	

History

FortiWeb v4.0.0 New.

Related topics

- config waf server-protection-rule

waf server-protection-rule

Use this command to configure 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 attack prevention
- sensitive information disclosure prevention
- prevention of other injection attacks

Before configuring a server protection rule, if there are any URLs to which you do not want to apply those protections, you must first configure a server protection exception. For details, see “config waf server-protection-exception” on page 209.

Each server protection rule can be uniquely configured with an severity and trigger that, that in combination with the action associated with each server protection rule, determines how a violation of the rule is handled.

For example, cross-site scripting and SQL injection attacks could have the action set to alert_deny, the severity set to high, and a trigger set to deliver an alert email each time these rule violations are detected.

To apply server protection rules, select them within an inline or offline protection profile. For details, see “config waf web-protection-profile inline-protection” on page 234 or “config waf web-protection-profile offline-protection” on page 239.

Use SNMP traps to notify you when information disclosure has been prevented, or a cross-site scripting, common exploit, or SQL injection attack has been detected. For details, see “config system snmp community” on page 150.

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 the *FortiWeb Administration Guide*.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see “Permissions” on page 29.

Syntax

Note: Each server protection rule has settings for -action, -severity and -trigger associated with a violation of the rule. For more information, see “config Server protection rule violations” on page 218.

```
config waf server-protection-rule
  edit <server-protection-rule_name>
    set common-exploits {enable | disable}
    set common-exploits-action {alert | alert_deny | redirect |
       send_403_forbidden}
    set common-exploits-subtype {<exploit_subtype>}
    set credit-card-detection {enable | disable}
    set credit-card-detection-action {alert | alert_deny}
    set credit-card-detection-threshold <instances_int>
    set cross-site-scripting {enable | disable}
    set cross-site-scripting-action {alert | alert_deny | redirect |
       send_403_forbidden}
    set cross-site-scripting-subtype {<xss_subtype>}
    set extended-sig-set {enable | disable}
```

```
    set basic-severity {Low | Medium | High}
    set basic-trigger <trigger-policy_name>
    set enhanced-severity {Low | Medium | High}
    set enhanced-trigger <trigger-policy_name>
    set full-severity {Low | Medium | High}
    set full-trigger <trigger-policy_name>
    set exception-name <server-protection-exception_name>
    set custom-protection-group <custom_protection_group_name>
    set information-disclosure {enable | disable}
    set information-disclosure-action {alert | alert_erase | redirect}
    set information-disclosure-subtype {info_subtype>}
    set sql-injection {enable | disable}
    set sql-injection-action {alert | alert_deny | redirect |
       send_403_forbidden}
    set sql-injection-subtype {<injectionsubtype>}
  next
end
```

Variable	Description	Default
`<server-protection-rule_name>`	Type the name of the server protection rule.	No default.
`common-exploits {enable | disable}`	Enable to detect an injection attack in a language other than SQL. Also configure `common-exploits-action {alert | alert_deny | redirect | send_403_forbidden}`.	`disable`
`common-exploits-action {alert | alert_deny | redirect | send_403_forbidden }`	Select the action that the FortiWeb unit will perform when an HTTP request attempts to perform an injection attack in a language other than SQL. • `alert`: Accept the connection and generate an alert and/or log message. • `alert_deny`: Block the connection and generate an alert and/or log message. • `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 “config log disk” on page 44 and `redirect-url <redirect_fqdn>`. • `send_403_forbidden`: Reply with an HTTP 403 (Access Forbidden) error message and generate an alert and/or log message. For details, see “config log disk” on page 44. For more information on logging and alerts, see “config log disk” on page 44. **Note:** If an auto-learning profile will be selected in the policy with offline protection 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. For more information on auto-learning requirements, see “config waf web-protection-profile autolearning-profile” on page 232.	No default.

Variable	Description	Default
common-exploits-subtype {<exploit_subtype>}	Leave this field blank to enable all subtypes, or enter one or more names of specific subtypes that you want to enable: • file-injection • command-access • command-injection • coldfusion-injection • ldap-injection • ssi-injection • php-injection • email-injection • response-splitting • injection-flaw • src-disclosure • trojans	No default.
credit-card-detection {enable | disable}	Enable to detect credit card numbers in the response from the server. Also configure credit-card-detection-action {alert | alert_deny} and credit-card-detection-threshold <instances_int>. 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: XXXX XXXX XXXX 1234 This mostly-obscured version protects the credit card number from unnecessary exposure and disclosure. It would ***not*** trigger the credit card number detection feature. 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 trigger credit card number disclosure detection.	disable
credit-card-detection-action {alert | alert_deny}	Select which action the FortiWeb unit will take when it detects credit card number disclosure: • alert: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "config log disk" on page 44. • alert_deny: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "config log disk" on page 44. Attack log messages and *Alert Message Console* messages contain DETECT_RESPONSE_INFORMATION_disclosure: credit card leakage when this feature detects credit card disclosure. **Note:** If an auto-learning profile will be selected in the policy with offline protection 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. For more information on auto-learning requirements, see "config waf web-protection-profile autolearning-profile" on page 232.	No default.
credit-card-detection-threshold <instances_int>	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. 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.	No default.
cross-site-scripting {enable | disable}	Enable to detect cross-site scripting (XSS) attacks. Also configure cross-site-scripting-action {alert | alert_deny | redirect | send_403_forbidden}.	disable

Variable	Description	Default
`cross-site-scripting-action {alert | alert_deny | redirect | send_403_forbidden }`	Select the action that the FortiWeb unit will perform when it detects a cross-site scripting attack. • `alert`: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "config log disk" on page 44 • `alert_deny`: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "config log disk" on page 44. • `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 "config log disk" on page 51 and `redirect-url <redirect_fqdn>`. • `send_403_forbidden`: Reply with an HTTP 403 (Access Forbidden) error message and generate an alert and/or log message. For details, see "config log disk" on page 44. Attack log messages and *Alert Message Console* messages contain `DETECT_XSS_ATTACK` when this feature detects a possible cross-site scripting attack. **Note:** If an auto-learning profile will be selected in the policy with offline protection 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. For more information on auto-learning requirements, see "config waf web-protection-profile autolearning-profile" on page 232.	No default.
`cross-site-scripting-subtype {<xss_subtype>}`	Leave this field blank to enable all subtypes, or enter the names of a specific subtypes that you want to enable; one of: • `xss-signature-1` • `xss-signature-2` • `xss-signature-3` • `xss-signature-4` • `xss-signature-5` • `xss-signature-6` • `xss-signature-7` • `xss-signature-8` • `xss-signature-9`	No default.
`exception-name <server-protection-exception_name>`	Type the name of the server protection exception to use, if any.	No default.
`custom-protection-group <custom_protection_group_name>`	Type the name of the custom protection group to be used, if any.	No default.
`extended-sig-set {enable | disable}`	Select the amount of attack definitions that will be used, either: • `disable`: Use only attack definitions that normally do not cause false positives. This option is recommended for most cases. • `enable`: Use more attack definitions, including some special attack definitions that are usually not used. While this option can detect more attacks, it may also cause more false positives. When enabled, you can set one of three extended attack definition severities and corresponding trigger policies.	No default.
`basic-severity {Low | Medium | High}`	Enter the severity level you want FortiWeb to associate with the rule violation.	`High`
`basic-trigger <trigger-policy_name>`	Type the name of the trigger policy you want FortiWeb to apply when the rule severity level is met.	No default.

Variable	Description	Default
`enhanced-severity {Low | Medium | High}`	Enter the severity level you want FortiWeb to associate with the rule violation.	`High`
`enhanced-trigger <trigger-policy_name>`	Type the name of the trigger policy you want FortiWeb to apply when the rule severity level is met.	No default.
`full-severity {Low | Medium | High}`	Enter the severity level you want FortiWeb to associate with the rule violation.	`High`
`full-trigger <trigger-policy_name>`	Type the name of the trigger policy you want FortiWeb to apply when the rule severity level is met.	No default.
`information-disclosure {enable | disable}`	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. Also configure `information-disclosure-action {alert | alert_erase | redirect}`. 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.	`disable`
`information-disclosure-action {alert | alert_erase | redirect}`	Select which action the FortiWeb unit will take when it detects information disclosure. • `alert`: Do not cloak. Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see “config log disk” on page 44. • `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 “config log disk” on page 44. **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 “config log disk” on page 44 and `redirect-url <redirect_fqdn>`. Attack log messages and *Alert Message Console* messages contain `DETECT_RESPONSE_INFORMATION_DISCLOSURE` when this feature detects sensitive information. **Note:** If an auto-learning profile will be selected in the policy with offline protection 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. For more information on auto-learning requirements, see “config waf web-protection-profile autolearning-profile” on page 232.	

Variable	Description	Default
`information-disclosure-subtype {info_subtype>}`	Leave this field blank to omit all subtypes, or enter the names of one or more specific subtypes that you want to omit: • `application-not-available` • `asp-jsp-source-code-leakage` • `cf-information-leakage` • `cf-source-code-leakage` • `directory-listing` • `file-or-dir-names-leakage` • `iis-errors-leakage` • `iis-default-location` • `isa-server-existence-revealed` • `ms-doc-properties-leakage` • `php-information-leakage` • `php-source-code-leakage` • `statistics-pages-revealed` • `sql-errors-leakage` • `weblogic-info-disclosure` • `zope-information-leakage` • `http-retcode-4xx` • `http-retcode-5xx`	No default.
`sql-injection {enable | disable}`	Enable to detect SQL injection attacks. Also configure `sql-injection-action {alert | alert_deny | redirect | send_403_forbidden}`.	`disable`
`sql-injection-action {alert | alert_deny | redirect | send_403_forbidden }`	Select the action that the FortiWeb unit will perform when it detects a SQL injection attack. • `alert`: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "config log disk" on page 44. • `alert_deny`: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "config log disk" on page 44. • `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 "config log disk" on page 44 and `redirect-url <redirect_fqdn>`. • `send_403_forbidden`: Reply with an HTTP 403 (Access Forbidden) error message and generate an alert and/or log message. For details, see "config log disk" on page 44. Attack log messages and *Alert Message Console* messages contain `DETECT_SQL_INJECTION` when this feature detects a possible SQL injection attack. **Note:** If an auto-learning profile will be selected in the policy with offline protection 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. For more information on auto-learning requirements, see "config waf web-protection-profile autolearning-profile" on page 232	No default.
`sql-injection-subtype {<injectionsubtype>}`	Leave this field blank to omit all subtypes, or enter the name of a specific subtypes that you want to omit; one of • `sql-injection-1` • `sql-injection-2` • `sql-injection-3` • `sql-injection-4` • `sql-injection-5` • `sql-injection-6` • `sql-injection-7` • `sql-injection-8` • `sql-injection-9` • `sql-injection-10`	No default.

Server protection rule violations

Each server protection rule has settings to define an action, severity and trigger associated with a violation of the rule. The action, severity and trigger settings can be applied as required to ensure the violation is clearly identified and communicated.

The syntax for setting server protection rule action, severity and trigger is as follows:

```
config waf server-protection-rule
  edit <server-protection-rule_name>
    set <protection-rule-name>-action {alert | alert_deny | alert_erase |
       redirect | send_403_forbidden}
    set <protection-rule-name>-severity {High | Medium | Low}
    set <protection-rule-name>-trigger <trigger-policy-name>
  next
end
```

Variable	Description	Default
`<protection-rule-name>-action {alert | alert_deny | alert_erase | redirect | send_403_forbidden }`	Each server protection rule has a configurable "action" command (i.e. `common-exploits-action`), which defines what the FortiWeb unit does if the server protection rule is violated. The action varies by server protection rule. Refer to "config Syntax" on page 203 for specific action settings associated with each rule. •	`alert`
`<protection-rule-name>-severity {High | Medium | Low}`	Each server protection rule has a configurable "severity" command (i.e. `common-exploits-severity`). You can configure each violation type to be recorded and reported as either Low, Medium or High severity.	`High`
`<protection-rule-name>-trigger <trigger-policy-name>`	Each violation type has a configurable "trigger" command (i.e. `common-exploits-trigger`). When a violation occurs, the FortiWeb unit invokes the specified trigger. The trigger determines whether an alert is created and an email sent to predefined users and/or whether the violation log message is recorded in Syslog. For more information, see "config log trigger-policy" on page 66.	No default.

Example

This example configures a server protection rule that blocks all known common exploits, SQL injection, cross-site scripting, credit card disclosure, and information disclosure attacks. There are no subtypes specified, so all subtypes are blocked. Common exploits are defined as a medium-level severity and use a trigger policy that sends an email to predefined users when a violation occurs.

```
config waf server-protection-rule
  edit server_protection_rule1
    set common-exploits enable
    set common-exploits-action alert_deny
    set common-exploits-severity Medium
    set common-exploits-trigger trigger_policy1
    set credit-card-detection enable
    set credit-card-detection-action alert_deny
    set cross-site-scripting enable
    set cross-site-scripting-action alert_deny
    set information-disclosure enable
    set information-disclosure-action alert_deny
    set sql-injection enable
    set sql-injection-action alert_deny
```

```
    next
end
```

History

FortiWeb v3.2.0	New.
FortiWeb v4.0.0	Added fields `common-exploits-subtype`, `cross-site-scripting-subtype`, `information-disclosure-subtype`, and `sql-injection-subtype`. Allows you to individually enable or disable signatures in each category of attacks. Added fields `credit-card-detection`, `credit-card-detection-action`, `credit-card-detection-threshold`. Enables and configures credit card number disclosure prevention. Added `exception-name`. Configures which server protection exception to use, if any. Added `redirect` and `send_403_forbidden` options to `common-exploit-action`, `cross-site-scripting-action`, and `sql-injection-action` fields. Redirects attacks to the URL specified in the profile, or replies with an HTTP 403 (Forbidden) message, respectively. Renamed `common-exploits-rule` to `common-exploits-action`. Renamed `sql-injection-rule` to `sql-injection-action`. Renamed `mode` to `extended-sig-set`.
FortiWeb v4.0.2	Added `redirect` option to `information-disclosure-action` field. Redirects the request to the URL that you specify in the protection profile and generates an alert and/or log message.
FortiWeb v4.1	Added `custom-protection-group` option.
FortiWeb v4.1.1	Added severity and trigger options to each protection rule.
FortiWeb v4.2	Added Set statements `basic-severity`, `basic-trigger, enhanced-severity, enhanced-trigger, full-severity`, and `full-trigger` to work with the `extended sig-set`.

Related topics

- config waf server-protection-exception
- config waf web-protection-profile inline-protection
- config waf web-protection-profile offline-protection
- config system snmp community
- config waf custom-protection-group
- config log trigger-policy

waf start-pages

Use this command to configure start page rules.

When a start page group is selected in the inline protection profile, HTTP clients must begin from a valid start page in order to initiate a valid session.

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.

To apply start pages, select them within an inline protection profile. For details, see "config waf web-protection-profile inline-protection" on page 234.

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 "config server-policy allow-hosts" on page 71.

Use SNMP traps to notify you when a start page rule is enforced. For details, see "config system snmp community" on page 150.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config waf start-pages
  edit <start-page-rule_name>
    set action {alert  alert_deny | redirect | send_403_forbidden}
    set severity {Low | Medium | High}
    set trigger <trigger-policy_name>
    config start-page-list
      edit <entry_index>
        set host <allowed-hosts_name>
        set host-status {enable | disable}
        set request-file <url_str>
        set request-type {plain | regular}
        set default {yes | no}
      next
    end
  next
end
```

Variable	Description	Default
`<start-page-rule_name>`	Type the name of the start page rule.	No default.
`action {alert alert_deny | redirect | send_403_forbidden }`	Select one of the following actions that the FortiWeb unit will perform 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 "config log disk" on page 44. • `alert_deny`: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "config log disk" on page 44. • `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 "config log disk" on page 44.	No default.

Variable	Description	Default
`severity {Low | Medium | High}`	Enter the severity level you want FortiWeb to associate with the rule violation.	`Low`
`trigger <trigger-policy_name>`	Type the name of the trigger policy you want FortiWeb to associate with the rule violation.	No default.
`<entry_index>`	Type the index number of the individual entry in the list.	No default.
`host <allowed-hosts_name>`	Type the name of a protected host that the `Host:` field of an HTTP request must be in order to match the start page rule. This setting applies only if `host-status` is `enable`.	No default.
`host-status {enable | disable}`	Enable to apply this start page rule only to HTTP requests for specific web hosts. Also configure `host <allowed-hosts_name>`. Disable to match the start page rule based upon the other criteria, such as the URL, but regardless of the `Host:` field.	`disable`
`request-file <url_str>`	Depending on your selection in `request-type {plain | regular}`, type either: • 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 (/). • 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`. Do not include the name of the web host, such as `www.example.com`, which is configured separately in `host <allowed-hosts_name>`. **Note:** Regular expressions beginning with an exclamation point (`!`) are not supported. For information on language and regular expression matching, see the *FortiWeb Administration Guide*.	No default.
`request-type {plain | regular}`	Select whether `request-file <url_str>` will contain a literal URL (`plain`), or a regular expression designed to match multiple URLs (`regular`).	`plain`
`default {yes | no}`	Type `yes` to use the page as the default for HTTP requests that either: • do not specify a URL • do not specify the URL of a valid start page (only if you have selected `redirect` from `action`) Otherwise, type `no`.	`no`

Example

This example redirects clients to the default start page, /index.html, if clients request a page that is not one of the valid start pages (`/index.html` or `/cart/login.jsp`). Redirection will occur only if the request is destined for one of the virtual or real hosts defined in the protected hosts group named `example_com_hosts`.

