WEB APPLICATION FIREWALL

FortiWeb CLI Reference

VERSION 5.6

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

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

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com

September 23, 2016

FortiWeb 5.6 CLI Reference

1st Edition

TABLE OF CONTENTS

Introduction 26
- Scope 26
- Conventions 27
  - IP addresses 27
  - Cautions, notes, & tips 27
  - Typographic conventions 28
  - Command syntax 28

What's new 29

Using the CLI 61
- Connecting to the CLI 61
  - Connecting to the CLI using a local console 61
  - Enabling access to the CLI through the network (SSH or Telnet or CLI Console widget) 62
  - Connecting to the CLI using SSH 64
  - Connecting to the CLI using Telnet 65
- Command syntax 66
  - Terminology 66
  - Indentation 67
  - Notation 68
- Subcommands 71
  - Table commands 72
    - Example of table commands 73
  - Field commands 73
    - Example of field commands 74
- Permissions 74
- Tips & tricks 77
  - Help 78
  - Shortcuts & key commands 78
  - Command abbreviation 79
  - Special characters 79
  - Language support & regular expressions 80
  - Screen paging 83
  - Baud rate 83
  - Editing the configuration file in a text editor 83
- Administrative domains (ADOMs) 84

Defining ADOMs 86
Assigning administrators to an ADOM 87
config 89
log alertemail 92
Syntax 92
Example 92
Related topics 93
log attack-log 93
Syntax 93
Example 95
Related topics 95
log custom-sensitive-rule 95
Syntax 96
Example 97
Related topics 98
log disk 98
Syntax 98
Example 99
Related topics 99
log email-policy 100
Syntax 100
Example 102
Related topics 102
log event-log 103
Syntax 103
Example 104
Related topics 104
log forti-analyzer 104
Syntax 105
Example 105
Related topics 106
log fortianalyzer-policy 106
Syntax 106
Example 107
Related topics 107
log ftp-policy 107
Syntax 107
Related topics 108
log reports 108
Syntax 109
Example 117
Related topics 118

log sensitive 118
Syntax 119
Example 119
Related topics 119
log siem-message-policy 119
Syntax 120
Example 120
Related topics 120
log siem-policy 121
Syntax 121
Example 122
Related topics 122
log syslogd 122
Syntax 122
Example 123
log syslog-policy 123
Syntax 124
Example 124
Related topics 125
log traffic-log 125
Syntax 125
Example 126
Related topics 126
log trigger-policy 126
Syntax 126
Example 127
Related topics 128
router policy 128
Syntax 128
Related topics 129
router setting 129
Syntax 130
Example 131
Related topics 131
router static 131
Syntax 132
Example 132
Related topics 133
server-policy allow-hosts 133
Syntax 134
Example 135
Related topics 136

server-policy custom-application application-policy 136
Syntax 136
Example 137
Related topics 137
server-policy custom-application url-replacer 137
Syntax 139
Example 141
Related topics 141
server-policy health 142
Syntax 142
Example 146
Related topics 146
server-policy http-content-routing-policy 146
Syntax 147
Example 152
Related topics 153
server-policy pattern custom-data-type 153
Syntax 153
Example 153
Related topics 154
server-policy pattern custom-global-white-list-group 154
Syntax 154
Example 156
Related topics 156
server-policy pattern custom-susp-url 156
Syntax 156
Example 157
Related topics 157
server-policy pattern custom-susp-url-rule 157
Syntax 157
Example 158
Related topics 158
server-policy pattern data-type-group 158
Syntax 159
Example 163
Related topics 164
server-policy pattern suspicious-url-rule 164
Syntax 164
Example 165
Related topics 166
server-policy persistence-policy 166
Syntax 166

Example 170
Related topics 171
server-policy policy 171
Syntax 172
Example 189
Related topics 189
server-policy server-pool 190
Syntax 190
Example 206
Related topics 207
server-policy service custom 207
Syntax 207
Example 208
Related topics 208
server-policy service predefined 208
Syntax 208
Example 209
Related topics 209
server-policy vserver 209
Syntax 210
Example 211
Related topics 211
system accprofile 211
Syntax 212
Example 214
Related topics 214
system admin 215
Syntax 215
Example 220
Related topics 221
system advanced 221
Syntax 221
Related topics 223
system antivirus 224
Syntax 224
Related topics 225
system autoupdate override 225
Syntax 225
Related topics 226
system autoupdate schedule 226
Syntax 226
Example 227

Related topics 227
system autoupdate tunneling 227
Syntax 228
Example 228
Related topics 228
system backup 229
Syntax 229
Example 231
Related topics 232
system certificate ca 232
Syntax 232
Example 232
Related topics 232
system certificate ca-group 232
Syntax 233
Example 233
Related topics 233
system certificate crl 234
Syntax 234
Related topics 234
system certificate intermediate-certificate 234
Syntax 234
Example 235
Related topics 235
system certificate intermediate-certificate-group 235
Syntax 235
Related topics 236
system certificate local 236
Syntax 236
Example 237
Related topics 237
system certificate sni 238
Syntax 238
Related topics 239
system certificate urlcert 239
Syntax 240
Related topics 240
system certificate verify 240
Syntax 241
Related topics 241
system conf-sync 241
Syntax 242

Related topics 244
system console 244
Syntax 244
Example 245
Related topics 245
system dns 245
Syntax 245
Example 246
Related topics 246
system eventhub 246
Syntax 247
Related topics 247
system fail-open 247
Syntax 248
Related topics 249
system fips-cc 249
system firewall address 249
Syntax 249
Related topics 250
system firewall service 250
Syntax 250
Related topics 251
system firewall firewall-policy 251
Syntax 251
Example 252
Related topics 253
system fortigate-integration 253
Syntax 253
Related topics 254
system fortisandbox 254
Syntax 255
Example 256
Related topics 256
system global 256
Syntax 256
Example 263
Related topics 263
system ha 263
Syntax 264
Example 272
Related topics 273
system hsm info 273

Syntax 273
Related topics 274
system hsm partition 274
Syntax 274
Related topics 275
system interface 275
Syntax 275
Example 282
Example 282
Related topics 283
system ip-detection 283
Syntax 283
Related topics 283
system network-option 283
Syntax 284
Example 286
Related topics 287
system raid 287
Syntax 287
Example 288
Related topics 288
system replacemsg 288
Syntax 288
Related topics 289
system replacemsg-image 290
Syntax 290
Related topics 290
system settings 290
Syntax 292
Related topics 293
system snmp community 294
Syntax 294
Example 298
Related topics 298
system snmp sysinfo 298
Syntax 299
Example 299
Related topics 300
system snmp user 300
Syntax 301
Example 304
Related topics 305

system v-zone 305
Syntax 305
Example 306
Related topics 306
system wccp 307
Syntax 307
Example 310
Related topics 310
user admin-usergrp 310
Syntax 310
Example 311
Related topics 311
user kerberos-user 311
Syntax 312
Related topics 312
user ldap-user 312
Syntax 313
Example 315
Related topics 316
user local-user 316
Syntax 316
Example 317
Related topics 317
user ntlm-user 317
Syntax 317
Example 318
Related topics 318
user radius-user 318
Syntax 319
Related topics 320
user user-group 320
Syntax 321
Example 322
Related topics 322
wad file-filter 322
Syntax 322
Example 323
Related topics 324
wad website 324
Syntax 324
Example 327
Related topics 328

waf allow-method-exceptions 328
Syntax 328
Example 330
Related topics 331
waf allow-method-policy 331
Syntax 331
Example 332
Related topics 333
waf application-layer-dos-prevention 333
Syntax 333
Example 335
Related topics 335
waf base-signature-disable 335
Syntax 335
Example 336
Related topics 336
waf brute-force-login 336
Syntax 336
Example 339
Related topics 339
waf cookie-security 339
Syntax 339
Related topics 343
waf csrf-protection 344
Syntax 344
Example 346
waf custom-access policy 347
Syntax 347
Example 348
Related topics 348
waf custom-access rule 348
Syntax 349
Example 358
Related topics 359
waf custom-protection-group 359
Syntax 359
Example 360
Related topics 360
waf custom-protection-rule 360
Syntax 360
Example 365
Related topics 366

waf exclude-url 366
Syntax 366
Example 367
Related topics 367
waf file-compress-rule 367
Syntax 368
Example 369
Related topics 369
waf file-uncompress-rule 369
Syntax 370
Example 371
Related topics 371
waf file-upload-restriction-policy 371
Syntax 372
Related topics 374
waf file-upload-restriction-rule 375
Syntax 375
Example 377
Related topics 378
waf geo-block-list 378
Syntax 378
Example 379
Related topics 380
waf geo-ip-except 380
Syntax 380
Example 381
Related topics 381
waf hidden-fields-protection 381
Syntax 381
Related topics 382
waf hidden-fields-rule 382
Syntax 383
Example 386
Related topics 386
waf http-authen http-authen-policy 386
Syntax 387
Example 388
Related topics 389
waf http-authen http-authen-rule 389
Syntax 389
Example 391
Related topics 391

waf http-connection-flood-check-rule 391
Syntax 392
Related topics 394
waf http-constraints-exceptions 394
Syntax 394
Example 397
Related topics 398
waf http-protocol-parameter-restriction 398
Syntax 398
Example 405
Related topics 406
waf http-request-flood-prevention-rule 406
Syntax 406
Example 408
Related topics 408
waf input-rule 408
Syntax 409
Example 413
Related topics 414
waf ip-intelligence 414
Syntax 414
Example 416
Related topics 417
waf ip-intelligence-exception 417
Syntax 417
Example 417
Related topics 417
waf ip-list 418
Syntax 418
Example 420
Related topics 420
waf layer4-access-limit-rule 420
Syntax 420
Example 423
Related topics 424
waf layer4-connection-flood-check-rule 424
Syntax 424
Example 426
Related topics 426
waf padding-oracle 426
Syntax 426
Example 430

Related topics 431
waf page-access-rule 431
Syntax 432
Example 433
Related topics 434
waf parameter-validation-rule 434
Syntax 434
Example 435
Related topics 435
waf signature 435
Syntax 437
Example 448
Related topics 449
waf site-publish-helper authentication-server-pool 449
Syntax 449
Example 450
Related topics 450
waf site-publish-helper keytab_file 450
waf site-publish-helper policy 450
Syntax 450
Example 451
Related topics 451
waf site-publish-helper rule 452
Syntax 453
Example 461
Related topics 462
waf start-pages 462
Syntax 463
Example 466
Related topics 466
waf url-access url-access-policy 466
Syntax 467
Example 467
Related topics 468
waf url-access url-access-rule 468
Syntax 468
Example 472
Related topics 473
waf url-rewrite url-rewrite-policy 473
Syntax 473
Related topics 474
waf url-rewrite url-rewrite-rule 474