```
config waf start-pages
  edit "start-page-rule1"
    edit 1
      set host "example_com"
      set host-status enable
      set request-file "/index.html"
      set default yes
    next
    edit 2
      set host "example_com_hosts"
      set host-status enable
      set request-file "/cart/login.jsp"
      set default no
    next
```

```
    next
end
```

History

FortiWeb v3.2.0	New.
FortiWeb v3.3.0	Field `request-file` now accepts regular expressions that do not begin with a slash (/) character.
FortiWeb v4.0.0	Added option `send_403_forbidden` to `action` field.
FortiWeb v4.2	Added Set statements for `severity` and `trigger`.

Related topics

- config server-policy allow-hosts
- config waf web-protection-profile inline-protection
- config system snmp community

waf url-access url-access-policy

Use this command to configure URL access policy group rules that define HTTP requests that will be allowed or denied.

To apply URL access policies, select them within an inline or offline protection profile. For details see, "config waf web-protection-profile inline-protection" on page 234 or "config waf web-protection-profile offline-protection" on page 239.

Use SNMP traps to notify you when a URL access rule is enforced. For details, see "config system snmp community" on page 150.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config waf url-access url-access-policy
  edit <url-access-policy-name>
    config rule
      edit <entry_index>
        set priority <priority_number>
        set url-access-rule-name <url-access-rule_name>
      next
    end
  next
end
```

Variable	Description	Default
`<url-access-policy-name>`	Type the name of the URL access policy.	No default
`<entry_index>`	Type the index number of the individual entry in the list.	No default.
`priority <priority_number>`	Type the number representing the priority of the rule in relation to other defined rules in the policy. Rules with lower priority numbers are applied first	No default
`url-access-rule-name <url-access-rule_name>`	Type the name of the predefined URL access rule to add to the policy.	No default.

Example

This example adds "URL Access Rule 1" to the policy and sets the "Blocked URL" to priority level 1.

```
config waf url-access url-access-policy
  edit "Url Access Policy 2"
    config rule
      edit 1
        set url-access-rule-name "URL Access Rule 1"
      next
      edit 2
        set priority 1
        set url-access-rule-name "Blocked URL"
      next
    next
  end
```

History

FortiWeb v4.1 New.

Related topics

- config waf web-protection-profile inline-protection
- config waf web-protection-profile offline-protection

waf url-access url-access-rule

Use this command to configure URL access rules that define HTTP requests that will be allowed or denied based on their host name and URL.

To apply URL access rules, select them within an inline or offline protection profile. For details see, “config waf web-protection-profile inline-protection” on page 234 or “config waf web-protection-profile offline-protection” on page 239.

URL access rules can also be grouped into URL access policies. For details see, ““config waf url-access url-access-policy” on page 223.

Use SNMP traps to notify you when a URL access rule is enforced. For details, see “config system snmp community” on page 150.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see “Permissions” on page 29.

Syntax

```
config waf url-access url-access-rule
  edit <url-access-rule_name>
    config match-condition
      edit <entry_index>
        set {reg-exp | reverse-match | type}
      next
    end
  next
end
```

Variable	Description	Default
`<url-access-rule_name>`	Type the name of the URL access rule.	No default
`<entry_index>`	Type the index number of the individual entry in the list.	No default.
`{reg-exp | reverse-match | type}`	Identify the type of matching to perform: • `reg-exp <string>` • `reverse-match {yes | no}` • `type {regex-expression | simple-string}` **Note:** Regular expressions beginning with an exclamation point (`!`) are not supported. Instead, use `reverse-match {yes | no}`.	No default

Example

This example defines the rules for URLs by setting a matching regular expression.

```
config waf url-access url-access-rule
  edit "Blocked URL"
    config match-condition
      edit 1
        set reg-exp "example.com"
      next
      edit 2
        set reg-exp "test.com"
      next
    end
  next
  edit "Allowed URL"
```

```
      config match-condition
        edit 1
          set reg-exp "example.com"
          set reverse-match yes
          set type regex-expression
        next
      end
    next
end
```

History

FortiWeb v4.1 New.

Related topics

- config waf web-protection-profile inline-protection
- config waf web-protection-profile offline-protection
- config waf url-access url-access-policy

waf url-rewrite url-rewrite-policy

Use this command to group URL rewrite rules.

Before you can configure a URL rewrite group, you must first configure any URL rewriting rules that you want to include. For details, see “config waf url-rewrite url-rewrite-rule” on page 228.

To apply a URL rewriting group, select it in an inline protection profile. For details, see “config waf web-protection-profile inline-protection” on page 234.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see “Permissions” on page 29.

Syntax

```
config waf url-rewrite url-rewrite-policy
  edit <url-rewrite-group_name>
    config rule
      edit <entry_index>
        set priority <priority_int>
        set [url-rewrite-rule-name <url-rewrite-rule_name>
        next
    end
  next
end
```

Variable	Description	Default
`<url-rewrite-group_name>`	Type the name of the URL rewriting rule group.	No default.
`<entry_index>`	Type the index number of the individual entry in the list.	No default.
`priority <priority_int>`	Type the order of evaluation for this rule in the group, starting from 0. To create an entry with the highest match priority, enter `0`. For lower-priority matches, enter larger numbers. **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. When the FortiWeb unit finds a matching rule, it applies the matching rule's specified actions to the connection.	No default.
`url-rewrite-rule-name <url-rewrite-rule_name>`	Type the name of an existing URL rewriting rule that you want to include in the group.	`disable`

History

FortiWeb v4.0.0 New.

Related topics

- config waf url-rewrite url-rewrite-rule
- config waf web-protection-profile inline-protection

waf url-rewrite url-rewrite-rule

Use this command to configure URL rewrite rules or to redirect requests.

URL rewriting rules can:

- rewrite the URL line in the HTTP header
- rewrite the `Referer:` field in the HTTP header
- redirect requests to another `Host:` name

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 will ***not*** be rewritten.

Note: URL rewrites are applicable only if the FortiWeb unit is operating in reverse proxy mode or either of the transparent modes for connections *without* SSL.

To apply a URL rewriting rule, you must add it to a group. For details, see “config waf url-rewrite url-rewrite-rule” on page 228.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see “Permissions” on page 29.

Syntax

```
config waf url-rewrite url-rewrite-rule
  edit <url-rewrite-rule_name>
    set action {403-forbidden | redirect | refer-rewrite | url-rewrite}
    set host {<server_fqdn> | <server_ipv4> | <host_pattern>}
    set host-status {enable | disable}
    set protocol {http | https}
    set protocol-status {enable | disable}
    set url <replacement_url>
    set url-status {enable | disable}
    set location <location>
    set referer-status {enable | disable}
    set referer <referer-url>
    set body_replace <string>
    config match-condition
      edit <entry_index>
        set is-essential {yes | no}
        set object {http-reference}
        set reg-exp <object_pattern>
        set reverse-match {yes | no}
      next
```

```
    end
  next
end
```

Variable	Description	Default
`<url-rewrite-rule_name>`	Type the name of the URL rewriting rule.	No default.
`action {403-forbidden | redirect | refer-rewrite | url-rewrite}`	Select either: • `403-forbidden`: Send a 403 (Forbidden) response to the client. • `redirect`: Send a 302 (Moved Temporarily) response to the client, with a new `Location:` field in the HTTP header. • `refer-rewrite`: Rewrite `Referer:` field in HTTP header. • `url-rewrite`: Rewrite both the `Host:` and request URL fields in HTTP header.	`url-rewrite`
`host {<server_fqdn> | <server_ipv4> | <host_pattern>}`	Type the name of the host, such as `store.example.com`, to which the request will be redirected. This field supports back references such as `$0` to the parts of the original request that matched any capture groups that you entered in `reg-exp <object_pattern>` for each object in the condition table. (A capture group is a regular expression, or part of one, surrounded in parentheses.) Use $***n*** (0 <= ***n*** <= 9) to invoke a substring, where ***n*** is the order of appearance of the regular expression, from left to right, from outside to inside, then from top to bottom. For example, regular expressions in the condition table in this order: (a)(b)(c(d))(e) (f) would result in invokable variables with the following values: • `$0`: a • `$1`: b • `$2`: cd • `$3`: d • `$4`: e • `$5`: f	No default.
`host-status {enable | disable}`	Enable to rewrite the `Host:` field or host name part of the `Referer:` field. If this option is available but you disable it, the FortiWeb unit will preserve the value from the client's request when rewriting it.	`disable`
`protocol {http | https}`	Select the protocol to use in the URL when redirecting or rewriting the `Referer:` field in the HTTP header. This setting applies only if `protocol-status` is `enable`.	`http`
`protocol-status {enable | disable}`	Enable to rewrite the protocol part of the request URL or `Referer:` field. This option is available only if `action` is `url-rewrite` or `refer-rewrite`. If this option is available but you disable it, the FortiWeb unit will preserve the value from the client's request when rewriting it.	`disable`
`url <replacement_url>`	Type the string, such as `/catalog/item1`, that will replace the request URL. Do not include the name of the web host, such as `www.example.com`, nor the protocol, which are configured separately in `host {<server_fqdn> | <server_ipv4> | <host_pattern>}` and `protocol {http | https}`, respectively. Like `host`, this field supports back references such as `$0` to the parts `reg-exp <object_pattern>` for each object in the condition table. For an example, see the *FortiWeb Administration Guide*.	No default.
`url-status {enable | disable}`	Enable to rewrite the URL part of the request URL or `Referer:` field. If you disable this option, the FortiWeb unit will preserve the value from the client's request when rewriting it.	`disable`
`location <location>`	The replacement value for the location field in the HTTP header for the 302 response.	No default.

Variable	Description	Default
`referer-status {enable | disable}`	Display the status of the URL referer.	`disable`
`referer <referer-url>`	The replacement value for the referer field in the HTML header.	No default.
`body_replace <string>`	Type the replacement value for the specific HTTP content in the body of responses. For an example, see “URL rewriting examples”.	No default.
`<entry_index>`	Type the index number of the individual entry in the list.	No default.
`is-essential {yes | no}`	Select what to do if there is no `Referer:` field, either: • `no`: Meet this condition. • `yes`: Do not meet this condition. 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. This option appears only if `object` is `http-reference`.	`yes`
`object {http-reference}`	Select which part of the HTTP request to test for a match: • `http-host` • `http-url` • `http-reference` (the `Referer:` field) If the request must match 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.	`http-reference`
`reg-exp <object_pattern>`	Depending on your selection in `object {http-reference}` and `reverse-match {yes | no}`, type a regular expression that defines either all matching or all non-matching `Host:` fields, URLs, or `Referer:` fields. Then, also configure `reverse-match {yes | no}`. For example, for the URL rewriting rule to match all URLs that begin with `/wordpress`, you could enter `^/wordpress`, then, in `reverse-match {yes | no}`, select `no`. The pattern is ***not*** required to begin with a slash (/). When you have finished typing the regular expression, click the >> (test) button. A pop-up window appears 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. **Note:** Regular expressions beginning with an exclamation point (`!`) are not supported. Instead, use `reverse-match {yes | no}`.	No default.
`reverse-match {yes | no}`	Indicate how to use `reg-exp <object_pattern>` when determining whether or not this URL rewriting condition has been met. • `no`: If the regular expression ***does*** match the request object, the condition is met. • `yes`: If the regular expression does ***not*** match the request object, the condition is met. The effect is equivalent to preceding a regular expression with an exclamation point (`!`). If all conditions are met, the FortiWeb unit will do your selected `action`.	`no`

History

FortiWeb v4.0.0	New.
FortiWeb v4.1	Added options for rewriting location, referer and referer status.
FortiWeb v4.2	Set statement `body_replace` was added.

Related topics

- config waf url-rewrite url-rewrite-rule

waf web-custom-robot

Use this command to configure custom robot groups.

Instead of using groups that reference predefined 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 rate limiting by robot control sensors. If your organization has written its own search indexer, or uses a third-party spider or link checker not identified in the predefined list, you may need to write a custom robot signature.

To apply custom robot exemptions, select a set of custom robot signatures in a robot control sensor. For details, see "config waf robot-control" on page 205.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config waf web-custom-robot
  edit <custom-robot-group_name>
    config list
      edit <entry_index>
        set expression <signature_pattern>
        set type-name <robot-name_str>
      next
    end
  next
end
```

Variable	Description	Default
`<custom-robot-group_name>`	Type the name of the custom robot group.	No default.
`<entry_index>`	Type the index number of the individual entry in the list.	No default.
`expression <signature_pattern>`	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. For example, if a custom robot causes either: • `User-Agent: happy-spider` • `User-Agent: happy-spider2.0`. but ***not*** `User-Agent: baiduspider`, you would write a regular expression to match the first two cases, but that would not match the third.	No default.
`type-name <robot-name_str>`	Type a name, such as `Intranet-Indexer`, for the signature. This name will appear in log messages where the signature is used to detect a robot.	No default.

History

FortiWeb v4.0.0 New.

Related topics

- config waf robot-control

waf web-protection-profile autolearning-profile

Use this command to configure 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. 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 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 or offline protection profiles.

Auto-learning profiles are designed to be used in conjunction with a protection or detection 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 a protection or detection 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.

To apply auto-learning profiles, select them within a policy. For details, see ""config waf web-protection-profile offline-protection" on page 239. Once applied in a policy, the FortiWeb unit will collect data and generate a report from it. For details, see the *FortiWeb Administration Guide*.

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 "config server-policy pattern data-type-group" on page 87)
- a suspicious URL rule group (see "config server-policy pattern suspicious-url-rule" on page 90)

Tip: Alternatively, you could generate an auto-learning profile and its required components, and then modify them. For details, see the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `learngrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config waf web-protection-profile autolearning-profile
  edit <auto-learning-profile_name>
    set data-type-group <data-type-group_name>
    set suspicious-url-rule <suspicious-url-rule-group_name>
    set attack-count-threshold <count_int>
    set attack-percent-range <percent_int>
    set application-policy <policy_name>
  next
end
```

Variable	Description	Default
`<auto-learning-profile_name>`	Type the name of the auto-learning profile.	No default.
`data-type-group <data-type-group_name>`	Type the name of the data type group for the profile to use. The auto-learning profile will learn about the names, length, and required presence of these types of parameter inputs as described in the data type group.	No default.
`suspicious-url-rule <suspicious-url-rule-group_name>`	Type the name of a suspicious URL rule group. 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.	No default.
`attack-count-threshold <count_int>`	Type the integer representing the threshold over which the auto-learning profile adds the attack to the server protection rules.	0
`attack-percent-range <percent_int>`	Type the integer representing the threshold of the percentage of attacks to total hits over which the auto-learning profile adds the attack to the server protection exceptions.	0
`application-policy <policy_name>`	Type the name of a custom application policy. See “config server-policy custom-application application-policy” on page 74.	No default.

History

FortiWeb v3.2.1 New.

FortiWeb v4.1 Added attack-count-threshold and attack-percent-range options.

FortiWeb v4.2 Added Set statement `application-policy` .

Related topics

- config server-policy pattern data-type-group
- config server-policy pattern suspicious-url-rule
- config waf web-protection-profile inline-protection
- config server-policy policy
- config system settings

waf web-protection-profile inline-protection

Use this command to configure inline protection profiles.

Inline protection profiles are a set of attack protection settings. The FortiWeb unit applies the profile when a connection matches a server policy that includes the protection profile. You can use inline protection profiles in server policies for any mode except offline protection.

To apply protection profiles, select them within a server policy. For details, see “config server-policy policy” on page 92.

Before configuring an inline protection profile, first configure any of the following that you want to include in the profile:

- protected hosts (see“config server-policy allow-hosts” on page 71)
- a parameter validation rule (see “config waf parameter-validation-rule” on page 203)
- a parameter restriction constraint (see “config waf http-protocol-parameter-restriction” on page 190)
- start pages (see “config waf start-pages” on page 220)
- a URL access policy (see “config waf url-access url-access-policy” on page 223
- a brute force login attack sensor (see “config waf brute-force-login” on page 170)
- a robot control sensor (see “config waf robot-control” on page 205)
- an allowed method exception (see “config waf allow-method-exceptions” on page 167)
- a hidden field rule group (see “config waf hidden-fields-protection” on page 179)
- an authentication policy (see “config waf http-authen http-authen-policy” on page 183)
- a listed of trusted and black-listed IPs (see “config waf ip-list” on page 198)
- a page access rule (see “config waf page-access-rule” on page 200)
- a server protection rule (see “config waf server-protection-rule” on page 212)
- a file upload restriction policy (see “config waf file-upload-restriction-policy” on page 176)

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see “Permissions” on page 29.

Syntax

```
config waf web-protection-profile inline-protection
  edit <inline-protection-profile_name>
    set allow-method-policy <allow-method-policy_name>
    set amf3-protocol-detection {enable | disable}
    set brute-force-login <brute-force-login-sensor_name>
    set cookie-poison {enable | disable}
    set cookie-poison-action {alert | alert_deny | remove_cookie}
    set cookie-poison-severity {High | Medium | Low}
    set cookie-poison-trigger <trigger-policy_name>
    set file-upload-policy <file-upload-policy_name>
    set hidden-fields-protection <hidden-field-rule-group_name>
    set http-authen-policy <http-auth_name>
    set http-conversion {enable | disable}
    set http-protocol-parameter-restriction <http-constraint_name>
    set http-session-management {enable | disable}
    set http-session-timeout <seconds_int>
    set ip-list-policy <ip-list-policy_name>
    set is-default-config {yes | no}
    set page-access-rule <page-access-rule_name>
```

```
    set parameter-validation-rule <parameter-validator_name>
    set redirect-url <redirect_fqdn>
    set rdt-reason {enable | disable}
    set robot-control <robot-control-sensor_name>
    set server-protection-rule <server-protection-rule_name>
    set start-pages <start-page-rule_name>
    set url-rewrite-policy <url-rewrite-group_name>
    set url-access-policy <url-access-policy_name>
    set x-forwarded-for {enable | disable}
  next
end
```

Variable	Description	Default
`<inline-protection-profile_name>`	Type the name of the inline protection profile.	No default.
`allow-method-policy <allow-method-policy_name>`	Type the name of an allowed method policy. See "config waf allow-method-policy" on page 169. The policy can contain exceptions and request methods.	No default.
`amf3-protocol-detection {enable | disable}`	Enable to scan requests that use action message format 3.0 (AMF3) for • cross-site scripting (XSS) attacks • SQL injection attacks • common exploits if you have enabled those in `server-protection-rule <server-protection-rule_name>`. AMF3 is a binary format that Adobe Flash clients can use to send input to server-side software. **Caution:** To scan for attacks or enforce input rules on AMF3, you ***must*** enable this option. Failure to enable the option will make the FortiWeb unit unable to scan AMF3 requests for attacks.	`disable`
`brute-force-login <brute-force-login-sensor_name>`	Type the name of a brute force login attack sensor. See "config waf brute-force-login" on page 170. Attack log messages contain `DETECT_BRUTE_FORCE_LOGIN` when this feature detects a brute force login attack.	No default.
`cookie-poison {enable | disable}`	Enable to detect cookie poisoning. 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.	`disable`
`cookie-poison-action {alert | alert_deny | remove_cookie}`	Select one of the following actions that the FortiWeb unit will perform when it detects cookie poisoning: • `alert`: Accept the connection and generate an alert and/or log message. • `alert_deny`: Block the connection and generate an alert and/or log message. • `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 "config log disk" on page 44.	No default.
`cookie-poison-severity {High | Medium | Low}`	Enter the severity level you want FortiWeb to associate with the profile violation.	`High`

Variable	Description	Default
`cookie-poison-trigger <trigger-policy_name>`	Type the name of the trigger policy you want FortiWeb to associate with the profile violation.	No default.
`file-upload-policy <file-upload-policy_name>`	Type the name of a file upload restriction policy. See "config waf file-upload-restriction-policy" on page 176.	No default.
`hidden-fields-protection <hidden-field-rule-group_name>`	Type the name of a hidden field rule group that you want to apply, if any. See "config waf hidden-fields-protection" on page 179.	No default.
`http-authen-policy <http-auth_name>`	Type the name of an HTTP authentication policy, if any, that will be applied to matching HTTP requests. See "config waf http-authen http-authen-policy" on page 183. If the HTTP client fails to authenticate, it will receive an HTTP 403 (Access Forbidden) error message.	No default.
`http-conversion {enable | disable}`	Enable this to: • 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. • 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. 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. **Note:** Do ***not*** enable this option if the physical server has multiple virtual hosts. **Note:** The FortiWeb unit does not support this option if the operating mode is true transparent proxy with HTTPS or transparent inspection.	`disable`
`http-protocol-parameter-restriction <http-constraint_name>`	Type the name of an HTTP protocol constraint that you want to apply, if any. See "config waf http-protocol-parameter-restriction" on page 190. Attack log 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.	No default.
`http-session-management {enable | disable}`	Enable to track the states of HTTP sessions. Also configure `http-session-timeout <seconds_int>`. This feature requires that the client support cookies. **Note:** You ***must*** enable this option: • to enforce the start page rule, page access rule, and hidden fields rule, if any of those are selected. • 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 "config log attack-log" on page 40 and "config log memory" on page 52. **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.	`disable`
`http-session-timeout <seconds_int>`	Type the HTTP session timeout in seconds. This setting is available only if `http-session-management` is `enable`.	`1200`
`ip-list-policy <ip-list-policy_name>`	Enter the name of a waf ip-list policy. See "config waf ip-list" on page 198.	No default.
`is-default-config {yes | no}`	Enter yes to set this configuration as the default specifications for new inline protection rules.	`no`

Variable	Description	Default
`page-access-rule <page-access-rule_name>`	Type the name of a page access rule. See “config waf page-access-rule” on page 200. Attack log 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.	No default.
`parameter-validation-rule <parameter-validator_name>`	Type the name of a parameter validation rule. See “config waf parameter-validation-rule” on page 203. Attack log messages contain `DETECT_PARAM_RULE_FAILED` when this feature detects a parameter rule violation.	No default.
`redirect-url <redirect_fqdn>`	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. For example, you could enter `www.example.com/products/`. 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.	No default.
`rdt-reason {enable | disable}`	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 <redirect_fqdn>`. 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). **Caution**: If you specify a redirect URL that is protected by the FortiWeb unit, you should enable this option to prevent infinite redirect loops.	No default
`robot-control <robot-control-sensor_name>`	Type the name of a robot control sensor, if any. See “config waf robot-control” on page 205. Attack log messages contain `DETECT_MALICIOUS_ROBOT` when this feature detects a misbehaving robot or any other HTTP client that exceeds the rate limit.	No default.
`server-protection-rule <server-protection-rule_name>`	Type the name of a server protection rule. See “config waf server-protection-rule” on page 212. Attack log messages for this feature vary by which type of attack was detected. For a list, see “config waf server-protection-rule” on page 212.	No default.
`start-pages <start-page-rule_name>`	Type the name of a start page rule. See “config waf start-pages” on page 220. Attack log messages contain `DETECT_START_PAGE_FAILED` when this feature detects a start page violation. This setting is available only if `http-session-management` is `enable`.	No default.
`url-rewrite-policy <url-rewrite-group_name>`	Type the name of a URL rewriting rule set, if any, that will be applied to matching HTTP requests. See “config waf url-access url-access-policy” on page 223.	No default.
`url-access-policy <url-access-policy_name>`	Type the name of a url access policy. See “config waf url-access url-access-policy” on page 223.	No default.
`x-forwarded-for {enable | disable}`	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: • Header absent: Add the header, using the source IP address of the connection. • 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. 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.	`disable`

History

FortiWeb v3.2.0	New.
FortiWeb v3.3.0	New field `hidden-fields-protection`. Renamed the `allow-request` option `track` to `trace`. New option `put`. New field x-forwarded-for. Enables inclusion of the `X-Forwarded-For:` HTTP header on connections forwarded from the FortiWeb unit to your web servers.
FortiWeb v4.0.0	New field `amf3-protocol-detection`. Enables scanning of AMF3 (Flash) objects. New field `redirect-url`. Configures a URL to which violation traffic will be redirected. New field `http-authen-policy`. Selects which HTTP authentication policy will be applied. New field `http-protocol-parameter-restriction`. Constrains the length of parts of an HTTP datagram.
FortiWeb v4.0.2	New field `rdt-reason`.Adds a reason for redirection as a parameter in the URL.
FortiWeb v4.1	New `url-access-policy` added to replace (remove) white-page rule and black-page-rule.
FortiWeb v4.2	Set statements `allow-method-policy` (which replaces `allow-request` and `allow-method-exceptions`), `cookie-poison-severity`, `cookie-poison-trigger`, `file-upload-policy`, and `ip-list-policy` were added.

Related topics

- config server-policy policy
- config server-policy allow-hosts
- config system snmp community
- config waf server-protection-rule
- config waf start-pages
- config waf page-access-rule
- config waf parameter-validation-rule
- config waf brute-force-login
- config waf hidden-fields-protection
- config waf http-authen http-authen-policy
- config waf http-protocol-parameter-restriction
- config waf url-access url-access-policy
- config waf robot-control
- config waf allow-method-exceptions

waf web-protection-profile offline-protection

Use this command to configure offline protection profiles.

Detection 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 protection profiles, a detection profile is designed for use in offline protection mode. Detection 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 detection profile to log only and not block attacks in order to gather complete session statistics for the auto-learning feature. As a result, detection profiles can only be selected in policies whose `deployment-mode` is `offline-detection`, and those policies will only be used by the FortiWeb unit when its operation mode is `offline-detection`.

Unlike inline protection profiles, offline protection profiles do not support HTTP conversion, cookie poisoning detection, start page rules, and page access rules.

To apply detection profiles, select them within a server policy. For details, see “config server-policy policy” on page 92.

Before configuring an offline protection profile, first configure any of the following that you want to include in the profile:

- a file upload restriction policy (see “config waf file-upload-restriction-policy” on page 176)
- a server protection rule (see “config waf server-protection-rule” on page 212)
- a listed of trusted and black-listed IPs (see “config waf ip-list” on page 198)
- a parameter validation rule (see “config waf parameter-validation-rule” on page 203)
- a URL access policy (see “config waf url-access url-access-policy” on page 223
- a robot control sensor (see “config waf robot-control” on page 205)
- an allowed method exception (see “config waf allow-method-exceptions” on page 167)

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see “Permissions” on page 29.

Syntax

```
config waf web-protection-profile offline-protection
  edit <offline-protection-profile_name>
    set allow-method-policy <allow-method-policy_name>
    set amf3-protocol-detection {enable | disable}
    set file-upload-policy <file-upload-policy_name>
    set http-session-keyword <key_str>
    set http-session-management {enable | disable}
    set http-session-timeout <seconds_int>
    set ip-list-policy <ip-list-policy_name>
    set is-default-config {yes | no}
    set parameter-validation-rule <parameter-validator_name>
    set robot-control <robot-control-sensor_name>
    set server-protection-rule <server-protection-rule_name>
    set url-access-policy <url-access-policy_name>
  next
end
```

Variable	Description	Default
`<offline-protection-profile_name>`	Type the name of the offline protection profile.	No default.
`allow-method-policy <allow-method-policy_name>`	Type the name of an allowed method policy. See "config waf allow-method-policy" on page 169. The policy can contain exceptions and allowed connections.	No default.
`amf3-protocol-detection {enable | disable}`	Enable to be able to scan requests that use action message format 3.0 (AMF3) for • cross-site scripting (XSS) attacks • SQL injection attacks • common exploits if you have enabled those in your selected `server-protection-rule <server-protection-rule_name>`. AMF3 is a binary format that can be used by Adobe Flash clients to send input to server-side software. **Caution:** To scan for attacks or enforce input rules on AMF3, you ***must*** enable this option. Failure to enable the option makes the FortiWeb unit unable to scan AMF3 requests for attacks.	`disable`
`file-upload-policy <file-upload-policy_name>`	Type the name of a file upload restriction policy. See "config waf file-upload-restriction-policy" on page 176.	No default.
`http-session-keyword <key_str>`	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`. This setting is available only if `http-session-management` is `enable`.	No default.
`http-session-management {enable | disable}`	Enable to track the states of HTTP sessions, which is required if you will select an auto-learning profile in the policy with this offline protection profile. Also configure `http-session-timeout <seconds_int>`. This feature requires that the client support cookies. **Note:** You ***must*** enable this option 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 "config log attack-log" on page 40 and "config log memory" on page 52.	`disable`
`http-session-timeout <seconds_int>`	Type the HTTP session timeout in seconds. This setting is available only if `http-session-management` is `enable`.	`1200`
`ip-list-policy <ip-list-policy_name>`	Enter the name of a trusted and black list IP policy. See "config waf ip-list" on page 198.	No default.
`is-default-config {yes | no}`	Enter yes to set this configuration as the default.	`no`
`parameter-validation-rule <parameter-validator_name>`	Type the name of a parameter validation rule. See "config waf parameter-validation-rule" on page 203.	No default.
`robot-control <robot-control-sensor_name>`	Type the name of a robot control sensor. See "config waf robot-control" on page 205.	No default.

Variable	Description	Default
`server-protection-rule <server-protection-rule_name>`	Type the name of a server protection rule. See “config waf server-protection-rule” on page 212.	No default.
`url-access-policy <url-access-policy_name>`	Type the name of a URL access policy. See “config waf url-access url-access-policy” on page 223.	No default.

History

FortiWeb v3.2.0	New.
FortiWeb v3.3.0	Renamed the `allow-request` option `track` to `trace`. New option `put`. New field `http-session-keyword`. Configures which HTTP header, if other than `Session-Id`:, will be used to track HTTP sessions.
FortiWeb v4.0.0	New field `amf3-protocol-detection`. Enables scanning of AMF3 (Flash) objects.
FortiWeb v4.1	New url-access policy added to replace (remove) white-page rule and black-page-rule.
FortiWeb v4.2	Set statements `allow-method-policy` (which replaces `allow-request` and `allow-method-exceptions`), `file-upload-policy`, and `ip-list-policy` were added.

Related topics

- config server-policy policy
- config waf server-protection-rulereferer
- config waf parameter-validation-rule
- config waf url-access url-access-rule
- config waf robot-control
- config waf allow-method-exceptions
- config system settings

waf web-robot

Use this command to configure groups of predefined robot signatures.

To apply robot groups, select them in the robot control sensor. For details, see “config waf robot-control” on page 205.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see “Permissions” on page 29.

Syntax

```
config waf web-robot
  edit <robot-group_name>
    config list
      edit <entry_index>
        set robot {robot_type}
      next
    end
  next
end
```

Variable	Description	Default
`<robot-group_name>`	Type the name of the robot group.	No default.
`<entry_index>`	Type the index number of the individual entry in the list.	No default.
`robot {robot_type}`	Type one name of a well-known robot that you want to add to the group. Allowed values are: `alltheweb`, `askjeeves`, `baidu`, `bing`, `excite`, `google`, `inktomi`, `looksmart`, `lycos`, `msn`, `scooter`, `teoma`, `wisenut`, `yahoo`.	No default.

Example

For an example, see “config waf robot-control” on page 205.

History

FortiWeb v3.3.2 New.

Related topics

- config waf robot-control

wvs policy

Use this command to define a web vulnerability scan policy. The policy enables you to set the frequency of the vulnerability scan, schedule the scan, and choose a format for the scan report. The policy also enables you to select an email policy that determines who receives the scan report.

Before you can complete a web vulnerability scan policy, you must first configure a scan profile using the FortiWeb web-based manager and a scan schedule using either the web-based manager or the CLI command config wvs schedule.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wvsgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config wvs policy
  edit <wvs-policy_name>
    set type {runonce | schedule}
    set schedule <wvs-schedule_name>
    set profile <vws-profile_name>
    set email <email-policy_name>
    set report_format {html mht pdf rtf text}
    set runtime <int>
  next
end
```

Variable	Description	Default
`<wvs-policy_name>`	Type the name of a new or existing web vulnerability scan policy.	No default.
`type {runonce | schedule}`	Enter `runonce` to run the scan immediately when you complete the policy. Enter `schedule` to have the scan run on a schedule set by the *schedule* setting.	`runonce`
`schedule <wvs-schedule_name>`	Type the name of an existing web vulnerability scan schedule. This setting is not needed if *type* is set to `runonce`.	No default.
`profile <vws-profile_name>`	Type the name of an existing web vulnerability scan profile.	No default.
`email <email-policy_name>`	Type the name of an existing email policy. When the scan completes, the FortiWeb unit will send email in the specified format to applicable addresses in the policy.	No default.
`report_format {html mht pdf rtf text}`	Type one or more formats for the email scan report.	No default.

`runtime <int>`	FortiWeb keeps track of how often the scan runs. To see that value, enter
	`show runtime`
	To reset the value to zero, enter
	`set runtime 0`
		No default.

Example

The following example defines a recurring vulnerability scan with email report output in RTF and text format.

```
config wvs policy
  edit "wvs-policy1"
    set type schedule
    set schedule "wvs-schedule1"
```

```
    set report_format rtf text
    set profile "wvs-profile1"
    set email "EmailPolicy1"
  next
end
```

History

FortiWeb v4.2 New.

Related topics

- config wvs profile
- config wvs schedule

wvs profile

A web vulnerability scan (WVS) profile defines the web server to scan, as well as the specific vulnerabilities to scan for. The WVS profiles are associated with WVS policies, which determine when to perform the scan and how to publish the results of the scan defined by the profile.

The CLI provides the *wvs profile* command to let you get or show existing profile names. To create the actual profile, you must use the FortiWeb web-based manager.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wvsgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config wvs profile
  show | get
end
```

History

FortiWeb v4.2 New.