Syntax 475
Related topics 481
waf user-tracking policy 481
Syntax 482
waf user-tracking rule 482
Syntax 483
Example 488
Related topics 488
waf web-cache-exception 489
Syntax 489
Related topics 490
waf web-cache-policy 491
Syntax 491
Related topics 494
waf web-protection-profile autolearning-profile 494
Syntax 495
Related topics 496
waf web-protection-profile inline-protection 496
Syntax 497
Related topics 508
waf web-protection-profile offline-protection 509
Syntax 510
Related topics 517
waf x-forwarded-for 517
Syntax 517
Example 520
wvs policy 521
Syntax 521
Example 522
Related topics 522
wvs profile 523
Syntax 523
Example 523
Example 523
Related topics 524
wvs schedule 524
Syntax 524
Example 525
Related topics 525
diagnose 526
debug 527
Syntax 528

Related topics ... 528
debug application autolearn ... 529
Syntax ... 529
Related topics ... 529
debug application detect ... 530
Syntax ... 530
Related topics ... 530
debug application dssl ... 530
Syntax ... 531
Related topics ... 531
debug application fds ... 531
Syntax ... 531
Related topics ... 532
debug application hasync ... 532
Syntax ... 532
Example ... 533
Related topics ... 534
debug application hatalk ... 535
Syntax ... 535
Example ... 535
Related topics ... 536
debug application http ... 536
Syntax ... 537
Related topics ... 537
debug application miglogd ... 537
Syntax ... 537
Related topics ... 538
debug application mulpattern ... 538
Syntax ... 538
Related topics ... 539
debug application proxy ... 539
Syntax ... 539
Related topics ... 540
debug application proxy-error ... 540
Syntax ... 540
Related topics ... 540
debug application snmp ... 541
Syntax ... 541
Related topics ... 541
debug application ssl ... 541
Syntax ... 541
Example ... 542

Related topics 542
debug application sysmon 542
Syntax 542
Related topics 543
debug application ustack 543
Syntax 543
Related topics 543
debug application waf-fds-update 544
Syntax 544
Related topics 544
debug cli 544
Syntax 544
Related topics 545
debug cmdb 545
Syntax 545
Related topics 545
debug comlog 546
Syntax 546
Related topics 546
debug console timestamp 546
Syntax 546
Related topics 547
debug crashlog 547
Syntax 547
Example 547
debug dnsproxy list 547
Syntax 548
Example 548
Related topics 548
debug emerglog 548
Syntax 548
debug flow filter 548
Syntax 548
Related topics 549
debug flow filter module-detail 549
Syntax 549
Related topics 550
debug flow reset 550
Syntax 550
Related topics 550
debug flow trace 550
Syntax 550

Example 551
Related topics 553
debug info 553
Syntax 553
Example 553
Related topics 554
debug init 554
Syntax 554
debug reset 555
Syntax 555
Related topics 555
debug upload 556
Syntax 556
Example 556
Related topics 556
hardware check 556
Syntax 557
Example 557
hardware cpu 557
Syntax 557
Example 557
Related topics 558
hardware fail-open 558
hardware harddisk 558
Syntax 558
Example 558
Related topics 559
hardware interrupts 559
Syntax 559
Example 559
Related topics 560
hardware logdisk info 560
Syntax 560
Example 560
Related topics 560
hardware mem 561
Syntax 561
Example 561
Related topics 562
hardware nic 562
Syntax 562
Example 563

Related topics 564
hardware raid list 564
Syntax 564
Example 565
Related topics 565
index 565
Syntax 565
Example 566
Related topics 566
log 566
Syntax 566
Example 566
Related topics 567
network arp 567
Syntax 567
Example 567
Related topics 568
network ip 568
Syntax 568
Example 568
Example 569
Related topics 569
network route 569
Syntax 569
Example 570
Example 570
Related topics 570
network rtcache 571
Syntax 571
Example 571
Example 571
Related topics 572
network sniffer 572
Syntax 572
Example 574
Example 575
Example 575
network tcp list 580
Syntax 580
Example 580
Related topics 581
network udp list 581

Syntax 581
Example 581
Related topics 582
policy 582
Syntax 582
Example 583
Related topics 583
system flash 583
Syntax 583
Example 584
Related topics 584
system ha file-stat 584
Syntax 584
Example 584
Related topics 585
system ha mac 585
Syntax 585
Example 585
Related topics 585
system ha status 586
Syntax 586
Example 586
Related topics 586
system ha sync-stat 586
Syntax 586
Example 587
Related topics 587
system kill 587
Syntax 587
Related topics 588
system mount 588
Syntax 588
Example 588
Related topics 589
system top 589
Syntax 589
Example 589
Related topics 590
system update info 590
Syntax 591
Example 591
execute 593

backup cli-config 593
Syntax 594
Example 595
Related topics 595
backup full-config 595
Syntax 595
Example 596
Related topics 596
certificate ca 596
Syntax 596
Example 597
Related topics 597
certificate crl 597
Syntax 598
Example 598
Related topics 599
certificate inter-ca 599
Syntax 599
Example 600
Related topics 600
certificate local 600
Syntax 600
Example 601
Related topics 601
create-raid level 601
Syntax 602
Related topics 602
create-raid rebuild 602
Syntax 602
Example 602
Related topics 603
date 603
Syntax 603
Example 603
Related topics 603
db rebuild 603
Syntax 604
Related topics 604
erase-disk 604
Syntax 604
factoryreset 604
Syntax 605

Related topics 605
formatlogdisk 605
Syntax 605
Related topics 605
ha disconnect 605
Syntax 606
Example 606
Related topics 606
ha manage 607
Syntax 607
Example 607
Related topics 607
ha md5sum 608
Syntax 608
Example 608
Related topics 608
ha synchronize 608
Syntax 609
Example 609
Related topics 609
ping 610
Syntax 610
Example 610
Example 610
Related topics 611
ping6 611
Syntax 611
Example 611
Related topics 612
ping-options 612
Syntax 612
Example 613
Related topics 614
ping6-options 614
Syntax 614
Example 615
Related topics 615
reboot 615
Syntax 616
Example 616
Related topics 616
restore config 616

Syntax 616
Example 617
Related topics 617
restore image 617
Syntax 617
Example 618
Related topics 618
restore secondary-image 618
Syntax 619
Example 619
Related topics 619
restore vmlicense 619
Syntax 620
Example 620
session-cleanup 620
Syntax 620
shutdown 621
Syntax 621
Example 621
Related topics 621
telnet 621
Syntax 622
Example 622
Related topics 622
telnettest 622
Syntax 622
Example 623
Related topics 623
time 623
Syntax 623
Example 624
Related topics 624
traceroute 624
Syntax 624
Example 625
Example 625
Example 625
Related topics 625
update-now 626
Syntax 626
get 627
router all 628

Syntax 628
Example 629
Related topics 629
system fortisandbox-statistics 629
Syntax 629
Example 629
Related topics 629
system logged-users 630
Syntax 630
Example 630
Related topics 630
system performance 630
Syntax 630
Example 631
Related topics 631
system status 631
Syntax 631
Example 631
Related topics 632
waf signature-rules 632
Syntax 632
Example 632
Related topics 633
show 634

Introduction

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

Scope

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

At this stage:

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

Once that basic installation is complete, you can use this document. This document explains how to use the CLI to:

- Update the FortiWeb appliance.
- Reconfigure features.
- Use advanced features, such as XML protection and reporting.
- Diagnose problems.

This document does **not** cover the web UI nor first-time setup. For that information, see the *FortiWeb Administration Guide*.

Conventions

This document uses the conventions described in this section.

IP addresses

To avoid IP conflicts that would occur if you used examples in this document with public IP addresses that belong to a real organization, the IP addresses used in this document are fictional. They belong to the private IP address ranges defined by these RFCs.

RFC 1918: Address Allocation for Private Internets

http://ietf.org/rfc/rfc1918.txt?number-1918

RFC 5737: IPv4 Address Blocks Reserved for Documentation

http://tools.ietf.org/html/rfc5737

RFC 3849: IPv6 Address Prefix Reserved for Documentation

http://tools.ietf.org/html/rfc3849

For example, even though a real network's Internet-facing IP address would be routable on the public Internet, in this document's examples, the IP address would be shown as a non-Internet-routable IP such as 10.0.0.1, 192.168.0.1, or 172.16.0.1.

Cautions, notes, & tips

This document uses the following guidance and styles for notes, tips and cautions.

Warns you about procedures or feature behaviors that could have unexpected or undesirable results including loss of data or damage to equipment.

Highlights important, possibly unexpected but non-destructive, details about a feature's behavior.

Presents best practices, troubleshooting, performance tips, or alternative methods.

Typographic conventions

Convention	Example
Button, menu, text box, field, or check box label	From **Minimum log level**, select **Notification**.

CLI input	`config system dns`
	`  set primary <address_ipv4>`
	`end`

CLI output	`FortiWeb# diagnose hardware logdisk info`
	`disk number: 1`
	`disk[0] size: 31.46GB`
	`raid level: no raid exists`
	`partition number: 1`
	`mount status: read-write`

Emphasis	HTTP connections are **not** secure and can be intercepted by a third party.
File content	<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4>
Hyperlink	https://support.fortinet.com
Keyboard entry	Type a name for the remote VPN peer or client, such as `Central_Office_1`.
Navigation	Go to **VPN** > **IPSEC** > **Auto Key (IKE)**.
Publication	For details, see the *FortiWeb Administration Guide*.

Command syntax

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

For command syntax conventions such as braces, brackets, and command constraints such as `<address_ipv4>`, see Notation on page 68.

What's new

The tables below list commands which have changed in FortiWeb 5.4 and later, including new commands, syntax changes, and new setting options.

FortiWeb 5.6

Command	Change
`config log siem-policy`	

`edit <policy_name>`
`config siem-server-list`
`edit <entry_index>`
`set type <arcsight-cef | azure-cef>`
	Changed. When FortiWeb-VM is deployed on Azure, you can now configure a SIEM policy that connects to Azure Security Center.

`config system eventhub`	New. When FortiWeb-VM is deployed on Azure, you can now configure the FortiWeb appliance to send log messages to Azure Security Center (ASC).

`set status {enable | disable}`
`set appliance_id <subscription_str>`
`set policy_saskey <primary-key_str>`
`set policy_name <policy-name_str>`
`set eventhub_name <ehub-name_str>`
`set servicebus_namespace <servicebus-namespace_str>`	

`config system firewall address`	New. You can configure IP addresses and address ranges that FortiWeb's built-in stateful firewall uses.

`edit <firewall-address_name>`
`set type {ip-netmask | ip-range}`
`set ip-netmask <firewall-address_ipv4mask>`
`set ip-address-value <firewall-address_ipv4>`	

Command	Change
config system firewall firewall-policy	New. You can configure FortiWeb's built-in stateful firewall to allow and deny TCP, UDP, and ICMP traffic.
set default-action {deny | accept} edit <entry_index> set in-interface <incoming_ interface_ name> set out-interface <outgoing_ interface_ name> set src-address <firewall-address_ name> set dest-address <firewall-address_ name> set service <firewall-service_name> set action {deny | accept}	
config system firewall service	New. You can configure the ports and protocols that FortiWeb's built-in stateful firewall uses
edit <firewall-service_ name> set protocol {TCP | UDP | ICMP} set source-port-min <source-port-min_ int> set source-port-max <source-port-max_ int> set destination-port-min <source-port-min_int> set destination-port-max <source-port-max_int>	
config system global	New. You can now configure FortiWeb to scan partial TCP connections.
set anypktstream {enable | disable}	
config system interface	

Command	Change
set allowaccess {http https ping snmp ssh telnet FWB-manager} set ip6-allowaccess {http https ping snmp ssh telnet FWB-manager} set mtu <mtu_int>	Changed. You now configure access to a FortiWeb appliance from FortiWeb Manager using a specific FortiWeb Manager administrative access option.
config waf cookie-security	New. You can now configure FortiWeb features that prevent cookie-based attacks as a policy you apply using a web protection profile.
edit <cookie-security_name> set security-mode {no |encrypted | signed} set action {alert |alert_deny | remove_cookie} set block-period <block-period_int> set severity {High |Medium | Low} set trigger <trigger-policy_name> set cookie-replay-protection-type {no | IP} set max-age <max-age_int> set secure-cookie {enable | disable} set http-only {enable | disable} set allow-suspicious-cookies(Never |Always | Custom} set allow-time <time_str> config cookie-security-exception-list edit <entry_index> set cookie-name <cookie-name_str> set cookie-domain <cookie-domain_str> set cookie-path <cookie-path_str> end next end	
config waf site-publish-helper authentication-server-pool	New. Site publishing rules now authenticate clients using a member of a pool of authentication servers.

Command	Change
edit <authentication-server-pool_name> edit <entry_index> set server-type {ldap | radius} set ldap-server <ldap-query_name> set radius-server <radius-query_name> set rsa-securid {enable | disable} end next end	
config waf site-publish-helper policy	New. You can now configure FortiWeb to prevent users from making further attempts to log in after a specified number of failed login attempts.
edit <site-publish-policy_name> set account-lockout {enable | disable} set lockout-threshold <lockout-threshold_int> set account-block-period <account-block-period_int> set reset-time <reset-time_int>	
config log email-policy	
edit <email-policy_name> set attach-compression {enable | disable}	New. You can enable/disable the compression (.zip) to attached event logs and alerts for an alert email policy.

FortiWeb 5.5 Patch 4

Command	Change
config log attack-log	

Command	Change
set packet-log {anti-virus-detection | cookie-security | custom-access | custom-protection-rule | fsa-detection | hidden-fields-failed | http-protocol-constraints | illegal-file-type | illegal-xml-format | ip-intelligence | padding-oracle | parameter-rule-failed | signature-detection | illegal-json-format | trojan-detection | illegal-filesize | csrf-detection | user-tracking-detection | account-lockout-detection}	New. You can now configure FortiWeb to keep the packet payloads associated with additional detected attack types or validation failures.
config server-policy http-content-routing-policy	
edit <routing-policy_name> config content-routing-match-list edit <entry_index> set match-object {http-host | http-request | url-parameter | http-referer | http-cookie | http-header | source-ip | x509-certificate-Subject | x509-certificate-Extension} set x509-subject-name {E | CN | OU | O | L | ST | C}	Changed. The HTTP content routing policy settings that match X509 certificate content now allow you to match values found in either in the client certificate's extension field or subject field.
config server-policy policy	
edit <policy_name> set client-real-ip {enable | disable}	New. By default, when the operation mode is reverse proxy, the source IP for connections between FortiWeb and back-end servers is the address of a FortiWeb network interface. You can now configure FortiWeb to use the source IP address of the client that originated the request when it connects to a back-end server on behalf of that client.
config system fortisandbox	

Command	Change
set cache-timeout <timeout_int>	New. You can now enter how long FortiWeb waits before it clears the hash table entry for an uploaded file that was evaluated by FortiSandbox.
config system v-zone	
edit <bridge_name> set use-interface-macs {<interface_name> <interface_name> ...}	New. You can now specify the names of network interfaces that are members of the bridge and send and transmit traffic using the MAC address of their corresponding FortiWeb network interface.
config waf csrf-protection	New. You can now configure FortiWeb to protect against cross-site request forgery (CSRF)

Command	Change

```
edit <csrf-rule_name>
   set action {alert |
       alert_deny | block-
       period}
   set block-period
       <seconds_int>
   set severity {High |
       Medium | Low}
   set trigger <trigger-
       policy_name>
   config csrf-url-list
      edit <entry_index>
         set host <host_name>
         set request-url <url_
             str>
         set host-status
             {enable |
             disable}
         set request-type
             {plain | regular}
         set parameter-filter
             {enable |
             disable}
         set parameter-name
             <parameter-name_
             str>
         set parameter-value-
             type
             {plain | regular}
         set parameter-value
             <parameter-value_
             str>
      next
   end
   config csrf-url-list
      edit <entry_index>
         set host <host_name>
         set request-url <url_
             str>
         set host-status
             {enable |
             disable}
         set request-type
             {plain | regular}
         set parameter-filter
             {enable |
             disable}
         set parameter-name
             <parameter-name_
             str>
         set parameter-value-
             type
             {plain | regular}
         set parameter-value
             <parameter-value_
             str>
```

Command	Change
config waf custom-access rule	
edit <custom-access_name> config source-ip-filter edit <entry_index> set source-ip <ip_range> end config user-filter edit <entry_index> set reverse-match {no | yes} set user-name <user-name_str>	New. In advanced access custom rules, you can now specify the IP address to match using a range of addresses and filter requests using a user name.
config waf file-upload-restriction-policy	
edit <file-upload-restriction-policy_name> set trojan-detection {enable |disable}	New. A file upload restriction policy can now scan for Trojans.
config waf http-protocol-parameter-restriction	
edit <http-constraint_name> set web-socket-protocol-check {enable | disable}	New. A HTTP protocol constraint can now detect traffic that uses the WebSocket TCP-based protocol.
config waf user-tracking policy	New. You can now configure FortiWeb to track sessions by user and capture a username to reference in traffic and attack log messages.
edit <user-tracking-policy_name> config input-rule-list edit <entry_index> set input-rule <input-rule_name>	
config waf user-tracking rule	New. You can now configure FortiWeb to track sessions by user and capture a username to reference in traffic and attack log messages. You can also use this feature to prevent a session fixation attack and set a period of time during which FortiWeb blocks requests with a session ID from a timed-out session.

Command	Change
edit <rule_name> set authentication-url <url_str> set username-parameter <username_str> set password-parameter <password_str> set session-id-name <session-id_str> set logoff-path <logoff_str> set session-fixation-protection { enable | disable} set session-timeout-enforcement { enable | disable} set session-timeout <timeout_int> set session-frozen-time <frozen-time_int> set session-frozen-action { alert | alert_deny | redirect | block-period} set session-frozen-block-period <block-period_int> set session-frozen-severity { High | Medium | Low} set session-frozen-trigger <trigger-policy_name> set default-action { failed | success} config match-condition edit <entry_index> set authentication-result-type { failed | success} set HTTP-match-target { return-code | response-body | redirect-url} set value-type { plain | regular} set value <value-str>	
config waf web-protection-profile inline-protection	

Command	Change
edit <inline-protection-profile_name> set json-protocol-detection {enable | disable} set malformed-json-check {enable | disable} set malformed-json-check-action {alert | alert_deny | block-period} set malformed-json-block-period <block-period_int> set malformed-json-check-severity {High | Medium | Low} set malformed-json-check-trigger <trigger-policy_name> set csrf-protection <rule_name> set user-tracking-policy <user-tracking-policy_name>	New. An inline protection profile can now scan for matches with attack and data leak signatures in JSON data submitted by clients in HTTP requests with `Content-Type:` values `application/json` or `text/json`. In addition, you can use the profile to apply a CSRF protection rule and user tracking policy.
config waf web-protection-profile offline-protection	

Command	Change
edit <offline-protection-profile_name> set json-protocol-detection {enable | disable} set malformed-json-check {enable | disable} set malformed-json-check-action {alert | alert_deny | block-period} set set malformed-json-block-period <block-period_int> set malformed-json-check-severity {High | Medium | Low} set malformed-json-check-trigger <trigger-policy_name> set waf web-protection-profile offline-protection set user-tracking-policy <user-tracking-policy_name>	New. An offline protection profile can now scan for matches with attack and data leak signatures in JSON data submitted by clients in HTTP requests with `Content-Type:` values `application/json` or `text/json`. In addition, you can use the profile to apply a CSRF protection rule and user tracking policy.
execute session-cleanup	New. This command allows you to immediately clean up all sessions

FortiWeb 5.5 Patch 3

Command	Change
config system fortisandbox	
set type {fsa | cloud}	New. You can now configure FortiWeb to upload files to FortiSandbox Cloud for evaluation (requires FortiWeb FortiGuard Sandbox Cloud Service subscription).
config system ha	
set ha-mgmt-status { enable | disable} set ha-mgmt-interface <interface_name>	New. You can now specify a network interface that provides administrative access to an appliance when it is a member of an HA cluster.
config system network-option	

Command	Change
set loopback-mtu <loopback-mtu_int> set tcp-usertimeout <tcp-usertimeout_int> set tcp-keepcnt <tcp-keepcnt_int> set tcp-keepidle <tcp-keepidle_int> set tcp-keepintvl <tcp-keepintvl_int>	New. You can now set a global MTU for v-zones when the operation mode is true transparent proxy and configure how FortiWeb handles clients that keep a connection with FortiWeb open without sending data.
config waf http-constraints-exceptions	
edit <http-exception_name> config http_constraints-exception-list edit <entry_index> set max-http-request-filename-length {enable | disable}	New. You can now create an exception to the HTTP protocol constraint that specifies the maximum acceptable length in bytes of the HTTP request filename.
config waf http-protocol-parameter-restriction	
config waf http-protocol-parameter-restriction edit <http-constraint_name> set max-http-request-filename-length <limit_int>	New. You can now create an HTTP protocol constraint that specifies the maximum acceptable length in bytes of the HTTP request filename.
execute ha manage	Changed. You can now use `execute ha manage` to log into another appliance in the same HA group via the HA link.

FortiWeb 5.5 Patch 2

Command	Change
config log event-log	
set logdisk-high <percentage_int>	New. You can configure FortiWeb to generate an alert when its log disk usage exceeds a percentage you specify.
config system interface	

Command	Change
edit <interface_name> set mtu <mtu_int>	New. You can now configure the maximum transmission unit (MTU) for network interfaces. This configuration allows the network interfaces to support Ethernet frames with more than 1500 bytes of payload.
config system v-zone	
edit <bridge_name> set monitor {enable | disable} set mtu <mtu_int>	New. You can specify whether FortiWeb automatically brings down all members of this v-zone if one member goes down. Also, you can now configure the maximum transmission unit (MTU) for the v-zone. This configuration allows the bridge to support Ethernet frames with more than 1500 bytes of payload.
config system snmp community	
edit <community_index> config hosts edit <snmp-manager_index> set ip {manager_ipv4 | manager_ipv6>	Changed. You can now use an IPv6 address to specify the SNMP manager that can receive traps from and query the FortiWeb appliance.