Related topics

- config wvs policy
- config wvs schedule

wvs schedule

Use this command to schedule a web vulnerability scan.

Vulnerability scanning can detect known vulnerabilities on your web servers and web applications, helping you to design protection profiles. Vulnerability scans start from an initial directory, then scan for vulnerabilities in web pages located in the same directory or subdirectory as the initial URL.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wvsgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config wvs schedule
  edit <schedule_name>
    set type {recurring | onetime}
    set date <hh:mm> <yyyy/mm/dd>
    set time <hh:mm>
    set wday <day-list>
  next
end
```

Variable	Description	Default
`<schedule_name>`	Type the name of an existing or new WVS schedule.	No default.
`type {recurring | onetime}`	Enter the interval for the vulnerability scan: `recurring` or `onetime` .	`onetime`
`date <hh:mm> <yyyy/mm/dd>`	For a one-time web vulnerability scan only, enter the time (24-hour clock) and date for the scan to run. Year range is 2001-2050. This only applies if *type* is set to `onetime`.	No default
`time <hh:mm>`	Specify the time the vulnerability scan is to be performed based on a 24-hour clock. This only applies if *type* is set to `recurring`.	No default.
`wday <day-list>`	For a recurring scan only, enter one or more days of the week the scan is to be performed. This only applies if *type* is set to `recurring`. Spell the full name of each day and use an initial capital letter: for example, `Wednesday`.	No default.

Example

The following example schedules a recurring vulnerability scan to run every Sunday and Thursday at 01:00.

```
config wvs schedule
  edit "WVS-schedule1"
    set type recurring
    set time 01:00
    set wday Sunday Thursday
  next
end
```

History

FortiWeb v4.2 New.

Related topics

- config wvs profile
- config wvs policy

xml-protection filter-rule

Use this command to configure XML content filter rules.

Content filter rules contain one or more individual rules that either accept or block and/or log specific XML content that matches their XPath expression, based upon their client IP address, time of the request, or content.

To apply content filter rules, select them in an XML protection profile. For details, see “config xml-protection xml-protection-profile” on page 260.

Before configuring a content filter rule, first create either a schedule if you want it to be applicable only during certain times. For details, see “config xml-protection period-time onetime” on page 254 or “config xml-protection period-time recurring” on page 255.

Use SNMP traps to notify you when a filter rule is enforced. For details, see “config system snmp community” on page 150.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `xmlgrp` area. For more information, see “Permissions” on page 29.

Syntax

```
config xml-protection filter-rule
  edit <content-filter_name>
    set status {enable | disable}
    set comment <comment_str>
    config rule-list
      edit <entry_index>
        set action {accept | alert | alert_deny | deny}
        set ip-address <ipv4-range_str>
        set period-time <schedule_name>
        set priority <priority_int>
        set xpath-expression <xpath_str>
      next
    end
  next
end
```

Variable	Description	Default
`<content-filter_name>`	Type the name of the content filter.	No default.
`status {enable | disable}`	Enable to apply the content filter rule. **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 “config xml-protection xml-protection-profile” on page 260.	No default.
`comment <comment_str>`	Type a description or other comment. If the comment is more than one word, surround the words with quotes (').	No default.
`<entry_index>`	Type the index number for the individual entry.	No default.

Variable	Description	Default
`action {accept | alert | alert_deny | deny}`	Select the action that the FortiWeb unit will perform when content matches `xpath-expression`. For details on how `action` interacts with `priority` to determine which content filter rules are applied, see the *FortiWeb Administration Guide*. • `accept`: Accept the connection. • `alert`: Accept the connection and generate an alert and/or log message. • `alert_deny`: Block the connection and generate an alert and/or log message. • `deny`: Block the connection. For more information on logging and alerts, see "config log disk" on page 44.	`accept`
`ip-address <ipv4-range_str>`	If this content filter should ***not*** apply to all IP addresses, enter a client IP address or IP address range.	No default.
`period-time <schedule_name>`	Type the name of the schedule that defines when to apply this content filter.	No default.
`priority <priority_int>`	Type the order of evaluation for this content filter, starting from 0. The priority value must be unique for this individual entry in the content filter. To enter a content filter with the highest match priority, enter `0`. For lower-priority matches, enter larger numbers. **Note:** Content filter rule order affects content filter rule matching and behavior. For details, see the *FortiWeb Administration Guide*.	No default.
`xpath-expression <xpath_str>`	Type an XPath expression that matches web service content to which the `action` will be applied. The maximum length of the expression is 1000 characters.	No default.

Example

This example blocks access by all client IP addresses, at all times, to items in a catalog whose status attribute has the value "hidden". The example blocks attempts to access this restricted access and logs the attempt, but allows access to all other content.

The restriction is evaluated first because its priority number is the smallest; remaining content is subject to the content filter that accepts everything. (The index number is only for entry identification purposes, and does not affect order of evaluation.)

If the priority values were switched, the first rule, which accepts all content, would always be matched and applied before the restriction, and therefore the restriction would never be applied. For more information on the interaction of the action and match evaluation order, see the *FortiWeb Administration Guide*.

```
config xml-protection filter-rule
  edit "content_filter1"
    set comment "Test XML filter rule"
      config rule-list
        edit 1
          set priority 1
          set ip-address ""
          set period-time ""
          set xpath-expression "//*"
          set action accept
      next
        edit 2
          set priority 0
          set ip-address ""
          set period-time ""
          set xpath-expression "//soap-env:Body/catalog/item[@status=hidden]"
```

```
            set action alert_deny
          next
        end
      set status enable
    next
end
```

History

FortiWeb v3.2.0 New.

Related topics

- config xml-protection period-time onetime
- config xml-protection period-time recurring
- config xml-protection xml-protection-profile
- config system snmp community

xml-protection intrusion-prevention-rule

Use this command to configure intrusion prevention rules.

Intrusion prevention rules define data constraints for XML elements, enabling you to prevent someone from using element depths, data types and lengths to execute attacks such as oversized payloads, recursive payloads, and buffer overflows.

To apply intrusion prevention rules, select them in an XML protection profile. For details, see "config xml-protection xml-protection-profile" on page 260.

Use SNMP traps to notify you when an intrusion prevention rule is enforced. For details, see "config system snmp community" on page 150.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `xmlgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config xml-protection intrusion-prevention-rule
  edit <intrusion-prevention-rule_name>
    set status {enable | disable}
    set comment <comment_str>
    set allowDTDs {enable | disable}
    set maxAttrValueLength <int>
    set maxAttrs <int>
    set maxAttrsPerElem <int>
    set maxCDataLength <int>
    set maxCDatas <int>
    set maxCharRefs <int>
    set maxElemDepth <int>
    set maxElems <int>
    set maxGenEntityRefs <int>
    set maxNameLength <int>
    set maxNamespaceDecls <int>
    set maxNamespaceDeclsPerElem <int>
    set maxPIs <int>
    set maxTextNodeLength <int>
    set maxTextNodeRatio <int>
    set maxTextNodes <int>
  next
end
```

Variable	Description	Default
`<intrusion-prevention-rule_name>`	Type the name of the intrusion prevention rule.	No default.
`status {enable | disable}`	Enable to apply the intrusion prevention rule when required by an XML protection profile that uses it.	`enable`
`comment <comment_str>`	Type a description or other comment. If the comment is more than one word, surround the comment with quotes (').	No default.
`allowDTDs {enable | disable}`	Enable to allow use of document type definitions (DTDs). Unlike W3C XML schema scanning, DTD scanning is currently not supported, and therefore inclusion of DTDs can only be categorically allowed or denied.	`disable`

Variable	Description	Default
`maxAttrValueLength <int>`	Type the maximum length of the value to allow for any attribute of any XML element.	`0`
`maxAttrs <int>`	Type the maximum number of attributes to allow in a single request.	`0`
`maxAttrsPerElem <int>`	Type the maximum number of attributes to allow for any XML element.	`0`
`maxCDataLength <int>`	Type the maximum length of the value to allow for any character data (CDATA) section in a single request.	`0`
`maxCDatas <int>`	Type the maximum number of character data (CDATA) section to allow in a single request.	`0`
`maxCharRefs <int>`	Type the maximum number of character entity references to allow in a single request.	`0`
`maxElemDepth <int>`	Type the maximum depth of XML elements to allow in the tree of a single request.	`0`
`maxElems <int>`	Type the maximum number of XML elements to allow in a single request.	`0`
`maxGenEntityRefs <int>`	Type the maximum number of general entity references to allow in a single request.	`0`
`maxNameLength <int>`	Type the maximum length to allow for any XML element, attribute or namespace.	`0`
`maxNamespaceDecls <int>`	Type the maximum number of XML namespace (XMLNS) declarations to allow in a single request.	`0`
`maxNamespaceDeclsPerElem <int>`	Type the maximum number of XML namespace (XMLNS) declarations to allow for any XML element.	`0`
`maxPIs <int>`	Type the maximum number of processing instructions (PIs) to allow in a single request.	`0`
`maxTextNodeLength <int>`	Type the maximum length to allow for any text node.	`0`
`maxTextNodeRatio <int>`	Type the maximum size ratio to allow for any text node, where the maximum size ratio is: `T/(D-T)` where `D` is the total size of the request and `T` is the size of the text node.	`0`
`maxTextNodes <int>`	Type the maximum number of text nodes to allow in a single request.	`0`

History

FortiWeb v3.2.0 New.

Related topics

- config xml-protection xml-protection-profile
- config system snmp community

xml-protection key-file

Use this command to edit the comment associated with a previously uploaded key file.

Key files are applied through key management groups. For details, see “config xml-protection key-management” on page 253.

For information on how to upload a key file, see the *FortiWeb Administration Guide*.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `xmlgrp` area. For more information, see “Permissions” on page 29.

Syntax

```
config xml-protection key-file
  edit <key_name>
    set comment <comment_str>
  next
end
```

Variable	Description	Default
`<key_name>`	Type the name of the key file.	No default.
`comment <comment_str>`	Type a description or other comment. If the comment is more than one word, surround the words with quotes (').	No default.

Example

This example configures a comment for the key named key1.

```
config xml-protection key-file
  edit "key1"
    set comment "Used by www.example.com. Last rotated July 1."
  next
end
```

History

FortiWeb v3.2.0 New.

Related topics

- config xml-protection key-management

xml-protection key-management

Use this command to configure key management groups.

Key management groups pair cryptographic algorithms with keys. To apply a group, select it when configuring XML signatures, XML encryption, or XML decryption in an XML protection profile.

Before you can create a key management group, you must first upload one or more key files. For details, see the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `xmlgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config xml-protection key-management
  edit <key-mgmt-group_name>
    set comment <comment_str>
    config keyinfo
      edit <entry_index>
        set algo {<algorithm>}
        set keyname <key_name>
      next
    end
  next
end
```

Variable	Description	Default
`<key-mgmt-group_name>`	Type the name of the key management group.	No default.
`comment <comment_str>`	Type a description or other comment. If the comment is more than one word, surround the comment with quotes (').	No default.
`<entry_index>`	Type the index number of the individual entry.	No default.
`algo {<algorithm>}`	Type the name of a supported encryption algorithm to use with the key; one of: • `aes-128` • `aes-192` • `aes-256` • `dsa` • `rsa` • `tripledes` • `x509cert` For algorithms that include the bit strength (e.g., 128, 192, or 256), a larger number indicates stronger security, which may increase the load on the FortiWeb unit.	No default.
`keyname <key_name>`	Type the name of a key file that you have previously uploaded.	No default.

History

FortiWeb v3.2.0 New.

Related topics

- config xml-protection key-file
- config xml-protection xml-protection-profile

xml-protection period-time onetime

Use this command to create a schedule for executing a content filter rule on a one-time or as needed basis..

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.

Use schedules when configuring a content filter rule in order to define when the rule will be applicable. For details, see “config xml-protection filter-rule” on page 247.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `xmlgrp` area. For more information, see “Permissions” on page 29.

Syntax

```
config xml-protection period-time onetime
  edit <schedule_name>
    set start {<hh:mm> <yyyy/mm/dd>}
    set end {<hh:mm> <yyyy/mm/dd>}
  next
end
```

Variable	Description	Default
`<schedule_name>`	Type the name of the schedule.	No default.
`start {<hh:mm> <yyyy/mm/dd>}`	Type the time of day according to a 24-hour clock, such as `13:01`, and the date starting with the year, such as `2011/12/31`, on which the schedule will begin. Separate the time and date with a space.	`00:00 2001/01/01`
`end {<hh:mm> <yyyy/mm/dd>}`	Type the time of day according to a 24-hour clock, such as `13:01`, and the date starting with the year, such as `2011/12/31`, on which the schedule will end. Separate the time and date with a space.	`00:00 2001/01/01`

History

FortiWeb v3.2.0 New.

Related topics

- config xml-protection period-time recurring
- config xml-protection filter-rule

xml-protection period-time recurring

Use this command to create a schedule that is in effect repeatedly, during specified times and days.

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

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.

Use schedules when configuring a content filter rule in order to define when the rule will be applicable. For details, see "config xml-protection filter-rule" on page 247.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `xmlgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config xml-protection period-time recurring
  edit <schedule_name>
    set day {day-list}
    set start <hh:mm>
    set end <hh:mm>
  next
end
```

Variable	Description	Default
`<schedule_name>`	Type the name of the schedule.	No default.
`day {day-list}`	Type the names of the days of the week separated by spaces during which the schedule will be in force. Type the whole day name without an initial capital; for example, `monday`.	No default.
`start <hh:mm>`	Type the time of day according to a 24-hour clock, such as `13:01`, on which the schedule will begin.	`00:00`
`end <hh:mm>`	Type the time of day according to a 24-hour clock, such as `13:01`, on which the schedule will end.	`00:00`

History

FortiWeb v3.2.0 New.

Related topics

- config xml-protection period-time onetime
- config xml-protection filter-rule

xml-protection schema-files

Use this command to enable or disable a previously uploaded W3C schema file, or to change the associated comment.

Schema files are used if you have enabled the `schema-validate {enable | disable}` option in XML protection profiles.

Note: Disabling a schema file could block traffic matching policies in whose XML protection profile you have selected the *Schema Validate* option, because the FortiWeb unit may not be able to perform schema validation. For details, see `schema-validate {enable | disable}`.

For information on how to upload a schema file, see the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `xmlgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config xml-protection schema-files
  edit <schema_name>
    set status {enable | disable}
    set comment <comment_str>
  next
end
```

Variable	Description	Default
`<schema_name>`	Type the name of a schema file.	No default.
`status {enable | disable}`	Enable to use the schema file when performing schema validation for XML protection profiles that have been configured to do so.	No default.
`comment <comment_str>`	Type a description or other comment. If the comment is more than one word, surround the words with quotes (').	No default.

History

FortiWeb v3.2.0 New.

Related topics

- config xml-protection web-service

xml-protection web-service

Use this command to enable or disable individual web service operations in a previously uploaded web service definition language (WSDL) file.

Caution: Disabling a web service action could allow traffic matching policies in whose XML protection profile you have selected the `wsdl-verify` option, because the FortiWeb unit will not be able to perform full WSDL verification. For details, see `wsdl-verify {enable | disable}`.

To apply a WSDL file and its operations, select the web service when configuring a web service group or a WSDL content routing table. For details, see "config xml-protection web-service-group" on page 258 and "config xml-protection wsdl-content-routing-table" on page 259.

For information on how to upload a WSDL file, see the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `xmlgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config xml-protection web-service
  edit <wsdl-file_name>
    config operations
      edit <operation_index>
        set name <string>
        set status {enable | disable}
      next
    end
  next
end
```

Variable	Description	Default
`<wsdl-file_name>`	Type the name of the WSDL file.	No default.
`<operation_index>`	Type the index number of an individual operation in the WSDL file.	No default.
`status {enable | disable}`	Enable to allow use of the web service operation for WSDL verification and WSDL content routing.	No default.
`name <string>`	Type the name of a web service operation defined in the WSDL file.	

History

FortiWeb v3.2.0 New.

Related topics

- config xml-protection web-service-group
- config xml-protection schema-files

xml-protection web-service-group

Use this command to configure a WSDL service group.

Apply a WSDL service group using the `wsdl-verify {enable | disable}` option in XML protection profiles.

Before you can create a WSDL file group, you must first upload one or more WSDL files. For details, see the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `xmlgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config xml-protection web-service-group
  edit <wsdl-group_name>
    set comment <comment_str>
    set web-services {<wsdl-file_name> ...}
  next
end
```

Variable	Description	Default
`<wsdl-group_name>`	Type the name of the WSDL file group	No default.
`comment <comment_str>`	Type a description or other comment. If the comment is more than one word, surround the comment with quotes (').	No default.
`web-services {<wsdl-file_name> ...}`	Type the name of one or more uploaded WSDL files that will be members of the WSDL file group. Separate the name of each file with a space.	No default.

History

FortiWeb v3.2.0 New.

Related topics

- config xml-protection web-service

xml-protection wsdl-content-routing-table

Use this command to configure WSDL-based content routing for use when protecting a specific server in a server farm.

To configure a WSDL content routing table, select a set of web service operations from uploaded WSDL files. Then include the routing table when configuring a server farm.

Tip: Alternatively, you can configure an XPath expression that will define what sets of content will be routed to the physical server. For more information, see "config server-policy pservers" on page 102.

Before you can create a WSDL content routing group, you must first upload one or more WSDL files. For details, see the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `xmlgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
config xml-protection wsdl-content-routing-table
  edit <wsdl-route_name>
    config routing-table
      edit <entry_index>
        set service <wsdl-file_name>
        set operation <operation_name>
      next
    end
  next
end
```

Variable	Description	Default
`<wsdl-route_name>`	Type the name of the WSDL content routing group.	No default.
`<entry_index>`	Type the index number of the individual entry.	No default.
`service <wsdl-file_name>`	Type the name of a uploaded WSDL file whose operation you want to route to a specific physical server in a server farm, then configure `operation <operation_name>`.	No default.
`operation <operation_name>`	Type the name of the web service operation contained in the WSDL file you specified in `service <wsdl-file_name>`.	No default.

History

FortiWeb v3.2.0 New.

Related topics

- config xml-protection xml-protection-profile
- config xml-protection web-service-group
- config xml-protection web-service

xml-protection xml-protection-profile

Use this command to configure XML protection profiles.

Protection profiles are a set of attack protection settings. When a connection matches an applicable server policy, the FortiWeb unit applies the protection profile that you have selected for that policy.

Before configuring an XML protection profile, you must first configure and/or upload all components that it requires. For details, see:

- “config xml-protection filter-rule” on page 247
- “config xml-protection intrusion-prevention-rule” on page 250
- ““config xml-protection key-management” on page 253
- “config xml-protection web-service-group” on page 258
- “config xml-protection wsdl-content-routing-table” on page 259

To apply XML protection profiles, select them within a policy. For details, see “config server-policy policy” on page 92.

Use SNMP traps to notify you when an XML protection profile has been enforced. For details, see “config system snmp community” on page 150.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `xmlgrp` area. For more information, see “Permissions” on page 29.

Syntax

```
config xml-protection xml-protection-profile
  edit <xml-protection-profile_name>
    set comment <comment_str>
    set external-entity-attack-prevention {enable | disable}
    set filter-rule-name <content-filter-rule_name>
    set intrusion-rule-name <intrusion-prevention-rule_name>
    set key-info <key-mgmt-group_name>
    set none-xml-traffic {allow | reject}
    set schema-poisoning-prevention {enable | disable}
    set schema-validate {enable | disable}
    set sql-injection-prevention {enable | disable}
    set sql-injection-prevention-action {accept | alert | alert_deny | deny}
    set wsdl-scanning-prevention {enable | disable}
    set wsdl-verify {enable | disable}
    set wsdl-verify-action {accept | alert | alert_deny | deny}
    set wsdl-web-service <wsdl-group_name>
    set xml-encryption {enable | disable}
    set xml-encryption-action {accept | alert | alert_deny | deny}
    set xml-signature {enable | disable}
    set xml-signature-action {accept | alert | alert_deny | deny}
    set xml-signature-key <key-mgmt-group_name>
    set reverse-encryption {enable | disable}
    set xml-encryption-key <key-mgmt-group_name>
    set xml-encryption-xpath <xpath_str>
    set reverse-signature {enable | disable}
    set xml-signature-key <key-mgmt-group_name>
    set xml-signature-xpath <xpath_str>
  next
end
```

Variable	Description	Default
`<xml-protection-profile_name>`	Type the name of the XML protection profile.	No default.
`comment <comment_str>`	Type a description or other comment. If the comment is more than one word, surround the comment with quotes (').	No default.
`external-entity-attack-prevention {enable | disable}`	Enable to perform external entity attack prevention for traffic matching the policy.	No default.
`filter-rule-name <content-filter-rule_name>`	Type the name of a content filter rule. See "config xml-protection filter-rule" on page 247.	No default.
`intrusion-rule-name <intrusion-prevention-rule_name>`	Type the name of an intrusion prevention rule. See "config xml-protection intrusion-prevention-rule" on page 250.	No default.
`key-info <key-mgmt-group_name>`	Type the key management group that will be used for XML signature verification and/or decryption of forward traffic, if enabled in `xml-encryption {enable | disable}` and/or `xml-signature {enable | disable}`. See "config xml-protection key-management" on page 253.	No default.
`none-xml-traffic {allow | reject}`	Select whether or not to accept HTTP requests that do ***not*** contain `Content-Type: text/xml` in the HTTP header. Accepting such requests may be required if the web service uses representational state transfer (REST) instead of SOAP.	`allow`
`reverse-encryption {enable | disable}`	Enable to apply XML encryption to reply traffic. Also configure `xml-encryption-key <key-mgmt-group_name>` and `xml-encryption-xpath <xpath_str>`. For the XML encryption/decryption specification, see http://www.w3.org/TR/xmlenc-core/.	No default.
`reverse-signature {enable | disable}`	Enable to sign reply traffic with XML signatures. Also configure `key-info <key-mgmt-group_name>` and `xml-encryption-xpath <xpath_str>`. For the XML signature specification, see http://www.w3.org/TR/xmldsig-core/.	No default.
`schema-poisoning-prevention {enable | disable}`	Enable to prevent external schema references, and thereby preventing schema poisoning attacks, for traffic matching the policy. This option does not permit schema referencing by URL for security reasons, and requires that you upload a schema. For details, see the *FortiWeb Administration Guide*.	No default.
`schema-validate {enable | disable}`	Enable to perform schema validation for traffic matching the policy. This option may require that you first upload a schema file to the FortiWeb unit, and enable it. • If this option is enabled, `wsdl-verify` is `enable`, and the schema file does not exist or is disabled, the schema validator will ***allow*** the connection. • If this option is enabled, `wsdl-verify` is `disable`, and the schema file does not exist or is disabled, the schema validator will ***block*** the connection. For details on uploading a schema file, see the *FortiWeb Administration Guide*.	No default.
`sql-injection-prevention {enable | disable}`	Enable to prevent SQL injection attacks by blocking requests that contain SQL statements.	No default.

Variable	Description	Default
`sql-injection-prevention-action {accept | alert | alert_deny | deny}`	Select the action that the FortiWeb unit will take if the connection contains SQL statements. • `accept`: Accept the connection. • `alert`: Accept the connection and generate an alert and/or log message. • `alert_deny`: Block the connection and generate an alert and/or log message. • `deny`: Block the connection. This option applies only if `sql-injection-prevention` is `enable`. For more information on logging and alerts, see "config log disk" on page 44.	`accept`
`wsdl-scanning-prevention {enable | disable}`	Enable to perform WSDL scanning prevention for traffic matching the policy.	No default.
`wsdl-verify {enable | disable}`	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. This option requires that you first upload a WSDL file to the FortiWeb unit. For details on uploading a WSDL file, see the *FortiWeb Administration Guide*.	No default.
`wsdl-verify-action {accept | alert | alert_deny | deny}`	Select the action that the FortiWeb unit will take if the connection fails WSDL verification. • `accept`: Accept the connection. • `alert`: Accept the connection and generate an alert and/or log message. • `alert_deny`: Block the connection and generate an alert and/or log message. • `deny`: Block the connection. This option applies only if `wsdl-verify` is `enable`. For more information on logging and alerts, see "config log disk" on page 44.	`accept`
`wsdl-web-service <wsdl-group_name>`	Type the name of the WSDL file group to use to verify the request.	No default.
`xml-encryption {enable | disable}`	Select to enable XML decryption of forward traffic. Also configure `xml-encryption-action {accept | alert | alert_deny | deny}` and `key-info <key-mgmt-group_name>`. For the XML encryption/decryption specification, see http://www.w3.org/TR/xmlenc-core/.	No default.
`xml-encryption-action {accept | alert | alert_deny | deny}`	Select the action that the FortiWeb unit will take if the forward traffic fails XML decryption. • `accept`: Accept the connection. • `alert`: Accept the connection and generate an alert and/or log message. • `alert_deny`: Block the connection and generate an alert and/or log message. • `deny`: Block the connection. This option applies only if `xml-encryption` is `enable`. For more information on logging and alerts, see "config log disk" on page 44.	`accept`
`xml-encryption-key <key-mgmt-group_name>`	Type the name of the key management group that will be used for XML encryption. See "config xml-protection key-management" on page 253. This option applies only if `reverse-encryption` is `enable`.	No default.
`xml-encryption-xpath <xpath_str>`	Type an XPath expression that matches XML elements in reply traffic to which you want to apply XML encryption. Surround the expression in quotes. This option applies only if `reverse-encryption` is `enable`.	No default.

Variable	Description	Default
`xml-signature {enable | disable}`	Enable to validate XML signatures for forward traffic. Also configure `xml-signature-action {accept | alert | alert_deny | deny}` and `key-info <key-mgmt-group_name>`. For the XML signature specification, see http://www.w3.org/TR/xmldsig-core/.	No default.
`xml-signature-action {accept | alert | alert_deny | deny}`	Select the action that the FortiWeb unit will take if the forward traffic fails XML signature verification. • `accept`: Accept the connection. • `alert`: Accept the connection and generate an alert and/or log message. • `alert_deny`: Block the connection and generate an alert and/or log message. • `deny`: Block the connection. This option applies only if `xml-signature` is `enable`. For more information on logging and alerts, see "config log disk" on page 44.	`accept`
`xml-signature-key <key-mgmt-group_name>`	Type the key management group that will be used for XML signing of reply traffic. See "config xml-protection key-management" on page 253. This option applies only if `reverse-signature` is `enable`.	No default.
`xml-signature-xpath <xpath_str>`	Type an XPath expression that matches XML elements in reply traffic to which you want to apply XML signatures. Surround the expression in quotes. This option applies only if `reverse-signature` is `enable`.	No default.

Example

This example configures XML encryption and decryption, XML signatures and signature verification, and all the available attack preventions. It also uses a content filter named content_filter1 to prevent web clients from viewing hidden content, and an intrusion prevention rule named intrusion_prevention_rule1 to define valid input constraints.

```
config xml-protection xml-protection-profile
  edit "xml_protection_profile1"
    set external-entity-attack-prevention enable
    set filter-rule-name "content_filter1"
    set intrusion-rule-name "intrusion_prevention_rule1"
    set none-xml-traffic reject
    set schema-poisoning-prevention enable
    set schema-validate enable
    set sql-injection-prevention enable
    set sql-injection-prevention-action alert_deny
    set wsdl-scanning-prevention enable
    set wsdl-verify enable
    set wsdl-verify-action alert_deny
    set wsdl-web-service "wsdl_group1"
    set xml-encryption enable
    set xml-encryption-action alert_deny
    set xml-signature enable
    set xml-signature-action alert_deny
    set key-info "key_mgmt_group1"
    set reverse-encryption enable
    set xml-encryption-key "key_mgmt_group1"
    set xml-encryption-xpath "//*"
    set reverse-signature enable
    set xml-signature-key "key_mgmt_group1"
```

```
    set xml-signature-xpath "//*"
    set status enable
  next
end
```

History

FortiWeb v3.2.0 New.

Related topics

- config server-policy policy
- config xml-protection filter-rule
- config xml-protection intrusion-prevention-rule
- config xml-protection key-management
- config xml-protection period-time onetime
- config xml-protection period-time recurring
- config xml-protection schema-files
- config xml-protection wsdl-content-routing-table
- config system settings
- config system snmp community

diagnose

The `diagnose` commands display diagnostic information that help you troubleshoot problems.

This chapter describes the following commands:

diagnose debug application
diagnose debug cli
diagnose debug console
diagnose debug crashlog
diagnose debug disable/enable
diagnose debug failopen-poweron-bypass
diagnose debug flow
diagnose debug info
diagnose debug proxy
diagnose debug reset
diagnose debug upload
diagnose hardware
diagnose network arp
diagnose network ip
diagnose network route
diagnose network sniffer
diagnose network tcp/udp
diagnose system flash
diagnose system kill
diagnose system mount
diagnose system raid
diagnose system top

debug application

Use this command to set the debug levels for by FortiAnalyzer. To generate debug information, the application must be running and diagnose debug disable/enable must be set to `enable`. The CLI displays output until you stop it by pressing Ctrl + C.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
debug application <application_name> <debug-level>
```

Variable	Description	Default
`<application_name>`	Type the name of the application or process to set the debug level for: • `alertmail` (alertmail daemon) • `autolearn` (auto learn module) • `detect` (intrusion detect module) • `dssl` (SSL decode module) • `fds` (FortiWeb Distribution Network updates) • `http` (HTTP parse module) • `miglogd` (log daemon) • `mulpattern` (multi-pattern module) • `proxy` (proxy daemon flow information) • `proxy-error` (proxy daemon error information) • `sshd` (sshd daemon) • `ustack` (user-space TCP/IP stack)	No default.
`<debug-level>`	Type the number indicating the level of debugging messages to output to the CLI display when the command executes. • 0: Do not display messages. • 1: Display verbose messages in the CLI. • 2: Display brief messages in the CLI.	0

History

FortiWeb v4.2 New.

debug cli

Use this command to set the debug level for the command line interface (CLI).

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug cli <debug-level>
```

Variable	Description	Default
`<debug-level>`	Type a number indicating the level of verbosity from 0 through 8.	3

History

FortiWeb v4.2 New.

debug console

Use this command to enable or disable the debug timestamp.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug console timestamp {enable | disable}
```

Variable	Description	Default
`{enable | disable}`	Type `enable` to add timestamps to debug output or `disable` to remove them.	`enable`

History

FortiWeb v4.2 New.

debug crashlog

Use this command to show application proxies that have back traces, traps, or registration dumps, or to clear the crash log.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug crashlog {show | clear}
```

Variable	Description	Default
`{show | clear}`	Type `show` to view the crash log. Enter `clear` to clear the log.	No default.

Example

```
diagnose debug crashlog show
```

Output similar to the following appears in the CLI window:

```
2011-02-08 06:20:46 <18632> firmware FortiWeb-1000B 4.20,build0403,110131
2011-02-08 06:20:46 <18632> application proxy
2011-02-08 06:20:46 <18632> *** signal 11 (Segmentation fault) received ***
2011-02-08 06:20:46 <18632> Register dump:
2011-02-08 06:20:46 <18632> RAX: 00000000 RBX: 00000001 RCX: 00000001 RDX: 00000001
2011-02-08 06:20:46 <18632> RSI: 008d91a4 RDI: 00000000 RBP: 2b8f90ee2b10 RSP: 0072af60
2011-02-08 06:20:46 <18632> RIP: 008d8660   EFLAGS: 2b8f9aaa0010
2011-02-08 06:20:46 <18632> CS: 86b0   FS: 0000   GS: 008d
2011-02-08 06:20:46 <18632> Trap: 7fff26859ee0   Error: 008d8710   OldMask: 00440f90
2011-02-08 06:20:46 <18632> CR2: 00010202
2011-02-08 06:20:46 <18632> Backtrace:
2011-02-08 06:20:46 <18632> [0x008d8660] => /bin/xmlproxy (g_proxy+0x00000000)
2011-02-08 06:20:46 proxy received SEGV signal - 11
```

History

FortiWeb v4.2 New.

debug disable/enable

Use this command to turn debug output on or off.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug {enable | disable}
```

Variable	Description	Default
`{enable | disable}`	Type `enable` to allow the display of debug information or `disable` to disable it.	`enable`

History

FortiWeb v4.2 New.

debug failopen-poweron-bypass

For FortiWeb units that support the fail-open function, use this command to switch between bypass and cutoff.

Fail-open is supported only when the FortiWeb unit operates in true transparent proxy (TTP) mode and transparent inspection (TI) mode, and only for models with a CP7 processor, such as the FortiWeb-1000C and FortiWeb-3000C. Fail-open is disabled if the FortiWeb unit is configured as a high availability master or backup.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug failopen-poweron-bypass {on | off}
```

Variable	Description	Default
`{on | off}`	Type `on` to enable the bypass function or `off` to disable it. The `on` parameter is equivalent to selecting *PowerOff-Bypass* on the *System* > *Network* > *Fail-open* page on the web-based manager, and the `off` parameter is equivalent to *PowerOff-Cutoff*.	No default.