FortiWeb 5.5 Patch 1

Command	Change
config log attack-log	
set show-all-log {enable | disable}	New. You can specify whether all signature violations that contributed to a threat scoring attack log message are displayed as individual entries in the attack log.
config server-policy server-pool	

Command	Change
edit <server-pool_name> set lb-algo {least-connections | round-robin | weighted-round-robin | uri-hash | full-uri-hash | host-hash | host-domain-hash | src-ip-hash}	Changed. Five new load balancing algorithms determine how to distribute new TCP connections using a hash. FortiWeb generates the hash based on the HTTP request (for example, the URI or host name).
config system antivirus	
set uncomp-size-limit <limit_int>	Changed. The maximum size that you can specify for the memory buffer that FortiWeb uses to temporarily undo the compression that a client or web server has applied to traffic is now 30720 kilobytes (30 MB).
config system global	
set maintainer-user {enable | disable}	New. The `maintainer-user` option enables or disables the maintainer administrator account. This account is enabled by default and allows you to reset the password for the admin account using a console connection.
config system settings	
set fast-forward {enable | disable}	New. Specifies whether FortiWeb activity is restricted to load balancing.
config system wccp	
edit service-id <service-id_int> set cache-engine-method {GRE | L2}	Changed. The WCCP configuration now allows you to select Layer 2 (L2) as the cache engine method. L2 redirection overwrites the original MAC header of the IP packets and replaces it with the MAC header for the WCCP client.
config waf custom-protection-rule	
edit <custom-protection rule_name> set action {alert | alert_deny | alert_erase | redirect | block-period | send_http_response}	Changed. You can now configure FortiWeb to block and reply to clients that violate a signature rule with an HTTP error message (attack block page) instead of resetting the connection.
config waf file-upload-restriction-rule	

Command	Change
edit waf file-upload-restriction-rule [set file-size-limit <size_int>]	Changed. The maximum size that you can specify for a file upload limit is now 30720 kilobytes (30 MB).
config waf signature	

Command	Change
edit <signature-set_name> set threat-scoring_mode {enable | disable} set scoring-threshold {Information-Security | Low-Security | Medium-Security | High-Security | Critical-Security} set scoring-scope {HTTP-Transaction | TCP-Session | HTTP-Session} set scoring-action {alert | alert_deny | redirect | block-period | send_http_response} set scoring-block-period <seconds_int> set scoring-severity {High | Medium | Low} set scoring-trigger config main_class_list edit {010000000 | 020000000 | 030000000 | 040000000 | 050000000 | 060000000 | 070000000 | 080000000 | 090000000 | 100000000} set scoring-status {enable | disable} set action {alert |alert_deny | block-period |only_erase | send_http_response | alert_erase | redirect} config scoring_override_disable_list edit <scoring-override-disable-list_signature-id_str> next end config score_grade_list edit <score-grade-list_signature-id_str> set scoring-grade {Information | Low | Medium | High | Critical} next end	Changed. You can configure your signature policy to take action based on multiple signature violations by a client, instead of a single signature violation. Also, you can now configure FortiWeb to block and reply to clients that violate a signature rule with an HTTP error message (attack block page) instead of resetting the connection.

Command	Change
`diagnose debug dnsproxy list`	New. Allows you to display the DNS cache that stores the results of resolving all fully qualified domain names in the server pools.

FortiWeb 5.5

Command	Change
`config log ftp-policy`	New. You can now configure a connection to a FTP or TFTP server. FortiWeb can use this connection to transmit reports to the server.

`edit <policy_name>`
`set type {ftp | tftp}`
`set server <ftp-server_ipv4>`
`set ftp_auth {enable | disable}`
`set ftp_user <ftp-user_str>`
`set ftp_passwd <ftp_pswd>`
`set ftp-dir <ftp-dir_str>`	

`config log reports`	

`edit <report_name>`
`set output_ftp {html pdf rtf txt mht}`
`set output_ftp_policy <ftp-policy_name>`
	Changed. Report configuration now allows you to automatically send reports to a specified FTP or TFTP server.

`config log fortianalyzer-policy`	

`edit <policy_name>`
`config fortianalyzer-server-list`
`edit <entry_index>`
`set ip-address <forti-analyzer_ipv4>`
`set enc-algorithm {disable | default}`
	Changed. You can now specify connections to multiple FortiAnalyzer instances in a single policy.

`config log siem-policy`	

Command	Change
edit <policy_name> config siem-server-list edit <entry_index> set type cef set port <port_int> set server <siem_ipv4>	Changed. You can now specify connections to multiple ArcSight SIEM servers in a single SIEM policy.
config server-policy health	
edit <health-check_name> configure health-list edit <entry_index> set type {icmp | tcp | http | https | tcp-ssl | tcp-half-open}	Changed. The two new methods for checking the health of a server in a pool are TCP Half Open and TCP SSL.
config server-policy http-content-routing-policy	

Command	Change
edit <routing-policy_name> set server-pool <server-pool_name> config content-routing-match-list edit <entry_index> set match-object {http-host | http-request | url-parameter | http-referer | http-cookie | http-header | source-ip | x509-certificate-Subject | x509-certificate-Extension} set match-condition {match-begin | match-end | match-sub | match-domain | match-dir | match-reg | ip-range | ip-range6 | equal} set match-expression <match-expression_str> set name <name_str> set name-match-condition {match-begin | match-end | match-sub | match-reg | equal} set value <value_str> set value-match-condition {match-begin | match-end | match-sub | match-reg | equal} set start-ip <start_ip> set end-ip <end_ip> set concatenate { and | or }	Changed. You can now route traffic by URL, HTTP parameter, HTTP header, source IP address (single or a range), or an X.509 certificate field. You can also concatenate the routing rules. For example, you can require traffic to match multiple rules or only one rule among many.
config server-policy persistence-policy	

Command	Change
edit <persistence-policy_name> set type { source-ip | persistent-cookie | asp-sessionid | php-sessionid | jsp-sessionid | insert-cookie | http-header | url-parameter | rewrite-cookie | embedded-cookie | ssl-session-id } set cookie-name <cookie-name_str> set timeout <timeout_int> set ipv4-netmask <v4mask> set ipv6-mask-length <v6mask> set http-header <http-header_str> set url-parameter <url-parameter_str> set cookie-path <cookie-path_str> set cookie-domain <cookie-domain_str>	Changed. You can now configure session persistence based on source IP, HTTP header, URL parameter, SSL session ID or additional cookie-based options.
config server-policy policy	
edit <policy_name> set deployment-mode {server-pool | http-content-routing | offline-protection | transparent-servers | wccp-servers} set ssl-custom-cipher {<cipher_1> <cipher2> <cipher3> ...} set ssl-chacha-cipher {enable | disable} set http-pipeline {enable | disable}	Changed. You can now configure a server policy to use when FortiWeb is acting as a WCCP client. In addition to selecting a medium or high-security configuration, you can now select a custom set of cipher suites for a server policy or server pool member. You can add support for the ChaCha-Poly1305 cipher suite. Also, the default setting for `http-pipeline` is `enable`.
config server-policy server-pool	

Command	Change
edit <server-pool_name> set type {offline-protection | reverse-proxy | transparent-servers-for-ti | transparent-servers-for-tp | transparent-servers-for-wccp} config pserver-list edit <entry_index> set conn-limit <conn-limit_int> set ssl-cipher {medium | high | custom} set ssl-custom-cipher {<cipher_1> <cipher2> <cipher3> ...} set ssl-chacha-cipher {enable | disable} set recover <recover_int> set warm-up <warm-up_int> set warm-rate <warm-rate_int>	New. You can configure a server pool to use when the operation mode is WCCP. You can now specify the maximum number of TCP connections that FortiWeb forwards to a pool member. In addition to selecting a medium or high-security configuration, you can now select a custom set of cipher suites for a server policy or server pool member. You can add support for the ChaCha-Poly1305 cipher suite. Also, you can specify how long to wait before sending traffic to a pool member that was recently unavailable, and the rate at which FortiWeb resumes sending traffic.
config system fortigate-integration	
set address <address_ipv4> set port <port_int> set protocol {HTTP | HTTPS} set username <username_str> set password <password_str> set schedule-frequency <schedule-frequency_int> set flag {enable | disable}	New. You can now specify a FortiGate appliance that transmits its list of quarantined source IPs to FortiWeb at regular intervals.
config system global	
set hsm {enable | disable}	New. You can specify whether the configuration settings that integrate FortiWeb with an HSM (hardware security module) are displayed in the web UI.

Command	Change
`config system hsm info`	New. You can now edit the configuration that allows FortiWeb to work with SafeNet Luna SA HSM (hardware security module). This configuration allows FortiWeb to retrieve a per-connection, SSL session key from the HSM instead of loading a local private key and certificate.

`set ip <hsm_ipv4>`
`set port <port_int>`
`set timeout <timeout_int>`
`set filename <filename_str>`
`set action {register | unregister}`	

`config system hsm partition`	New. You can now edit the configuration that allows FortiWeb to work with SafeNet Luna SA HSM (hardware security module).
`edit <partition_name>` `set password <password_int>`	
`config system interface`	
`edit <interface_name>` `set wccp {enable | disable}`	Changed. You can now specify the interfaces that FortiWeb uses to communicate with a FortiGate unit configured as a WCCP server.
`config system settings`	
`set opmode {offline-protection | reverse-proxy | transparent | transparent-inspection | wccp}`	Changed. The new WCCP operation mode allows you to configure FortiWeb as a WCCP client that receives and inspects specified traffic from a FortiGate unit.
`config system snmp user`	New. You can create an SNMP v3 community instead of in addition to SNMP v1 and v2c communities.

Command	Change
edit name <community_str> set status {enable | disable} set security-level {noauthnopriv | authnopriv | authpriv >} set auth-proto {sha1 | md5} set auth-pwd <auth-password_str> set priv-proto {aes | des} set priv-pwd <priv-password_str> set query-status {enable | disable} set query-port <port_int> set trap-status {enable | disable} set trapport-local <port_int> set trapport-remote <port_int> set trapevent {cpu-high | intf-ip | log-full | mem-low | netlink-down-status | netlink-up-status | policy-start | policy-stop | pserver-failed | sys-ha-hbfail | sys-mode-change | waf-access-attack | waf-amethod-attack | waf-blogin-attack |waf-hidden-fields | waf-pvalid-attack | waf-signature-detection | waf-url-access-attack | waf-spage-attack} config hosts edit <snmp-user_index> set ip <manager_ipv4> set system snmp user	
config system wccp	New. You can now configure FortiWeb as a WCCP client that receives and inspects specified traffic from a FortiGate unit or other device acting as a WCCP server.