History

FortiWeb v4.2 New.

debug flow

Use this command to trace the flow of packets through the FortiWeb unit.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug flow filter policy policy-name <policy_name>
diagnose debug flow filter policy source-ip <ipv4>
diagnose debug flow reset
diagnose debug flow show
```

Variable	Description	Default
`filter policy policy-name <policy_name>`	Type a server policy name to use when debugging traffic.	No default.
`filter policy source-ip <ipv4>`	Enter an IP address of the server whose traffic flow you want traced.	No default.
`reset`	Removes all debug flow settings.	No default.
`show`	Displays the current debug flow settings.	No default.

You can specify both the `policy-name` and `source-ip` options to narrow the scope of debug flow tracing.

History

FortiWeb v4.2 New.

debug info

Use this command to view a list of debug settings.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug info
```

Example

```
diagnose debug info
```

Output similar to the following appears in the CLI window:

```
debug output:           enable
console timestamp:      disable
alertmail debug level:  1
sshd debug level:       1
http debug level:       2
detect debug level:     1
autolearn debug level:  1
ustack debug level:     2
fds debug level:        1
CLI debug level:        4
```

History

FortiWeb v4.2 New.

debug proxy

Use this command to show the current operation mode for the local FortiWeb unit.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug proxy
```

Example

```
diagnose debug proxy
```

Output similar to the following appears in the CLI window:

```
opmode is 4
```

The integer returned indicates the current operation mode.

Table 11: Debug proxy opmode values

Integer	Meaning
2	True transparent proxy
4	Reverse proxy
8	Offline protection
32	Transparent inspection

History

FortiWeb v4.2 New.

debug reset

Use this command to reset all debug settings to default settings for the currently installed firmware version. If you have not upgraded or downgraded the firmware, this restores the factory default settings.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug reset
```

History

FortiWeb v4.2 New.

debug upload

Use this command to export debug information to an FTP server.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug upload <ftp-address> <username> <password> <upload-dir>
```

Variable	Description	Default
`<ftp-address>`	Enter an IP address or host name for the FTP server.	No default.
`<username>`	Enter a valid user name to log in to the FTP server.	No default.
`<password>`	Enter a valid password to log in to the FTP server.	No default.
`<upload-dir>`	Enter the directory path where the uploaded files are to be stored.	No default.

Example

```
diagnose debug upload 10.11.101.170 user1 pass1239 c:/uploads
```

History

FortiWeb v4.2 New.

hardware

Use the hardware command to display a list of specifications and settings on the FortiWeb unit for CPUs, hard disks, interrupts, memory, and network interface cards (NIC).

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
diagnose hardware <hardware-type> list
```

Variable	Description	Default
`<hardware-type>`	Type one of the following hardware keywords: • `cpu` • `harddisk` • `interrupts` • `mem` • `nic <interface name>` The `nic` keyword requires an interface name as a parameter; for example: `diagnose hardware nic list port1`	No default.

Example

```
diagnose hardware cpu list
```

Output similar to the following appears in the CLI window:

```
processor       : 0
vendor_id       : GenuineIntel
cpu family      : 6
model           : 23
model name      : Intel(R) Xeon(R) CPU           E5405  @ 2.00GHz
stepping        : 10
cpu MHz         : 1995.056
cache size      : 6144 KB
physical id     : 0
siblings        : 4
core id         : 0
cpu cores       : 4
fpu             : yes
fpu_exception   : yes
cpuid level     : 13
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat
pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm syscall nx lm constant_tsc pni monitor
ds_cpl vmx tm2 cx16 xtpr lahf_lm
bogomips        : 3994.51
clflush size    : 64
cache_alignment : 64
address sizes   : 38 bits physical, 48 bits virtual
power management:
```

History

FortiWeb v4.2 New.

network arp

Use this command to add or delete an address resolution protocol (ARP) in the internal ARP table, or to list the table contents.

Caution: Take care when deleting a table entry. FortiWeb presents no confirmation message and provides no undelete mechanism.

To use this command, your administrator account's access control profile must have `rw` or `w` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
diagnose network arp add <interface_name> <ipv4> <mac-address>
diagnose network arp delete <interface_name> <ipv4> <mac-address>
diagnose network arp list
```

Variable	Description	Default
`<interface_name>`	Type the name of the interface to add or delete from the ARP table.	No default.
`<ipv4>`	Enter the IP address of the interface.	No default.
`<mac-address>`	Enter the MAC address of the interface.	No default.

Example

This example displays a list of ARP table entries and then deletes one.

```
diagnose network arp list
  IP address       HW type     Flags       HW address           Mask     Device
  172.20.120.29    0x1         0x2         00:13:72:38:72:21     *        port1
  172.20.120.26    0x1         0x2         00:26:2D:24:B7:D3     *        port2
diagnose network arp delete port2 172.20.120.26 00:26:2D:24:B7:D3
```

History

FortiWeb v4.2 New.

network ip

Use this command to add or delete an IP address in the internal IP table, or to list the table contents.

Caution: Take care when deleting a table entry. FortiWeb presents no confirmation message and provides no undelete mechanism.

To use this command, your administrator account's access control profile must have `rw` or `w` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
diagnose network ip add <interface_name> <ipv4> <mask>
diagnose network ip delete <interface_name> <ipv4>
diagnose network ip list
```

Variable	Description	Default
`<interface_name>`	Type the name of the interface to add or delete from the IP table.	No default.
`<ipv4>`	Enter the IP address of the interface.	No default.
`<mask>`	Enter the network mask.	No default.

Example

This example displays a list of IP addresses and then deletes one.

```
diagnose network ip list
  3 IP 10.10.10.1/255.255.255.0 port2
  4 IP 172.20.120.169/255.255.255.0 port1
  5 IP 127.0.0.1/255.255.255.0 lo
diagnose network ip delete port2 10.10.10.1
```

History

FortiWeb v4.2 New.

network route

Use this command to add or delete a static route in the internal route table, or to list the table contents. A static route causes packets to be forwarded to a destination other than the default gateway.

Caution: Take care when deleting a table entry. FortiWeb presents no confirmation message and provides no undelete mechanism.

To use this command, your administrator account's access control profile must have `rw` or `w` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
diagnose network route add <interface_name> <ipv4> <mask> <next-hop>
   <distance> <priority> verify
diagnose network route delete <interface_name> <ipv4> <mask> <next-hop>
   <distance> <priority> verify
diagnose network route list
```

Variable	Description	Default
`<interface_name>`	Type the name of the interface to add or delete from the routing table.	No default.
`<ipv4>`	Enter the IP address of the interface.	No default.
`<mask>`	Enter the network mask.	No default.
`<next-hop>`	Enter the preferred IP address of the next router to which this route directs traffic.	No default.
`<distance>`	Type an administrative distance for the route. The distance value is arbitrary and should reflect the distance to the next-hop router. A lower value indicates a more preferred route. The value can be an integer from 1 to 255.	No default.
`<priority>`	Enter the priority of the route in the routing table. The lower the number the higher the priority. The value can be an integer from 1 to 255.	No default.
`verify`	Type this keyword to have FortiWeb verify the route.	No default.

Example

This example adds a route to the routing table.

```
diagnose network route add vlan2 160.1.12.0 255.0.0.0 172.20.01.169 32 3 verify
```

History

FortiWeb v4.2 New.

network sniffer

Use this command to perform a packet trace on one or more network interfaces.

Packet capture, also known as sniffing, records some or all of the packets seen by a network interface. By recording packets, you can trace connection states to the exact point at which they fail, which may help you diagnose some types of problems that are difficult to detect.

FortiWeb units have a built-in sniffer. Packet capture on FortiWeb units is similar to that of FortiGate units. Packet capture is displayed on the CLI, which you may be able to save to a file for later analysis, depending on your CLI client.

Packet capture output appears on your CLI display until you stop it by pressing Ctrl + C, or until it reaches the number of packets that you have specified to capture.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
diagnose network sniffer packet <interface_name> <filter_str> <verbose-
    level> <count_int>
```

Variable	Description	Default
`<interface_name>`	Type the name of a network interface whose packets you want to capture, such as `port1`, or type `any` to capture packets on all network interfaces.	No default.

`<filter_str>`	Type either `none` to capture all packets, or type a filter that specifies which protocols and port numbers that you do or do not want to capture, such as `'tcp port 25'`. Surround the filter string in quotes.
	The filter uses the following syntax:
	`'[[src|dst] host {<host1_fqdn> | <host1_ipv4>}] [and|or] [[src|dst] host {<host2_fqdn> | <host2_ipv4>}] [and|or] [[arp|ip|gre|esp|udp|tcp] port <port1_int>] [and|or] [[arp|ip|gre|esp|udp|tcp] port <port2_int>]'`
	To display only the traffic between two hosts, specify the IP addresses of both hosts. To display only forward or reply packets, indicate which host is the source, and which is the destination.
	For example, to display UDP port 1812 traffic between 1.example.com and either 2.example.com or 3.example.com, you would enter:
	`'udp and port 1812 and src host 1.example.com and dst \( 2.example.com or 2.example.com \)'`
		`none`

`<verbose-level>`	Type one of the following integers indicating the depth of packet headers and payloads to capture: • 1 for headers only • 2 for IP headers and payload • 3 for Ethernet headers and payload Verbose level 3 is best set when troubleshooting.	No default.
`<count_int>`	Type the number of packets to capture before stopping. If you do not specify a number, the command will continue to capture packets until you press Ctrl + C.	No default.

Example

The following example captures three packets of traffic from any port number or protocol and between any source and destination (a filter of `none`), which passes through the network interface named port1. The capture uses a low level of verbosity (indicated by `1`).

```
diagnose network sniffer packet port1 none 1 3
```

Below is an example command a representative output.

```
interfaces=[port1]
filters=[none]
0.918957 192.168.0.1.36701 -> 192.168.0.2.22: ack 2598697710
0.919024 192.168.0.2.22 -> 192.168.0.1.36701: psh 2598697710 ack 2587945850
0.919061 192.168.0.2.22 -> 192.168.0.1.36701: psh 2598697826 ack 2587945850
```

If you are familiar with the TCP protocol, you may notice that the packets are from the middle of a TCP connection. Because port 22 is used (highlighted above in bold), which is the standard port number for SSH, the packets might be from an SSH session.

Example

The following example captures packets traffic on TCP port 80 (typically HTTP) between two hosts, 192.168.0.1 and 192.168.0.2. The capture uses a low level of verbosity (indicated by `1`). Because the filter does not specify either host as the source or destination in the IP header (`src` or `dst`), the sniffer captures both forward and reply traffic.

```
diagnose network sniffer packet port1 'host 192.168.0.2 or host 192.168.0.1 and
tcp port 80' 1
```

A specific number of packets to capture is not specified. As a result, the packet capture continues until the administrator presses Ctrl + C. The sniffer then confirms that five packets were seen by that network interface. Below is a sample output.

```
192.168.0.2.3625 -> 192.168.0.1.80: syn 2057246590
192.168.0.1.80 -> 192.168.0.2.3625: syn 3291168205 ack 2057246591
192.168.0.2.3625 -> 192.168.0.1.80: ack 3291168206
192.168.0.2.3625 -> 192.168.0.1.80: psh 2057246591 ack 3291168206
192.168.0.1.80 -> 192.168.0.2.3625: ack 2057247265
5 packets received by filter
0 packets dropped by kernel
```

Example

The following example captures all TCP port 443 (typically HTTPS) traffic occurring through port1, regardless of its source or destination IP address. The capture uses a high level of verbosity (indicated by 3).

A specific number of packets to capture is not specified. As a result, the packet capture continues until the administrator presses Ctrl + C. The sniffer then confirms that five packets were seen by that network interface.

Verbose output can be very long. As a result, output shown below is truncated after only one packet. For example:

```
diagnose network sniffer packet port1 'tcp port 443' 3
```

Below is a sample output.

```
interfaces=[port1]
filters=[tcp port 443]
10.651905 192.168.0.1.50242 -> 192.168.0.2.443: syn 761714898
0x0000   0009 0f09 0001 0009 0f89 2914 0800 4500        ..........)...E.
0x0010   003c 73d1 4000 4006 3bc6 d157 fede ac16        .<s.@.@.;..W....
0x0020   0ed8 c442 01bb 2d66 d8d2 0000 0000 a002        ...B..-f........
0x0030   16d0 4f72 0000 0204 05b4 0402 080a 03ab        ..Or............
```

History

FortiWeb v3.2.2	New.
FortiWeb v4.2	Syntax changed to add the keyword `network`.

network tcp/udp

Use this command to view a list of TCP or UDP sockets.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
diagnose network tcp list
diagnose network udp list
```

Variable	Description	Default
`tcp list`	Display a list of TCP sockets.	No default.
`udp list`	Display a list of UDP sockets.	No default.

History

FortiWeb v4.2 New.

system flash

Use this command to change the currently active firmware partition or to display partition information.

FortiWeb units have two partitions that each contain a firmware image: one is the primary and one is the backup. If the FortiWeb unit is unable to successfully boot using the primary firmware partition, you may be able to boot using the alternative firmware partition, which can contain another version of the firmware.

Note: The `flash default` command takes effect when the FortiWeb unit next starts or reboots.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
diagnose system flash default <partition_int>
diagnose system flash list
```

Variable	Description	Default
`<partition_int>`	Type the number of the partition that will be used as the primary firmware partition during the next reboot or startup. The other partition will become the backup firmware partition.	No default.

Example

This example lists the partition settings.

```
diagnose system flash list
```

Below is a sample output.

```
Image#  Version                              TotalSize(KB)  Used(KB)  Use%  Active
1       FV-1KB-4.20-FW-build0397-110120   38733          33125     86%   No
2       FV-1KB-4.20-FW-build0396-110112   38733          33125     86%   Yes
3                                         836612         16980     2 %   No
```

History

FortiWeb v3.2.2 New.

system kill

Use this command to terminate a process currently running on the system. You must own the process or be a privileged user to kill it.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
diagnose system kill <signal> <pid>
```

Variable	Description	Default
`<signal>`	Type the Linux-style signal to send. This in an integer between 1 and 32. Some common signals are: • 1 = hangup • 2 = interrupt • 3 = quit • 9 = kill • 15 = terminate software	No default.
`<pid>`	Type the process ID where the signal is sent to.	No default.

History

FortiWeb v4.2 New.

system mount

Use this command to display a list of mounted file systems, including their available disk space, disk usage, and mount locations.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
diagnose system mount list
```

Example

```
diagnose system mount list
```

Below is a sample output.

```
Filesystem           1k-blocks      Used Available Use% Mounted on
/dev/ram0                61973     31207     30766  50% /
none                    262144       736    261408   0% /tmp
none                    262144         0    262144   0% /dev/shm
/dev/sdb2                38733     25119     11614  68% /data
/dev/sda1            153785572    187068 145783964   0% /var/log
/dev/sdb3               836612     16584    777528   2% /home
```

History

FortiWeb v3.2.2 New.

system raid

Use this command to display information about existing RAID disks.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
diagnose system raid list
```

History

FortiWeb v4.2 New.

system top

Use this command to view a list of the most system-intensive processes and to change the refresh rate.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
diagnose system top [<delay_int>] [<max-lines>}
```

Variable	Description	Default
`<delay_int>`	Type the reporting delay in seconds.	5
`<max-lines>`	Set the maximum number of top process to display.	All top processes are shown.

Once you execute this command, it continues to run and display in the CLI window until you enter `q` (quit).

While the command is running, you can press `Shift + P` to sort the five columns of data by CPU usage (the default) or `Shift + M` to sort by memory usage.

Example

This example displays a list of the top FortiWeb processes and sets the reporting rate at 10 seconds.

```
diagnose system top 10
```

Below is a sample output.

```
Run Time:  4 days, 3 hours and 27 minutes
0U, 0S, 100I; 2008T, 445F
 alertmail      423      S       0.0     2.3
   cmdbsvr      396      S       0.0     0.8
    httpsd      404      S       0.0     0.4
    httpsd    10957      S       0.0     0.3
    httpsd    10092      S       0.0     0.3
  xmlproxy      405      S       0.0     0.3
       cli    12907      S       0.0     0.2
   hasyncd      409      S       0.0     0.2
   synconf      410      S       0.0     0.1
 al_daemon      407      S       0.0     0.1
   updated      403      S       0.0     0.1
backup_con      418      S       0.0     0.1
log_indexe      413      S N     0.0     0.1
   cp7init      411      S       0.0     0.1
crl_update      417      S       0.0     0.1
  monitord      406      S       0.0     0.1
   miglogd      402      S       0.0     0.1
      sshd      421      S       0.0     0.1
       cli    13017      R       0.0     0.1
```

The first line indicates the up time. The second line lists the processor and memory usage, where the parameters from left to right mean:

- U = the percent of user CPU usage (in this case 0%)
- S = the percent of system CPU usage (in this case 0%)
- I = idle CPU usage percent (in this case 100%)

- T = total memory in kilobytes (in this case 2008 KB)
- F = free memory in kilobytes (in this case 445 KB)

The five columns of data provide the process name, the process ID (pid), the status, the CPU usage, and the memory usage. The status values are:

- S: sleeping (idle)
- R: running
- Z: zombie (crashed)
- <: high priority
- N: low priority

History

FortiWeb v4.2 New.

execute

The `execute` command performs an immediate action. Unlike `config` commands, most `execute` commands do not result in any configuration change.

This chapter describes the following commands:

execute backup
execute create-raid
execute date
execute factoryreset
execute ping
execute ping-options
execute reboot
execute restore
execute shutdown
execute time
execute traceroute
execute update-now

backup

Use this command to back up the configuration file to a TFTP server.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
execute backup {config | full-config } tftp <filename_str> <tftp_ipv4>
   [<password_str>]
```

Variable	Description	Default
`{config | full-config }`	Type either: • `config`: Back up configuration changes only. The default settings will not be backed up. • `full-config`: Back up the entire configuration file, including the default settings.	No default.
`<filename_str>`	Type the name of the file to be used for the backup file, such as `FortiWeb_backup.txt`.	No default.
`<tftp_ipv4>`	Type the IP address of the TFTP server.	No default.
`[<password_str>]`	Type a password for use when encrypting the backup file. You must provide the same password when restoring the backup file. If you do not provide a password, the backup file is stored as clear text.	No default.

Example

This example uploads the FortiWeb unit's system configuration to a file named `fweb.cfg` on a TFTP server at IP address 192.168.1.23. The file will not be password-encrypted.