Command	Change
edit service-id <service-id_int> set cache-id <cache-id_ipv4> set router-list <router-list_ipv4> set group-address <group-address_ipv4> set authentication {enable | disable} set password <passwd_str> set cache-engine-method {GRE | L2} set ports <ports_int> set primary-hash [src-ip | dst-ip | src-port | dst-port} set priority <priority_int> set protocol <priority_int> set assignment-weight <assignment-weight_int> set assignment-bucket-format {ciso-implementation | wccp-v2} set system wccp	
config wad website	
edit <entry_index> set auto {disable | restore | acknowledge}	Changed. The web anti-defacement settings now allow you to configure FortiWeb to automatically acknowledge (accept) any changes that it detects.
config waf custom-protection-rule	

Command	Change
edit <custom-protection rule_name> config meet-condition edit <entry_index> set operator {RE | GT | LT | NE | EQ} set request-target {REQUEST_FILENAME REQUEST_URI REQUEST_HEADERS_ NAMES REQUEST_ HEADERS REQUEST_ COOKIES_NAMES REQUEST_COOKIES ARGS_NAMES ARGS_ VALUE REQUEST_ RAW_URI REQUEST_ BODY CONTENT_ LENGTH HEADER_ LENGTH BODY_ LENGTH COOKIE_ NUMBER ARGS_ NUMBER} set response-target {RESPONSE_BODY RESPONSE_HEADER CONTENT_LENGTH HEADER_LENGTH BODY_LENGTH RESPONSE_CODE} set threshold <threshold_int> set case-sensitive {enable | disable} set expression <regex_pattern>	Changed. You can now specify a value to match for each meet condition rule in a custom signature. The value can be either a regular expression to match or a value to compare to the target's value (greater than, less than, and so on).
config waf http-constraints-exceptions	

Command	Change
edit waf http-constraints-exceptions config http_constraints-exception-list edit waf http-constraints-exceptions set Illegal-content-length-check {enable | disable} set Illegal-content-type-check {enable | disable} set Illegal-header-name-check {enable | disable} set Illegal-header-value-check {enable | disable} set Illegal-responese-code-check {enable | disable} set max-http-body-parameter-length {enable | disable} set max-http-content-length {enable | disable} set max-http-header-length {enable | disable} set max-http-header-name-length {enable | disable} set max-http-header-value-length {enable | disable} set parameter-name-check {enable | disable} set parameter-value-check {enable | disable}	Changed. New exceptions for use with HTTP protocol constraints are now available.
config waf http-protocol-parameter-restriction	

Command	Change
edit <http-constraint_name> set Illegal-content-length-check {enable | disable} set Illegal-content-type-check {enable | disable} set Illegal-header-name-check {enable | disable} set Illegal-header-value-check {enable | disable} set Illegal-response-code-check {enable | disable} set max-http-header-name-length <limit_int> set max-http-header-value-length <limit_int> set parameter-name-check {enable | disable} set parameter-value-check {enable | disable} set Post-request-ctype-check {enable | disable} set waf http-protocol-parameter-restriction	Changed. Additional HTTP protocol constraints are now available.
config waf signature	

Command	Change
edit <signature-set_name> config main_class_list edit {010000000 | 020000000 | 030000000 | 040000000 | 050000000 | 060000000 | 070000000 | 080000000 | 090000000 | 100000000} set fpm-status {enable | disable} config fpm_disable_list edit <fpm-disable-list_ signature-id_str> config filter_list edit <entry_index> set signature_id <signature-id_ str> set match-target {HTTP_METHOD | CLIENT_IP | HOST | URI| FULL_URL | PARAMETER| COOKIE} set operator {STRING_ MATCH | REGEXP_ MATCH | EQ | NE| INCLUDE | EXCLUDE} set http-method {get post head options trace connect delete put others} set ip {<ipv4> | <ipv6>} set name {name_str | name_pattern] set value-check {enable | disable} set value {value_str | value_pattern set concatenate-type {AND | OR}	Changed. To reduce false positives, FortiWeb can now perform additional lexical and syntax analysis after a SQL injection signature matches a request. You can disable this feature for one or both of the SQL injection signature categories, or disable it for individual signatures within the categories. Also, you can now use additional criteria to specify which requests FortiWeb does not scan, including elements such as HTTP methods, client IP, and cookie name. You can create a signature exemption using any of the criteria either individually or in combination.
config waf web-protection-profile inline-protection	

Command	Change
edit <inline-protection-profile_name> set fortigate-quarantined-ips {enable | disable} setquarantined-ip-action {alert | alert_deny} set quarantined-ip-severity {High | Medium | Low} set quarantined-ip-trigger <trigger-policy_name>	New. You can now detect quarantined source IPs using a list that a FortiGate appliance transmits to FortiWeb at regular intervals.
execute erase-disk { flash | disk } [<erase-times>]	New. Erases the hard disk or flash memory. Requires a console connection to the appliance. Available only when Federal Information Processing Standards (FIPS) and Common Criteria (CC) compliant mode is enabled (see config system fips-cc).

FortiWeb 5.4

Command	Change
config log attack-log	
set packet-log {anti-virus-detection | cookie-security | custom-access | custom-protection-rule | fsa-detection | hidden-fields-failed | http-protocol-constraints | illegal-file-type | illegal-xml-format | ip-intelligence | padding-oracle | parameter-rule-failed | signature-detection | illegal-json-format | trojan-detection | illegal-filesize | csrf-detection | user-tracking-detection | account-lockout-detection}	Changed. FortiWeb can preserve packet payloads associated with attack log messages generated by information from FortiSandbox.

Command	Change
`config log syslog-policy`	

`edit <policy_name>`
`config log-server-list`
`edit <entry_index>`
`set csv {enable | disable}`
`set port <port_int>`
`set server <syslog_ipv4>`
	New. Each Syslog policy can now specify connections to up to 3 Syslog servers.

`config router policy`	
`edit <policy_index>` `set priority <priorty_int>`	New. You can now specify a priority value for a policy route. When packets match more than one policy route, FortiWeb directs traffic to the route with the lowest value.
`config server-policy health`	

`edit <health-check_name>`
`configure health-list`
`edit <entry_index>`
`set host <host_str>`
	New. Server health checks now allow you to test the availability of a specific host on the server pool member.

`config server-policy policy`	

`edit <policy_name>`
`config http-content-routing-list`
`edit <entry_index>`
`set profile-inherit {enable | disable}`
	New. When you configure a server policy, instead of assigning web protection profiles to each HTTP content routing policy, you can now configure the routing policies to inherit the profile that the server policy uses.

`config server-policy server-pool`	

`edit <server-pool_name>`
`config pserver-list`
`edit <entry_index>`
`set backup-server {enable | disable}`
	New. You can now specify one or more server pool members to which FortiWeb directs traffic only when all other members are unavailable.

`config system fortisandbox`	New. You can now configure a connection to FortiSandbox that FortiWeb uses to send and receive information about uploaded files.

Command	Change
config system fortisandbox set server <server_ipv4> set ssl {enable | disable} set email <email_str> set interval <interval_int>	
config waf file-upload-restriction-policy	New. You can now configure FortiWeb to submit all files that match your upload restriction rules to FortiSandbox.
config waf site-publish-helper rule	
edit <site-publish-rule_name> [set logoff-path-type {plain | regular}] [set Published-Server-Logoff-Path <url_str>]	New. In a site publish rule, you can now specify the optional value `Published-Server-Logoff-Path` using a regular expression instead of a literal value.

Using the CLI

The command line interface (CLI) is an alternative to the web UI.

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

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

Connecting to the CLI

You can access the CLI in two ways:

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

Local access is required in some cases.

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

Before you can access the CLI through the network, you usually must enable SSH and/or HTTP/HTTPS and/or Telnet on the network interface through which you will access the CLI.

Connecting to the CLI using a local console

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

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 procedure describes connection using PuTTY software; steps may vary with other terminal emulators.

To connect to the CLI using a local console connection

1. Using the null modem or RJ-45-to-DB-9 cable, connect the FortiWeb appliance's console port to the serial communications (COM) port on your management computer.
2. On your management computer, start PuTTY.
3. In the **Category** tree on the left, go to **Connection > Serial** and configure the following:

Serial line to connect to	COM1 (or, if your computer has multiple serial ports, the name of the connected serial port)
Speed (baud)	9600
Data bits	8
Stop bits	1
Parity	None
Flow control	None

4. In the **Category** tree on the left, go to **Session** (**not** the sub-node, **Logging**) and from **Connection type**, select **Serial**.
5. Click **Open**.
6. Press the Enter key to initiate a connection.

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

   The CLI displays the following text, followed by a command line prompt:

   ```
   Welcome!
   ```

   You can now enter CLI commands, including configuring access to the CLI through SSH or Telnet. For details, see Enabling access to the CLI through the network (SSH or Telnet or CLI Console widget) on page 62.

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

SSH, Telnet, or **CLI Console** widget (via the web UI) access to the CLI requires connecting your computer to the FortiWeb appliance using one of its RJ-45 network ports. You can either connect directly, using a peer connection between the two, or through any intermediary network.

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

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

You can do this using either:

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

Requirements

- a computer with an available serial communications (COM) port and RJ-45 port
- terminal emulation software such as PuTTY
- the RJ-45-to-DB-9 or null modem cable included in your FortiWeb package
- a crossover Ethernet cable (if connecting directly) or straight-through Ethernet cable (if connecting through a switch or router)
- prior configuration of the operating mode, network interface, and static route (for details, see the *FortiWeb Administration Guide*.

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

1. Using the network cable, connect the FortiWeb appliance's network port either directly to your computer's network port, or to a network through which your computer can reach the FortiWeb appliance.
2. Note the number of the physical network port.
3. Using a local console connection, connect and log into the CLI. For details, see Connecting to the CLI using a local console on page 61.
4. Enter the following commands:

```
config system interface
   edit <interface_name>
      set allowaccess {http https ping snmp ssh telnet}
end
```

where:

- `<interface_name>` is the name of the network interface associated with the physical network port, such as `port1`
- `{http https ping snmp ssh telnet}` is the complete, space-delimited list of permitted administrative access protocols, such as `https ssh telnet`; omit protocols that you do not want to permit

For example, to exclude HTTP, SNMP, and Telnet, and allow only HTTPS, ICMP ECHO (ping), and SSH administrative access on `port1`:

```
config system interface
   edit "port1"
      set allowaccess ping https ssh
   next
end
```

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

5. To confirm the configuration, enter the command to view the access settings for the interface.

```
show system interface <interface_name>
```

The CLI displays the settings, including the management access settings, for the interface.

6. If you will be connecting indirectly, through one or more routers or firewalls, configure the appliance with at least one static route so that replies from the CLI can reach your client. See `config router static`.

To connect to the CLI through the network interface, see Connecting to the CLI using SSH on page 64 or Connecting to the CLI using Telnet on page 65.

Connecting to the CLI using SSH

Once you configure the FortiWeb appliance to accept SSH connections, you can use an SSH client on your management computer to connect to the CLI.

Secure Shell (SSH) provides both secure authentication and secure communications to the CLI. Supported SSH protocol versions, ciphers, and bit strengths vary by whether or not you have enabled FIPS-CC mode or are using a low encryption (LENC) version, but generally include SSH version 2 with AES-128, 3DES, Blowfish, and SHA-1.

Requirements

- a computer with an RJ-45 Ethernet port
- a crossover Ethernet cable
- a FortiWeb network interface configured to accept SSH connections (see Enabling access to the CLI through the network (SSH or Telnet or CLI Console widget) on page 62)
- an SSH client such as PuTTY

To connect to the CLI using SSH

1. On your management computer, start PuTTY.

Initially, the **Session** category of settings is displayed.

2. In **Host Name (or IP Address)**, type the IP address of a network interface on which you have enabled SSH administrative access.
3. In **Port**, type `22`.
4. From **Connection type**, select **SSH**.
5. Click **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.

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

   The CLI displays a login prompt.

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

   Alternatively, you can log in using an SSH key. For details, see `config system admin`

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

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

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

Connecting to the CLI using Telnet

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

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

Requirements

- a computer with an RJ-45 Ethernet port
- a crossover Ethernet cable
- a FortiWeb network interface configured to accept Telnet connections (see Enabling access to the CLI through the network (SSH or Telnet or CLI Console widget) on page 62)
- terminal emulation software such as PuTTY

To connect to the CLI using Telnet

1. On your management computer, start PuTTY.
2. In **Host Name (or IP Address)**, type the IP address of a network interface on which you have enabled Telnet administrative access.
3. In **Port**, type `23`.
4. From **Connection type**, select **Telnet**.
5. Click **Open**.
6. Type a valid administrator account name (such as `admin`) and press Enter.
7. Type the password for this administrator account and press Enter.

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

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

Command syntax

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

For example, if you do not type the entire object that will receive the action of a command operator such as `config`, the CLI will return an error message such as:

```
Command fail. CLI parsing error
```

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

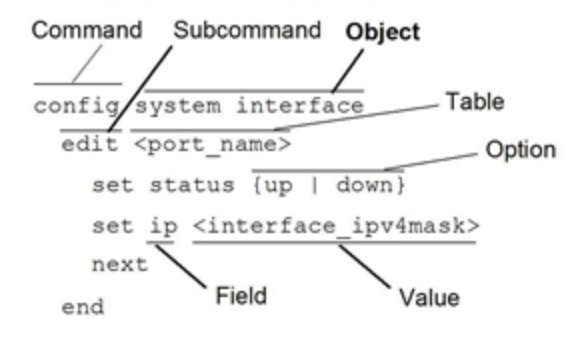
Terminology

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

```
get system admin
```

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

Command syntax terminology



- **command** — A word that begins the command line and indicates an action that the FortiWeb appliance should perform on a part of the configuration or host on the network, such as `config` or `execute`. Together with other words, such as fields or values, that you terminate by pressing the Enter key, it forms a command line. Exceptions include multi-line command lines, which can be entered using an escape sequence. (See Shortcuts & key commands on page 78.)

Valid command lines must be unambiguous if abbreviated. (See Command abbreviation on page 79.) Optional words or other command line permutations are indicated by syntax notation. (See Notation on page 68.)

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

If you do not enter a known command, the CLI will return an error message such as:

```
Unknown action 0
```

- **subcommand** — A kind of command that is available only when nested within the scope of another command. After entering a command, its applicable subcommands are available to you until you exit the scope of the command, or until you descend an additional level into another subcommand. Indentation is used to indicate levels of nested commands. (See Indentation on page 67.)

  Not all top-level commands have subcommands. Available subcommands vary by their containing scope. (See Subcommands on page 71.)
- **object** — A part of the configuration that contains tables and/or fields. Valid command lines must be specific enough to indicate an individual object.
- **table** — A set of fields that is one of possibly multiple similar sets that each have a name or number, such as an administrator account, policy, or network interface. These named or numbered sets are sometimes referenced by other parts of the configuration that use them. (See Notation on page 68.)
- **field** — The name of a setting, such as `ip` or `hostname`. Fields in some tables must be configured with values. Failure to configure a required field will result in an invalid object configuration error message, and the FortiWeb appliance will discard the invalid table.
- **value** — A number, letter, IP address, or other type of input that is usually the configuration setting held by a field. Some commands, however, require multiple input values which may not be named but are simply entered in sequential order in the same command line. Valid input types are indicated by constraint notation. (See Notation on page 68.)
- **option** — A kind of value that must be one or more words from a fixed set of options. (See Notation on page 68.)

Indentation

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

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

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

For information about available subcommands, see Subcommands on page 71.

Notation

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

If you do not use the expected data type, the CLI returns an error message such as:

```
object set operator error, -4003 discard the setting
```

```
The request URL must start with "/" and without domain name.
```

or:

```
invalid unsigned integer value :-:
```

```
value parse error before '-'
```

```
Input value is invalid.
```

and may either **reject** or **discard** your settings instead of saving them when you type `end`.

Command syntax notation

Convention	Description
Square brackets [ ]	A non-required (optional) word or words. For example: `[verbose {1 | 2 | 3}]` indicates that you may either omit or type both the `verbose` word and its accompanying option, such as: verbose 3
Curly braces { }	A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [ ].

Convention	Description
Options delimited by vertical bars |	Mutually exclusive options. For example: `{enable | disable}` indicates that you must enter either `enable` or `disable`, but must not enter both.

Options delimited by spaces	Non-mutually exclusive options. For example:
	`{http https ping snmp ssh telnet}`
	indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as:
	`ping https ssh`
	Note: To change the options, you must re-type the entire list. For example, to add `snmp` to the previous example, you would type:
	`ping https snmp ssh`
	If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.

Convention	Description
Angle brackets < >	A word constrained by data type. To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (_) and suffix that indicates the valid data type. For example: `<retries_int>` indicates that you should enter a number of retries, such as `5`. Data types include: • `<xxx_name>` — A name referring to another part of the configuration, such as `policy_A`. • `<xxx_index>` — An index number referring to another part of the configuration, such as `0` for the first static route. • `<xxx_pattern>` — A regular expression or word with wild cards that matches possible variations, such as `*@example.com` to match all e-mail addresses ending in `@example.com`. • `<xxx_fqdn>` — A fully qualified domain name (FQDN), such as `mail.example.com`. • `<xxx_email>` — An email address, such as `admin@mail.example.com`. • `<xxx_url>` — A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as `http://www.fortinet.com/`. • `<xxx_ipv4>` — An IPv4 address, such as `192.168.1.99`. • `<xxx_v4mask>` — A dotted decimal IPv4 netmask, such as `255.255.255.0`. • `<xxx_ipv4mask>` — A dotted decimal IPv4 address and netmask separated by a space, such as `192.168.1.99 255.255.255.0`. • `<xxx_ipv4/mask>` — A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as such as `192.168.1.99/24`. • `<xxx_ipv6>` — A colon(`:`)-delimited hexadecimal IPv6 address, such as `3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234`. • `<xxx_v6mask>` — An IPv6 netmask, such as `/96`. • `<xxx_ipv6mask>` — An IPv6 address and netmask separated by a space. • `<xxx_str>` — A string of characters that is **not** another data type, such as `P@ssw0rd`. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. See Special characters on page 79. • `<xxx_int>` — An integer number that is **not** another data type, such as `15` for the number of minutes.

Subcommands

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

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

```
get system admin
```

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

```
config system admin
```

the command prompt becomes:

```
(admin)#
```

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

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

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

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

- commands that affect fields (see Field commands on page 73)
- commands that affect tables (see Table commands on page 72)

Subcommand scope is indicated in this CLI Reference by indentation. See Indentation on page 67.

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

Table commands

delete <table_name>	Remove a table from the current object. For example, in `config system admin`, you could delete an administrator account named `newadmin` by typing `delete newadmin` and pressing Enter. This deletes `newadmin` and all its fields, such as `newadmin`'s `first-name` and `email-address`. `delete` is only available within objects containing tables.
edit <table_name>	Create or edit a table in the current object. For example, in `config system admin`: • edit the settings for the default `admin` administrator account by typing `edit admin`. • add a new administrator account with the name `newadmin` and edit `newadmin`'s settings by typing `edit newadmin`. `edit` is an interactive subcommand: further subcommands are available from within `edit`. `edit` changes the prompt to reflect the table you are currently editing. `edit` is only available within objects containing tables.
end	Save the changes to the current object and exit the `config` command. This returns you to the top-level command prompt.
get	List the configuration of the current object or table. • In objects, `get` lists the table names (if present), or fields and their values. • In a table, `get` lists the fields and their values. For more information on `get` commands, see get on page 627.

purge	Remove all tables in the current object. For example, in `config user local-user`, you could type `get` to see the list of all local user names, then type `purge` and then `y` to confirm that you want to delete all users. `purge` is only available for objects containing tables. **Caution:** Back up the FortiWeb appliance before performing a purge because it cannot be undone. To restore purged tables, the configuration must be restored from a backup. For details, see `execute backup cli-config`. **Caution:** Do not purge `system interface` or `system admin` tables. This can result in being unable to connect or log in, requiring the FortiWeb appliance to be formatted and restored.
show	Display changes to the default configuration. Changes are listed in the form of configuration commands. For more information on `show` commands, see show on page 634.

Example of table commands

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

```
edit admin_1
```

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

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

Field commands

abort	Exit both the `edit` and/or `config` commands without saving the fields.
end	Save the changes made to the current table or object fields, and exit the `config` command. (To exit without saving, use `abort` instead.)
get	List the configuration of the current object or table. • In objects, `get` lists the table names (if present), or fields and their values. • In a table, `get` lists the fields and their values.

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

Example of field commands

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

```
set password my1stExamplePassword
```

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

Permissions

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

Access profiles control which commands and areas an administrator account can access. 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. For more information on configuring the access profile for an administrator account to use, see `config system accprofile`.