```
execute backup config tftp fweb.cfg 192.168.1.23
```

History

FortiWeb v3.2.0 New.

Related topics

- execute restore

create-raid

Use this command to set the a RAID level.

Currently, FortiWeb supports only RAID level 1 and only on models 1000B, 1000C, and 3000C shipped with version 4.1 or later. On older units that were upgrade to version 4.1, the RAID status cannot be activated.

Note: Rebuilding RAID after a disk failure will result in some loss of data in packet logs.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
execute create-raid level level <raid_level>
execute create-raid rebuild
```

Variable	Description	Default
`level <raid_level>`	Type the Raid level. Currently only raid1 is supported.	No default.
`rebuild`	Type this command to rebuild the current raid level.	No default.

Example

This example sets the RAID level to raid1.

```
execute create-raid rebuild
```

The CLI displays the following:

```
This operation will clear all data on disk :0!
Do you want to continue? (y/n
```

After you enter `y` (yes), the CLI displays additional messages.

History

FortiWeb v4.1 New.

FortiWeb v4.2 Added the `rebuild` option.

date

Use this command to display or set the system date.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
execute date [<date_str>]
```

Variable	Description	Default
`date [<date_str>]`	Type the current date for the FortiWeb unit's time zone, using the format `yyyy-mm-dd`, where: • `yyyy` is the year. Valid years are `2001` to `2037`. • `mm` is the month. Valid months are `01` to `12`. • `dd` is the day of the month. Valid days are `01` to `31`. If you do not specify a date, the command returns the current system date. Shortened values, such as `06` instead of `2006` for the year or `1` instead of `01` for the month or day, are not valid.	No default.

Example

This example sets the date to 17 September 2011:

```
execute date 2011-09-17
```

History

FortiWeb v3.2.0 New.

Related topics

- execute time
- config system global

factoryreset

Use this command to reset the FortiWeb unit to its default settings for the currently installed firmware version. If you have not upgraded or downgraded the firmware, this restores factory default settings.

Caution: Back up your configuration first. This command resets all changes that you have made to the FortiWeb unit's configuration file and reverts the system to the default values for the firmware version, including factory default settings for the IP addresses of network interfaces. For information on creating a backup, see "execute backup" on page 292.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
execute factoryreset
```

History

FortiWeb v3.2.0 New.

Related topics

- execute backup
- execute restore

ping

Use this command to perform an ICMP ECHO request (also called a ping) to a host by specifying its fully qualified domain name (FQDN) or IP address, using the options configured by “execute ping-options” on page 298.

Pings are often used to test connectivity during troubleshooting.

To use this command, your administrator account’s access control profile must have at least `r` permission to the `sysgrp` area. For more information, see “Permissions” on page 29.

Syntax

```
execute ping {<fqdn_str> | <host_ipv4>}
```

Variable	Description	Default
`ping {<fqdn_str> | <host_ipv4>}`	Enter either the IP address or fully qualified domain name (FQDN) of the host.	No default.

Example

This example pings a host with the IP address 172.16.1.10.

```
execute ping 172.16.1.10
```

The CLI displays the following:

```
PING 172.16.1.10 (172.16.1.10): 56 data bytes
64 bytes from 172.16.1.10: icmp_seq=0 ttl=128 time=0.5 ms
64 bytes from 172.16.1.10: icmp_seq=1 ttl=128 time=0.2 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=128 time=0.2 ms
64 bytes from 172.16.1.10: icmp_seq=3 ttl=128 time=0.2 ms
64 bytes from 172.16.1.10: icmp_seq=4 ttl=128 time=0.2 ms

--- 172.16.1.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.5 ms
```

The results of the ping indicate that a route exists between the FortiWeb unit and 172.16.1.10. It also indicates that during the sample period, there was no packet loss, and the average response time was 0.2 milliseconds (ms).

Example

This example pings a host with the IP address 10.0.0.1.

```
execute ping 10.0.0.1
```

The CLI displays the following:

```
PING 10.0.0.1 (10.0.0.1): 56 data bytes
```

After several seconds, no output appears. The administrator halts the ping by pressing Ctrl + C. The CLI displays the following:

```
--- 10.0.0.1 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

The results of the ping indicate that the host may be down, or that there is no route between the FortiWeb unit and 10.0.0.1. To determine the cause, further diagnostic tests are required, such as “execute traceroute” on page 304.

History

FortiWeb v3.2.0 New.

Related topics

- execute ping-options
- execute traceroute

ping-options

Use this command to configure the behavior of the execute ping command.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
execute ping-options data-size <bytes_int>
execute ping-options df-bit {yes | no}
execute ping-options pattern <bufferpattern_hex>
execute ping-options repeat-count <repeat_int>
execute ping-options source {auto | <interface_ipv4>}
execute ping-options timeout <seconds_int>
execute ping-options tos {<service_type>}
execute ping-options ttl <hops_int>
execute ping-options validate-reply {yes | no}
execute ping-options view-settings
```

Variable	Description	Default
`data-size <bytes_int>`	Enter datagram size in bytes.This allows you to send out packets of different sizes for testing the effect of packet size on the connection. If you want to configure the pattern that will be used to buffer small datagrams to reach this size, also configure `pattern <bufferpattern_hex>`.	`56`
`df-bit {yes | no}`	Enter either `yes` to set the DF bit in the IP header to prevent the ICMP packet from being fragmented, or enter `no` to allow the ICMP packet to be fragmented.	`no`
`pattern <bufferpattern_hex>`	Enter a hexadecimal pattern, such as `00ffaabb`, to fill the optional data buffer at the end of the ICMP packet. The size of the buffer is determined by `data-size <bytes_int>`.	No default.
`repeat-count <repeat_int>`	Enter the number of times to repeat the ping.	5
`source {auto | <interface_ipv4>}`	Select the network interface from which the ping is sent. Enter either `auto` or a FortiMail network interface's IP address.	auto
`timeout <seconds_int>`	Enter the ping response timeout in seconds.	2
`tos {<service_type>}`	Enter the IP type-of-service option value, either: • `default`: Do not indicate. (That is, set the TOS byte to 0.) • `lowcost`: Minimize cost. • `lowdelay`: Minimize delay. • `reliability`: Maximize reliability. • `throughput`: Maximize throughput.	`default`
`ttl <hops_int>`	Enter the time-to-live (TTL) value.	`64`
`validate-reply {yes | no}`	Select whether or not to validate ping replies.	`no`
`view-settings`	Display the current ping option settings.	No default.

Example

This example sets the number of pings to three and the source IP address to that of the port2 network interface, 10.10.10.1, then views the ping options to verify their configuration.

```
execute ping-option repeat-count 3
execute ping-option source 10.10.10.1
execute ping-option view-settings
```

The CLI would display the following:

```
Ping Options:
```

```
Repeat Count: 3
Data Size: 56
Timeout: 2
TTL: 64
TOS: 0
DF bit: unset
Source Address: 10.10.10.1
Pattern:
Pattern Size in Bytes: 0
Validate Reply: no
```

History

FortiWeb v3.2.0 New.

Related topics

- execute ping
- execute traceroute

reboot

Use this command to restart the FortiWeb unit.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
execute reboot
```

Example

This example shows the reboot command in action.

```
execute reboot
```

The CLI displays the following:

```
This operation will reboot the system !
Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following:

```
System is rebooting...
```

If you are connected to the CLI through a local console, the CLI displays messages while the reboot is occurring.

If you are connected to the CLI through the network, the CLI will not display any notification while the reboot is occurring, as this occurs after the network interfaces have been shut down. Instead, you may notice that the connection is terminated. Time required by the reboot varies by many factors, such as whether or not hard disk verification is required, but may be several minutes.

History

FortiWeb v3.2.0 New.

Related topics

- execute shutdown

restore

Use this command to restore the configuration from a configuration backup file on an TFTP server, or to install primary or backup firmware.

Caution: Back up your configuration. This command can make large changes to your configuration.

Unlike installing firmware via TFTP during a boot interrupt, installing firmware using this command will attempt to preserve settings and files, and not necessarily restore the FortiWeb unit to its firmware/factory default configuration.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
execute restore {config | full-config } tftp <filename_str> <tftp_ipv4>
   [<password_str>]
execute restore {image | secondary-image} tftp <filename_str> <tftp_ipv4>
```

Variable	Description	Default
`{config | full-config }`	Type either: • `config`: Restore configuration changes only. The default settings will not be restored. • `full-config`: Restore the entire configuration file, including the default settings. All settings will be overwritten by the backup, including administrator accounts and their passwords.	No default.
`<filename_str>`	Type the name of the backup file, such as `FortiWeb_backup.txt`, or firmware image file.	No default.
`<tftp_ipv4>`	Type the IP address of the TFTP server.	No default.
`[<password_str>]`	Type the password that was used to encrypt the backup file, if any. If you do not provide a password, the backup file must have been stored as clear text.	No default.
`{image | secondary-image}`	Type either: • `image`: Install the firmware on FortiWeb unit's primary firmware partition and reboot. • `secondary-image`: Install the firmware on FortiWeb unit's primary firmware partition and reboot.	No default.

Example

This example downloads a configuration file named `backupconfig` from the TFTP server, 192.168.1.23, to the FortiWeb unit.

```
execute restore config tftp backupconfig 192.168.1.23
```

The FortiWeb unit downloads the configuration file, applies it, and restarts.

History

FortiWeb v3.2.0 New.

Related topics

- execute backup

shutdown

Use this command to prepare the FortiWeb unit to be powered down by halting the software, clearing all buffers, and writing all cached data to disk.

Caution: Power off the FortiWeb unit only after issuing this command. Unplugging or switching off the FortiWeb unit without issuing this command could result in data loss.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
execute shutdown
```

Example

This example shows the reboot command in action.

```
execute shutdown
```

The CLI displays the following:

```
This operation will halt the system
(power-cycle needed to restart)!Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following:

```
System is shutting down...(power-cycle needed to restart)
```

If you are connected to the CLI through a local console, the CLI displays a message when the shutdown is complete.

If you are connected to the CLI through the network, the CLI will not display any notification when the shutdown is complete, as this occurs after the network interfaces have been shut down. Instead, you may notice that the connection times out.

History

FortiWeb v3.2.0 New.

Related topics

- execute reboot

time

Use this command to display or set the system time.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
execute time [<time_str>]
```

Variable	Description	Default
`time [<time_str>]`	Type the current date for the FortiWeb unit's time zone, using the format `hh:mm:ss`, where: • `hh` is the hour. Valid hours are `00` to `23`. • `mm` is the minute. Valid minutes are `00` to `59`. • `ss` is the second. Valid seconds are `00` to `59`. If you do not specify a time, the command returns the current system time. Shortened values, such as `1` instead of `01` for the hour, are valid. For example, you could enter either `01:01:01` or `1:1:1`.	No default.

Example

This example sets the system time to 15:31:03:

```
execute time 15:31:03
```

History

FortiWeb v3.2.0 New.

Related topics

- execute date
- config system global

traceroute

Use this command to use ICMP to test the connection between the FortiWeb unit and another network device, and display information about the time required for network hops between the device and the FortiWeb unit.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
execute traceroute {<fqdn_str> | <host_ipv4>}
```

Variable	Description	Default
`traceroute {<fqdn_str> | <host_ipv4>}`	Enter the IP address or fully qualified domain name (FQDN) of the host.	No default.

Example

This example tests connectivity between the FortiWeb unit and http://docs.fortinet.com. In this example, the trace times out after the first hop, indicating a possible connectivity problem at that point in the network.

```
FortiWeb# execute traceroute docs.fortinet.com
traceroute to docs.fortinet.com (65.39.139.196), 30 hops max, 38 byte
   packets
 1  172.16.1.200 (172.16.1.200)  0.324 ms  0.427 ms  0.360 ms
 2  * * *
```

Example

This example tests the availability of a network route to the server example.com.

```
execute traceroute example.com
```

The CLI displays the following:

```
traceroute to example.com (192.168.1.10), 32 hops max, 72 byte packets
 1 172.16.1.2   0 ms  0 ms  0 ms
 2  10.10.10.1  <static.isp.example.net>  2 ms  1 ms  2 ms
 3  10.20.20.1   1 ms   5 ms   1 ms
 4  10.10.10.2  <core.isp.example.net>  171 ms  186 ms  14 ms
 5  10.30.30.1  <isp2.example.net>  10 ms  11 ms  10 ms
 6  10.40.40.1  73 ms  74 ms  75 ms
 7 192.168.1.1  79 ms  77 ms  79 ms
 8 192.168.1.2  73 ms  73 ms  79 ms
 9 192.168.1.10 73 ms  73 ms  79 ms
10 192.168.1.10 73 ms  73 ms  79 ms
```

Example

This example attempts to test connectivity between the FortiWeb unit and example.com. However, the FortiWeb unit could not trace the route, because the primary or secondary DNS server that the FortiWeb unit is configured to query could not resolve the FQDN `example.com` into an IP address, and it therefore did not know to which IP address it should connect. As a result, an error message is displayed.

```
FortiWeb# execute traceroute example.com
traceroute: unknown host example.com
Command fail. Return code 1
```

To resolve the error message in order to perform connectivity testing, the administrator would first configure the FortiWeb unit with the IP addresses of DNS servers that are able to resolve the FQDN `example.com`. For details, see "config system dns" on page 130.

History

FortiWeb v3.2.0 New.

Related topics

- execute ping
- execute ping-options

update-now

Use this command to initiate an update of the predefined robots, data types, suspicious URLS, and attack signatures used by your FortiWeb unit.

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

The time required for the update varies with the availability of the updates, the size of the updates, and the speed of the FortiWeb unit's network connection. If event logging is enabled, and the FortiWeb unit cannot connect successfully, it will log the message `update failed, failed to connect any fds servers!`

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see "Permissions" on page 29.

Syntax

```
execute update-now
```

History

FortiWeb v4.2. New.

get

The `get` command displays parts of your FortiWeb unit's configuration in the form of a list of settings and their values.

Unlike `show`, `get` displays ***all*** settings, even if they are still in their default state.

For example, you might get the current DNS settings:

```
get system dns
primary             : 172.16.95.19
secondary           : 0.0.0.0
domain              : example.com
```

Notice that the command displays the setting for the secondary DNS server, even though it has not been configured, or has reverted to its default value.

Also unlike `show`, unless used from within an object or table, `get` requires that you specify the object or table whose settings you want to display.

For example, at the root prompt, this command would be valid:

```
get system dns
```

and this command would not be:

```
get
```

Depending on whether or not you have specified an object, like `show`, `get` may display one of two different outputs: either the configuration that you have just entered but not yet saved, or the configuration as it currently exists on the disk, respectively.

For example, immediately after configuring the secondary DNS server setting but ***before*** saving it, `get` displays two different outputs (differences highlighted in bold):

```
config system dns
  set secondary 192.168.1.10
  get
    primary             : 172.16.95.19
    secondary           : 192.168.1.10
    domain              : example.com
  get system dns
    primary             : 172.16.95.19
    secondary           : 0.0.0.0
    domain              : example.com
```

The first output from `get` indicates the value that you have configured but not yet saved; the second output from `get` indicates the value that was last saved to disk.

If you were to now enter `end`, saving your setting to disk, `get` output for both syntactical forms would again match. However, if you were to enter `abort` at this point and discard your recently entered secondary DNS setting instead of saving it to disk, the FortiWeb unit's configuration would therefore match the second output, not the first.

Tip: If you have entered settings but cannot remember how they differ from the existing configuration, the two different forms of `get`, with and without the object name, can be a useful way to remind yourself.

Most `get` commands, such as `get system dns`, are used to display configured settings. You can find relevant information about such commands in the corresponding config commands in the `config` chapter.

Other `get` commands, such as `get system performance`, are used to display system information that is ***not*** configurable. This chapter describes this type of `get` command.

The get commands require at least read (r) permission to applicable administrator profile groups.

This chapter describes the following commands.

get router all

get system logged-users

get system performance

get system status

Note: Although not explicitly shown in this section, for all `config` commands, there are related `get` and `show` commands which display that part of the configuration. `get` and `show` commands use the same syntax as their related `config` command, unless otherwise mentioned. For syntax examples and descriptions of each configuration object, field, and option, see "config" on page 37.

router all

Use this command to display the list of configured static routes.

Syntax

```
get router all
```

Example

```
get router all
IP                  Mask                Gateway             Distance     Device
0.0.0.0             0.0.0.0             172.22.14.1         10           port1
192.168.1.0         255.255.255.0       192.168.1.10        0            port4
```

History

FortiWeb v3.2.0 New.

Related topics

- config router static

system logged-users

Displays the administrators that are currently logged in to the FortiWeb unit via the local console, web-based manager, or CLI (including through the JavaScript-based *CLI Console* widget of the web-based manager).

For information on allowing only one administrator to be logged in at any given time, see “config system global” on page 134.

Syntax