Areas of control in access profiles

Access profile setting	Grants access to*	
Admin Users	**System > Admin** ... **except Settings**	Web UI
`admingrp`	`config system admin` `config system accprofile`	CLI
Auth Users	**User** ...	Web UI
`authusergrp`	`config user ...`	CLI
Autolearn Configuration	**Auto Learn > Auto Learn Profile > Auto Learn Profile**	Web UI

`learngrp`	`config server-policy custom-application ...`
	`config waf web-protection-profile`
	`autolearning-profile`
	Note: Because generating an auto-learning profile also generates its required components, this area also confers **Write** permission to those components in the **Web Protection Configuration**/`wafgrp` area.
		CLI

Log & Report	**Log&Report** ...	Web UI
`loggrp`	`config log ...` `execute formatlogdisk`	CLI
Maintenance	**System > Maintenance except System Time** tab	Web UI

`mntgrp`	`diagnose system ...`
	`execute backup ...`
	`execute factoryreset`
	`execute reboot`
	`execute restore ...`
	`execute shutdown`
	`diagnose system flash ...`
		CLI

Network Configuration	**System > Network** ...	Web UI

Access profile setting	Grants access to*	

`netgrp`	`config router ...`
	`config system interface`
	`config system dns`
	`config system v-zone`
	`diagnose network ...` **`except`** `sniffer ...`
		CLI

System Configuration	**System** ... **except Network**, **Admin**, and **Maintenance** tabs	Web UI

`sysgrp`	`config system` **except** `accprofile`, `admin`, `dns`, `interface`, and `v-zone`
	`diagnose hardware ...`
	`diagnose network sniffer ...`
	`diagnose system ...` **`except`** `flash ...`
	`execute date ...`
	`execute ha ...`
	`execute ping ...`
	`execute ping-option ...`
	`execute traceroute ...`
	`execute time ...`
		CLI

Server Policy Configuration	**Policy** > **Server Policy** ... **Server Objects** ... **Application Delivery** ...	Web UI

`traroutegrp`	`config server-policy ...` **`except`** `custom-application ...`
	`config waf file-compress-rule`
	`config waf file-uncompress-rule`
	`config waf http-authen ...`
	`config waf url-rewrite ...`
	`diagnose policy ...`
		CLI

Web Anti-Defacement Management	**Web Anti-Defacement** ...	Web UI
`wadgrp`	`config wad ...`	CLI
Web Protection Configuration	**Policy** > **Web Protection** ... **Web Protection** ... **DoS Protection** ...	Web UI

Access profile setting	Grants access to*	
wafgrp	`config system dos-prevention` `config waf` **except**: • `config waf file-compress-rule` • `config waf file-uncompress-rule` • `config waf http-authen ...` • `config waf url-rewrite ...` • `config waf web-custom-robot` • `config waf web-protection-profile autolearning-profile` • `config waf web-robot` • `config waf x-forwarded-for`	CLI
Web Vulnerability Scan Configuration	**Web Vulnerability Scan** ...	Web UI
wvsgrp	`config wvs ...`	CLI
***** For each `config` command, there is an equivalent `get/show` command, unless otherwise noted. `config` access requires write permission. `get/show` access requires read permission.		

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

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, you must log in with the administrator account named `admin`.

Tips & tricks

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

This section includes:

- Help
- Shortcuts & key commands
- Command abbreviation
- Special characters
- Language support & regular expressions
- Screen paging
- Baud rate
- Editing the configuration file in a text editor

Help

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

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

Shortcuts & key commands

Action	Keys
List valid word completions or subsequent words. If multiple words could complete your entry, display all possible completions with helpful descriptions of each.	?
Complete the word with the next available match. Press the key multiple times to cycle through available matches.	Tab
Recall the previous command. Command memory is limited to the current session.	Up arrow, or Ctrl + P
Recall the next command.	Down arrow, or Ctrl + N
Move the cursor left or right within the command line.	Left or Right arrow
Move the cursor to the beginning of the command line.	Ctrl + A
Move the cursor to the end of the command line.	Ctrl + E
Move the cursor backwards one word.	Ctrl + B

Action	Keys
Move the cursor forwards one word.	Ctrl + F
Delete the current character.	Ctrl + D
Abort current interactive commands, such as when entering multiple lines. If you are not currently within an interactive command such as `config` or `edit`, this closes the CLI connection.	Ctrl + C
Continue typing a command on the next line for a multi-line command. For each line that you want to continue, terminate it with a backslash (\ ). To complete the command line, terminate it by pressing the spacebar and then the Enter key, without an immediately preceding backslash.	\ then Enter

Command abbreviation

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

```
g sy st
```

If you enter an ambiguous command, the CLI returns an error message such as:

```
ambiguous command before 's'
Value conflicts with system settings.
```

Special characters

Special characters <, >, (,), #, ', and " are usually not permitted in CLI. If you use them, the CLI will often return an error message such as:

```
The string contains XSS vulnerability characters

value parse error before '%^@'
Input not as expected.
```

Some may be enclosed in quotes or preceded with a backslash (\ ) character.

Entering special characters

Character	Key
?	Ctrl + V then ?
Tab	Ctrl + V then Tab

Character	Key
Space (to be interpreted as part of a string value, not to end the string)	Enclose the string in quotation marks: “`Security Administrator`”. Enclose the string in single quotes: `'Security Administrator'`. Precede the space with a backslash: `Security\ Administrator`.
' (to be interpreted as part of a string value, not to end the string)	\'
" (to be interpreted as part of a string value, not to end the string)	\"
\	\\

Language support & regular expressions

Languages currently supported by the CLI interface include:

- English
- Japanese
- simplified Chinese
- traditional Chinese

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

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

To use other languages in those cases, you must use the correct encoding.

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

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

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

For best results, you should:

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

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

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

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

Similarly to input, your web browser or CLI client should usually interpret display output as encoded using UTF-8. If it does not, your configured items may not display correctly in the web 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.

To enter non-ASCII characters in the CLI Console widget

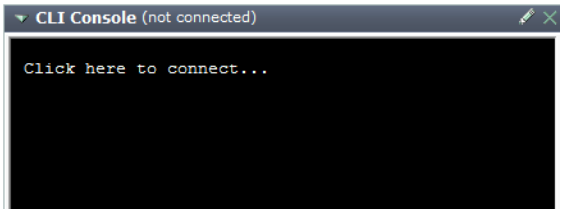
1. On your management computer, start your web browser and go to the URL for the FortiWeb appliance's web UI.
2. Configure your web browser to interpret the page as UTF-8 encoded.
3. Log in to the FortiWeb appliance.
4. Go to **System > Status > Status**.
5. In title bar of the **CLI Console** widget,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

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

The **Command** field appears below the usual input and display area of the **CLI Console** widget.

8. In **Command**, type a command.

CLI Console widget



9. Press Enter.

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

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

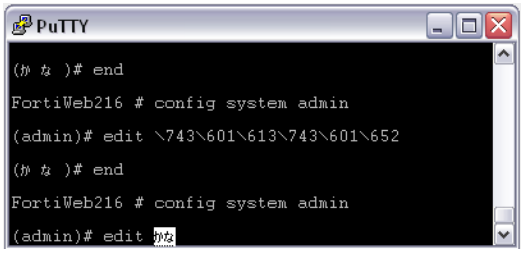
   and the command's output.

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

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

   Support for sending and receiving international characters varies by each Telnet or SSH client. Consult the documentation for your Telnet or SSH client.
3. Log in to the FortiWeb appliance.
4. At the command prompt, type your command and press Enter.

Entering encoded characters (PuTTY)



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

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

For example, you might need to enter:

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

5. The CLI displays your previous command and its output.

Screen paging

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

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

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

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

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

For more information, see `config system console`.

Baud rate

You can change the default baud rate of the local console connection. For more information, see `config system console`.

Editing the configuration file in a text editor

Editing the configuration file with a plain text editor can be time-saving if:

- you have many changes to make,
- are not sure where the setting is in the CLI, and/or
- own several FortiWeb appliances

This is true especially if your plain text editor provides advanced features such as regular expressions for find-and-replace, or batch changes across multiple files. Several free text editors are available with these features, such as Text Wrangler and Notepad++.

Do **not** use a rich text editor such as Microsoft Word. Rich text editors insert special characters into the file in order to apply formatting, which may corrupt the configuration file.

To edit the configuration on your computer

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

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

3. Use `execute restore config` to upload the modified configuration file back to the FortiWeb appliance.

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

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.

Differences between administrator accounts when ADOMs are enabled

	`admin` administrator account	Other administrators
Access to `config global`	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 `execute backup full-config`.

2. Enter the following commands:

```
config system global
   set adom-admin enable
end
```

   FortiWeb terminates your administrative session.

3. Log in again.

   When ADOMs are enabled, and if you log in as `admin`, the top level of the shell changes: the two top level items are `config global` and `config vdom`.

   - `config global` contains settings that only `admin` or other accounts with the **prof_admin** access profile can change.
   - `config vdom` 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 on page 86).

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 `execute backup full-config`.

2. Enter the following commands:

```
config system global
   set adom-admin disable
end
```

   FortiWeb terminates your administrative session.

3. Continue by reconfiguring the appliance (see the *FortiWeb Administration Guide*).

See also

- Permissions
- Defining ADOMs
- Assigning administrators to an ADOM
- `config system admin`
- `config system accprofile`

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
- X.509 certificates
- 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. Enter the following commands:

```
config vdom
  edit <adom_name>
```

where <adom_name> is the name of your new ADOM. (Alternatively, to configure the default root ADOM, type root.)

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 the *FortiWeb Administration Guide*.

The new ADOM exists, but its settings are not yet configured.

3. Either:

- assign another administrator account to configure the ADOM (continue with Assigning administrators to an ADOM on page 87), or
- configure the ADOM yourself by entering commands such as:

```
config log...
config server-policy...
config system...
config waf...
```

See also

- Assigning administrators to an ADOM
- Administrative domains (ADOMs)
- Permissions
- config system admin
- config system accprofile

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 config system accprofile.
2. In the administrator account's accprofile <access-profile_name> 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 domains <adom_name> setting, select the account's assigned ADOM. Currently, in this version of FortiWeb, administrators cannot be assigned to more than one ADOM.

See also

- Permissions
- `config system admin`
- `config system accprofile`
- Defining ADOMs

config

The `config` commands configure your FortiWeb appliance's feature settings.