```
get system logged-users
```

Example

```
get system logged-users
INDEX USERNAME        TYPE  FROM                  TIME
    0 admin           cli   jsconsole             Sun Jul  4 22:22:38 2009

    1 admin           cli   ssh(172.16.1.20)      Sun Jul  4 20:47:59 2009
```

History

FortiWeb v3.2.0 New.

Related topics

- config system admin
- config system global

system performance

Displays the FortiWeb unit's CPU usage, memory usage and up time.

Syntax

```
get system performance
```

Example

```
get system performance
CPU states:    4% used, 96% idle
Memory states: 18% used
Up:            4 days,  11 hours,  38 minutes.
```

History

FortiWeb v3.2.0 New.

Related topics

- get system status

system status

Use this command to display system status information including:

- FortiWeb firmware version, build number and date
- FortiWeb unit serial number and BIOS version
- log hard disk availability
- host name
- current HA status

Syntax

```
get system status
```

Example

```
get system status
  International Version:FortiWeb-1000B 3.30,build098,090702
  Serial-Number:FV-1KB3M08600012
  Bios version:00010009
  Log hard disk:Available
  Hostname:FortiWeb123456789012
  Current HA status: mode=Master, master
```

History

FortiWeb v3.2.0 New.

Related topics

- get system performance

show

The show command displays parts of your FortiWeb unit's configuration in the form of commands that are required to achieve that configuration from the firmware's default state.

The show commands require at least read (r) permission to applicable administrator profile groups.

Note: Although not explicitly shown in this section, for all config commands, there are related get and show commands which display that part of the configuration. get and show commands use the same syntax as their related config command, unless otherwise mentioned. For syntax examples and descriptions of each configuration object, field, and option, see "config" on page 37.

Unlike get, show does ***not*** display settings that are assumed to remain in their default state.

For example, you might show the current DNS settings:

```
show system dns
config system dns
    set primary 172.16.1.10
    set domain "example.com"
end
```

Notice that the command does ***not*** display the setting for the secondary DNS server. This indicates that it has not been configured, or has reverted to its default value.

Depending on whether or not you have specified an object, like get, show may display one of two different outputs: either the configuration that you have just entered but not yet saved, or the configuration as it currently exists on the disk, respectively.

For example, immediately after configuring the secondary DNS server setting but ***before*** saving it, show displays two different outputs (differences highlighted in bold):

```
config system dns
  set secondary 192.168.1.10
  show
config system dns
  set primary 172.16.1.10
  set secondary 192.168.1.10
  set domain "example.com"
end
show system dns
config system dns
  set primary 172.16.1.10
  set domain "example.com"
end
```

The first output from show indicates the value that you have configured but not yet saved; the second output from show indicates the value that was last saved to disk.

Tip: If you have entered settings but cannot remember how they differ from the existing configuration, the two different forms of show, with and without the object name, can be a useful way to remind yourself.

If you were to now enter `end`, saving your setting to disk, `show` output for both syntactical forms would again match. However, if you were to enter `abort` at this point and discard your recently entered secondary DNS setting instead of saving it to disk, the FortiWeb unit's configuration would therefore match the second output, not the first.

Index

Symbols

_email, 26
_fortinet_waf_auth, 235
_fqdn, 26
_index, 26
_int, 26
_ipv4, 26
_ipv4/mask, 26
_ipv4mask, 26
_ipv4range, 26
_ipv6, 26
_ipv6mask, 26
_name, 26
_pattern, 26
_str, 26
_v4mask, 26
_v6mask, 26

Numerics

302 Moved Temporarily, 229
3DES, 22
403 Forbidden, 181, 194, 206, 213, 215, 217, 220, 229, 236, 237
404 File Not Found, 237

A

abort, 28
access profile, 29, 30, 110, 113
action message format (AMF), 235, 240
Active Directory, 161
active-passive, 138
address resolution protocol, 278
address resolution protocol (ARP), 139
admin, 20
admin account, 30
administrator
  access, restricting, 113, 114, 143
  logged in, 310
  netmask, 114
  password, 113
administrator account
  netmask, 114
alert, 181, 194, 206, 213, 214, 215, 216, 217, 220, 235, 248, 262, 263
alert email, 39
alphanumeric, 88, 196
ambiguous command, 24, 32
anonymous, 158
ANSI, 88, 196
ANSI escape code, 88, 196
Apache Tomcat, 90
application-policy, 74
ARP table, 278
ASCII, 33, 34
attributes, XML, 251
authentication, 158, 160, 161, 163, 183, 185
auto-learning, 111

B

batch changes, 19, 35
baud rate, 35, 129
bind DN, 159
bits per second (bps), 20
Black IP, 198
black-listed IPs, 198
Blowfish, 22
boot interrupt, 19
bridge, 92, 156
broadcast, 139
brute force login attack, 170
buffer overflow, 190, 250
buffer, terminal emulator, 35
bypass, 108, 271

C

Cell Command
  basic-severity {Low | Medium | High}, 215
  basic-trigger, 215
  enhanced-severity {Low | Medium | High}, 216
  enhanced-trigger, 216
  full-severity {Low | Medium | High}, 216
  full-trigger, 216
  type-checked {enable | disable}, 195
certificate, 95, 103
  default, 124
  local, 124
  personal, 98
  server, 124
  user, 98
certificate authority (CA), 98, 119, 121, 126
certificate revocation list (CRL), 98, 121, 126
character data (CDATA), 251
character encoding, 96
character entity references, 251
Cisco discovery protocol (CDP), 142
classless inter-domain routing (CIDR), 26
cloaking, 216
cluster, 138
color code, 88, 196
command, 24
  abbreviation, 32
  ambiguous, 24, 32
  completion, 31
  constraints, 15
  help, 31
  incomplete, 24
  interactive, 31
  multi-line, 24, 31
  prompt, 26, 31, 35, 129
  scope, 24, 25

command line interface (CLI), 10, 15, 23, 113
  connecting, 19
  Console widget, 20
  prompt, 135
command prompt, 135
comma-separated value (CSV) format, 64, 88, 196
config, 37
configuration script, 19
conf-sync, 128
console port, 19, 20
content routing, 95, 102
  WSDL, 102
  XPath, 102
Content-Length, 191
Content-Type, 261
conventions, 14
cookie, 235
country code, 88, 196
cp1252, 33
CPU usage, 152, 311
crash log, 269
create-raid, 293
credit card number, 88, 196, 209, 214
cross-site request forgery (CSRF), 200
cross-site scripting (XSS), 116, 210, 212, 235, 240
customer service, 10
cutoff, 271

D

data constraints, 250
data-size
  execute ping-options, 298
dates, 88, 196
daylight savings time (DST), 134
DB-9, 19
debug application, 266
debug cli, 267
debug enable, 270
debug flow, 272
debug settings, 273, 275
debug upload, 276
default
  administrator account, 20, 30
  gateway, 69
  password, 20
  route, 69
denial of service (DoS) attack, 132
DETECT_ALLOW_HOST_FAILED, 95
DETECT_ALLOW_ROBOT, 206
DETECT_ALLOW_ROBOT_GOOGLE, 206
DETECT_ALLOW_ROBOT_MSN, 206
DETECT_ALLOW_ROBOT_YAHOO, 206
DETECT_BRUTE_FORCE_LOGIN, 235
DETECT_MALICIOUS_ROBOT, 237
DETECT_PAGE_RULE_FAILED, 237
DETECT_PARAM_RULE_FAILED, 237
DETECT_RESPONSE_INFORMATION_DISCLOSURE, 216
DETECT_RESPONSE_INFORMATION_disclosure credit
    card leakage, 214
DETECT_SQL_INJECTION, 217
DETECT_START_PAGE_FAILED, 237
DETECT_XSS_ATTACK, 215
df-bit
  execute ping-options, 298
diagnose, 265
Diffie-Hellman exchange, 104
display refresh rate, 134
DNS server, 130
document object model (DOM), 180
document type description (DTD), 250
domain name
  local, 130
dotted decimal, 26

E

elements, XML, 251
Email policy, 46
encoding, 33, 135
environment variables, 32
error message, 24
escape codes, 88, 196
execute, 291
expected input, 15, 23
external entity attack, 261
external schema reference, 261

F

fail open, 133
fail-open, 271
false positive, 40, 187, 209, 215
field, 24
file upload restriction policy, 176
file upload restriction rule, 177
firewall, 68
firmware
  installing, 301
  restoring, 19, 301
firmware partition, 284
Flash, 235, 240
flow, 272
flow control, 20
forensic analysis, 40
FortiAnalyzer, 266
forti-analyzer, 50
fortianalyzer-policy, 51
FortiGuard Distribution Network (FDN), 116
Fortinet
  documentation, 14
  Knowledge Base, 13
Fortinet customer service, 10
FTP server, 276
fully qualified domain name (FQDN), 26

G

gateway, 148
gateway router, 69
GB2312, 33

general entity reference, 251
greedy, 43
group ID, 138

H

hardware, 277
health check, 78, 102
health check, server, 78, 102
heartbeat, 140, 152
hexadecimal, 88, 196
high availability (HA), 138
  cluster, 138
  mode, 138
  pair, 138
Host, 71, 72, 95, 228, 229, 230
host name, 134, 135
HTTP, 68, 78, 143
  headers, 71
HTTP authentication, 158, 160, 161, 163, 183, 185
HTTP_HEADER_LEN_OVERFLOW, 190, 236
HTTP_HEADER_LINE_LEN_OVERFLOW, 190, 236
http-constraints-exceptions, 187
HTTPS, 68, 124, 143
HyperTerminal, 20, 21
hypertext markup language (HTML), 88, 196

I

ICMP ECHO, 78, 143, 156
IEEE 802.1d, 156
IEEE 802.1q, 144
IIS, 90
incomplete command, 24
indentation, 25
index number, 26
injection attack, 209, 213
Inline Protection mode, 144
input constraints, 15, 23
input method, 33
interface address
  resetting, 295
Internet Explorer 6, 135
interval
  health check, 78
inter-VLAN routing, 144
IP address, 143, 152
ip list, 198
IP table, 279
ISO 8859-1, 33

J

Java, 90
JavaScript, 180, 310
jsconsole, 310

K

key, 22, 253
key management group, 261, 263
kill process, 285

L

language, 33, 134, 135
  web-based manager, 135
Layer 2, 144, 156
  loop, 156
Layer 3, 144
LDAP
  bind, 159
  password, 158
  query, 158
LDAPS, 158, 159
limit,rate, 231
line endings, 36
listening ports, 134
load balancing, 95
  algorithm, 102
  weight, 102
local console access, 19
local domain name, 130
locale, 33
Location, 229, 236
login prompt, 20
loop, 156

M

MAIL TO, 164
management information block (MIB), 150, 154
markup, 88, 196
master, 138
maximum transmission unit (MTU), 144
MD5, 136
media access control (MAC), 156
memory usage, 152, 311
Microsoft
  Active Directory, 161
  IIS, 90
  Internet Explorer 6, 135
mode
  high availability (HA), 138
  inline protection, 144
  offline protection, 148
  reverse proxy, 148
  transparent, 133, 144
  transparent inspection, 148
  true transparent proxy, 148
more, 35, 129
mount, 286
multi-line command, 24, 31
multiple pages, 129

N

netmask, 114, 143
  administrator account, 114
network address translation (NAT), 92, 156, 171, 206
network interface
  heartbeat, 139
  SNMP monitoring, 152

network route, 280
next-hop router, 69
no object in the end, 24
NT LAN Manager (NTLM), 161
NTP
  synchronization, 134
null modem, 20, 21

O

object, 24
Offline Protection mode, 92, 148
offloading, 97, 124
one-arm, 108
Online Certificate Status Protocol (OCSP), 98, 126
operation mode, 92, 148, 274
  switching, 148
option, 24
oversized payload, 250

P

packet
  capture, 281
  payload, 40, 65
  trace, 281
packets, 281
paging, 129
pair, 138
parity, 20
password, 20, 113
  LDAP bind, 158
  lost, 30
  reset, 30
  weak, 88
pattern, 26
  execute ping-options, 298
PCI DSS, 214
peer, 128
peer connection, 20
permissions, 29, 30, 110, 113
phone number, 88, 196
ping, 78, 143, 156
plain text editor, 35
policy
  and operation mode, 92
  SNMP monitoring, 152
port number, 97
postal code, 88, 196
power interruption, 133
predefined, 107
processing instruction (PI), 251
proxy, 237

Q

query
  anonymous, 158
  DNS, 130
  LDAP, 158

R

RADIUS, 162
radius-user, 162
RAID disks, 287
rapid spanning tree protocol (RTSP), 156
rate limit, 231
reachable, 69
recursive payload, 250
recursive URL encoding, 96
redirect, 228, 229
Referer, 228, 229, 230, 236
regular expression, 26, 40, 42, 88, 168, 194, 201, 210, 221, 225, 230, 231
repeat-count
  execute ping-options, 298
report
  on demand, 53
  periodically generated, 53
representational state transfer (REST), 261
reset, 275
reset password, 30
restoring the firmware, 19
retry
  health check, 78
reverse proxy, 144
Reverse Proxy mode, 148
rewrite, 228, 229
RFC
  2616, 118, 230
RJ-45, 21
robot, 205
  control sensor, 205
  custom, 231
  group, 242
root, 30
route
  by XPath, 102
  content, 102
  default, 69
  static, 69
  web service operations, 102
route table, 280
RTF bookmarks, 88, 196

S

schema poisoning attack, 261
Secure Shell (SSH), 19, 20, 21, 22, 143
  key, 22
sensitive information, 212
serial communications (COM) port, 20, 21
Server, 216
server
  farm, 92
  health check, 78, 102
  status, 78, 102
session timeout, 96
Session-Id, 241
Shift-JIS, 33
show, 313

signing chain, 96
simple network management protocol (SNMP), 150
slave, 138
sniffer, 281
SNMP, 143
  change of IP address, 152
  configuring community, 150
  CPU usage, 152
  event, 152
  HA monitoring, 152
  manager, 150, 154
  memory usage, 152
  policy change monitoring, 152
  system name, 135
Social Insurance Number (SIN), 88, 196
Social Security Number (SSN), 88, 196
source
  execute ping-options, 298
spanning-tree protocol (STP), 156
special characters, 33
spider, 205
SQL
  injection, 116, 211, 212, 235, 240, 261
  statements, 88, 196
SSL, 9, 97, 104, 124, 158
  certificate, 95, 103
  hardware accelerated, 97
  offload, 97
  on the web servers, 149
SSL v2 support, 136
standalone, 138
STARTTLS, 158, 159
state name, 88, 196
static route, 69
status
  server, 78, 102
string, 26
sub-command, 24, 25, 26, 28
subnet, 143
SYN flood, 132
synchronize, 128
syntax, 15, 23
Syslog, 64

T

table, 24
TCP, 107, 283
  session timeout, 96
  SYN flood, 132
technical support, 10
Telnet, 19, 20, 21, 23, 143
text node, 251
text/xml, 261
time zone, 134
timeout, 96
  execute ping-options, 298
  health check, 78
  TCP session, 96
times, 88, 196
timestamp, 268
tips and tricks, 30
TLS, 97, 104
Tomcat, 90
top processes, 288
tos
  execute ping-options, 298
trace, 272, 281
Transparent Inspection mode, 148
Transparent mode, 92, 133, 142, 144, 148
transport layer security (TLS), 119
traps, 150
troubleshooting, 265
trusted host, 114
trusted IPs, 198
ttl
  execute ping-options, 298

U

UDP, 107, 283
UK vehicle registration, 88, 196
Unicode, 33
uniform resource identifier (URI), 88, 196
unknown action, 24
up time, 311
URL
  encoding, 96
  rewrite, 227, 228
url- replacer, 76
US-ASCII, 33, 34, 135
User-Agent, 231
UTF-8, 33, 135

V

validate-reply
  execute ping-options, 298
value, 24
value parse error, 24, 26
VBScript, 88, 196
view-settings
  execute ping-options, 298
virtual LAN (VLAN), 144
virtual MAC, 139
virtual server, 92, 98
VLAN, 142
VLAN trunk, 144

W

W3C XML Schema, 250
waf file-upload-restriction-policy, 176
waf file-upload-restriction-rule, 177
waf http-constraints-exceptions, 187
waf ip-list, 198
web crawler, 205
web service definition language (WSDL), 102, 257
  content routing, 95
  scanning attack, 262
  verification, 262
web vulnerability scan policy, 243

web vulnerability scan schedule, 246
web-based manager
  language, 135
wiki code, 88, 196
wild cards, 26
WSDL
  verification, 262
wvs, 246
wvs policy, 243
wvs profile, 245
wvs schedule, 246

X

X-Forwarded-For, 237, 238
XML
  attributes, 251
  decryption, 261, 262
  elements, 251
  encryption, 261, 262
  signature, 261, 263
XML namespace (XMLNS), 251
XPath, 95, 102, 259, 262, 263
  content filter rule, 247, 248
  expression, 104

Z

ZIP code, 88, 196

www.fortinet.com

www.fortinet.com