This chapter describes the following commands:

log alertemail
log attack-log
log custom-sensitive-rule
log disk
log email-policy
log event-log
log forti-analyzer
log fortianalyzer-policy
log ftp-policy
log reports
log sensitive
log siem-message-policy
log siem-policy
log syslogd
log syslog-policy
log traffic-log
log trigger-policy
router policy
router setting
router static
server-policy allow-hosts
server-policy custom-application application-policy
server-policy custom-application url-replacer
server-policy http-content-routing-policy
server-policy http-content-routing-policy
server-policy pattern custom-data-type
server-policy pattern custom-global-white-list-group
server-policy pattern custom-susp-url
server-policy pattern custom-susp-url-rule
server-policy pattern data-type-group
server-policy pattern suspicious-url-rule
server-policy persistence-policy
server-policy policy
server-policy server-pool
server-policy service custom
server-policy vserver
system accprofile
system admin
system advanced
system antivirus
system autoupdate override
system autoupdate schedule
system autoupdate tunneling
system backup
system certificate ca
system certificate ca-group
system certificate crl
system certificate intermediate-certificate
system certificate intermediate-certificate-group
system certificate local
system certificate sni
system certificate urlcert
system certificate verify
system conf-sync
system console
system dns
system eventhub
system fail-open
system fips-cc
system firewall address
system firewall firewall-policy
system firewall service
system fortigate-integration
system fortisandbox

system global
system ha
system hsm info
system hsm partition
system interface
system ip-detection
system network-option
system raid
system replacemsg
system replacemsg-image
system settings
system snmp community
system snmp sysinfo
system snmp user
system v-zone
system wccp
user admin-usergrp
user kerberos-user
user ldap-user
user local-user
user ntlm-user
user radius-user
user user-group
wad file-filter
wad website
waf allow-method-exceptions
waf allow-method-policy
waf application-layer-dos-prevention
waf base-signature-disable
waf brute-force-login
waf cookie-security
waf csrf-protection
waf custom-access policy
waf custom-access rule
waf custom-protection-group
waf custom-protection-rule
waf exclude-url
waf file-compress-rule
waf file-upload-restriction-policy
waf file-upload-restriction-rule
waf geo-block-list
waf geo-ip-except
waf hidden-fields-protection
waf hidden-fields-rule
waf http-authen http-authen-policy
waf http-authen http-authen-rule
waf http-connection-flood-check-rule
waf http-constraints-exceptions
waf http-protocol-parameter-restriction
waf http-request-flood-prevention-rule
waf input-rule
waf ip-intelligence
waf ip-intelligence-exception
waf ip-list
waf layer4-access-limit-rule
waf layer4-connection-flood-check-rule
waf padding-oracle
waf page-access-rule
waf parameter-validation-rule
waf signature
waf site-publish-helper authentication-server-pool
waf site-publish-helper keytab_file
waf site-publish-helper policy
waf site-publish-helper rule
waf start-pages
waf url-access url-access-policy
waf url-access url-access-rule
waf url-rewrite url-rewrite-policy
waf url-rewrite url-rewrite-rule
waf user-tracking policy
waf user-tracking rule
waf web-cache-exception
waf web-cache-policy
waf web-protection-profile autolearning-profile
waf web-protection-profile inline-protection
waf web-protection-profile offline-protection
waf x-forwarded-for
wvs policy
wvs profile
wvs schedule

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

log alertemail

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

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see Permissions on page 74.

Syntax

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

Variable	Description	Default
`status {enable | disable}`	Enable to generate an alert email when the FortiWeb appliance records a log message, if that log message meets or exceeds the severity level configured in `config log email-policy`.	`enable`
`email-policy <policy_name>`	Type the name of a previously configured email policy. The maximum length is 35 characters. To display a list of the existing email policies, type: `set email-policy ?`	No default.

Example

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

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

Related topics

- log email-policy

log attack-log

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

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

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

Packet payloads can be retained for specific attack types or validation failures detected by the FortiWeb appliance. Packet payloads supplement the log message by providing the actual data that triggered the attack log, which may help you to fine-tune your regular expressions to prevent false positives. You can also examine changes to attack behavior for subsequent forensic analysis. (Alternatively, for more extensive packet logging, you can run a packet trace. See `diagnose network sniffer`.)

If the offending HTTP request exceeds 4 kilobytes (KB), the FortiWeb appliance retains only 4 KB' of the part of the payload that triggered the log message.

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

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see Permissions on page 74.

Syntax

```
config log attack-log
   set status {enable | disable}
   set http-parse-error-output {enable | disable}
   set packet-log {anti-virus-detection | cookie-security | custom-access |
       custom-protection-rule  | fsa-detection | hidden-fields-failed | http-
       protocol-constraints | illegal-file-type | illegal-xml-format | ip-
       intelligence | padding-oracle | parameter-rule-failed | signature-
       detection | illegal-json-format | trojan-detection | illegal-filesize |
       csrf-detection | user-tracking-detection | account-lockout-detection}
   set no-ssl-error {enable | disable}
   set show-all-log {enable | disable}
end
```

Variable	Description	Default
`status {enable | disable}`	Enable to record attack log messages on the disk. To record attack logs, disk log storage must be enabled, and the severity levels selected using the `config log disk` command.	`enable`
`http-parse-error-output {enable | disable}`	Enable while debugging only, to log errors of the HTTP protocol parser.	`disable`
`packet-log {anti-virus-detection | cookie-security | custom-access | custom-protection-rule | fsa-detection | hidden-fields-failed | http-protocol-constraints | illegal-file-type | illegal-xml-format | ip-intelligence | padding-oracle | parameter-rule-failed | signature-detection | illegal-json-format | trojan-detection | illegal-filesize | csrf-detection | user-tracking-detection | account-lockout-detection}`	Select one or more detected attack types or validation failures. FortiWeb keeps packet payloads from its HTTP parser buffer with their associated attack log message. Separate each attack type with a space. To add or remove a packet payload type, re-type the entire space-delimited list with the new option included or omitted. Some options have historical names. Correlations with current feature names are: • `custom-protection-rule` — Custom signature detection (not predefined) To empty this list and keep no packet payloads, effectively disabling the feature, type `unset packet-log`.	No default.
`no-ssl-error {enable | disable}`	Enable to stop FortiWeb from logging SSL errors. This setting is useful when you use high-level security settings, which generate a high volume of these types of errors.	`disable`
`show-all-log {enable | disable}`	Specifies whether all signature violations that contributed to a threat scoring attack log message are displayed as individual entries in the attack log. In addition, messages for signature violations that generated a threat score but did not exceed the threat scoring threshold are displayed. If the value of this setting is `disable` (the default), a single attack log message is displayed for the signature violations that contributed to a combined threat score that exceeded the maximum. However, all the signature violations that contributed to the score are displayed in the message details. (Double-click the message to display its details.)	`disable`

Example

This example enables log storage on the hard disk and sets `information` as the minimum severity level that a log message must meet in order for the log to be stored. It also enables retention of packet payloads that triggered custom protection rules along with their correlating attack logs. (Conversely, it disables any other packet payload retention that may have been enabled before, because it completely replaces the list each time it is configured.)

```
config log disk
   set status enable
   set severity information
end
config log attack-log
   set status enable
   set packet-log custom-protection-rule
end
```

Related topics

- `config log sensitive`
- `config log custom-sensitive-rule`
- `config log event-log`
- `config log traffic-log`
- `diagnose debug application miglogd`
- `diagnose log`

log custom-sensitive-rule

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

Use this command in conjunction with `config log sensitive`.

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

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

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see Permissions on page 74.

Syntax

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

Variable	Description	Default
`<custom-sensitive-rule_name>`	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: `edit ?`	No default.
`expression "<sensitive-type_pattern>"`	Type a regular expression that matches all and only the strings or numbers that you want to obscure in the packet payloads. For example, to hide a parameter that contains the age of users under 13, you could enter: `age\=[1-13]` Expressions must not start with an asterisk (`*`). The maximum length is 255 characters.	No default.
`type {field-mask-rule | general-mask-rule}`	Select either `general-mask-rule` (a regular expression that will match any substring in the packet payload) or `field-mask-rule` (a regular expression that will match only the value of a specific form input). If you select `general-mask-rule`, configure expression "<sensitive-type_pattern>". If you select `field-mask-rule`, configure field-name "<parameter-name_pattern>" and field-value "<parameter-value_pattern>".	`general-mask-rule`
`field-name "<parameter-name_pattern>"`	Type a regular expression that matches all and only the input names whose values you want to obscure. (The input name itself will **not** be obscured. If you wish to do this, use `general-mask-rule` instead.) The maximum length is 255 characters.	No default.

Variable	Description	Default

`field-value "<parameter-value_pattern>"`	Type a regular expression that matches all and only the input values that you want to obscure. The maximum length is 255 characters.
	
	For example, to hide a parameter that contains the age of users under 13, for field-name "<parameter-name_pattern>", enter `age`, and for field-value "<parameter-value_pattern>", enter `[1-13].`
	
	Valid expressions must not start with an asterisk (`*`).
	
	Caution: Field masks using asterisks are greedy: a match for the parameter's value will obscure it, but will **also** obscure the rest of the parameters in the line. To avoid this, enter an expression whose match terminates with, but does not consume, the parameter separator.
	
	For example, if parameters are separated with an ampersand (&), and you want to obscure the value of the field name `username` but **not** any of the parameters that follow it, you could enter the field value:
	
	`.*?(?=\&)`
	
	This would result in:
	
	`username****&age=13&origurl=%2Flogin`
		No default.

Example

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

```
config log attack-log
   set status enable
   set packet-log anti-virus-detection cookie-poison custom-access custom-protection-rule
       hidden-fields-failed http-protocol-constraints illegal-file-type illegal-xml-format
       ip-intelligence padding-oracle parameter-rule-failed signature-detection
end
config log sensitive
   set type custom-rule
end
config log custom-sensitive-rule
   edit rule1
      set type general-mask-rule
      set expression "age\\=[1-13]*$"
   next
end
```

Related topics

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

log disk

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

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

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

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

Syntax

```
config log disk
   set diskfull {nolog | overwrite}
   set severity {alert | critical | debug | emergency | error | information |
       notification | warning}
   set status {enable | disable}
end
```

Variable	Description	Default
status {enable | disable}	Enable to store log messages on the local hard disk. Log messages are stored only if logging is enabled for the individual log types using the config log attack-log, config log event-log, and config log traffic-log commands. Also configure severity, diskfull and max-log-file-size.	enable

Variable	Description	Default
`diskfull {nolog | overwrite}`	Type what the FortiWeb does when the local disk is full and a new log message is caused, either: • `nolog` — Discard the new log message. • `overwrite` — Delete the oldest log file in order to free disk space, then store the new log message. This field is available only if `status` is `enable`.	`overwrite`
`severity {alert | critical | debug | emergency | error | information | notification | warning}`	Select the severity level that a log message must meet or exceed in order to cause the FortiWeb appliance to record it.	`information`

Example

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

```
config log event-log
   set status enable
end
config log attack-log
   set status enable
end
config log disk
   set status enable
   set severity notification
   set diskfull overwrite
end
```

Related topics

- `config log attack-log`
- `config log event-log`
- `config log traffic-log`
- `config system snmp community`
- `config log reports`
- `execute formatlogdisk`

log email-policy

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

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see Permissions on page 74.

Syntax

```
config log email-policy
   edit <email-policy_name>
      set mailfrom <address_str>
      set mailto1 <recipient_email>
      set mailto2 <recipient_email>
      set mailto3 <recipient_email>
      set smtp-server {<smtp_ipv4> | <smtpfqdn>}
      set smtp-port <smtp-port_int>
      set smtp-auth {enable | disable}
      set smtp-username <auth_str>
      set smtp-password <password_str>
      set severity {alert | critical | debug | emergency | error | information |
          notification | warning}
      set interval <interval_int>
      set connection-security {NONE | STARTTLS | SSL/TLS}
      set attach-compression {enable | disable}
   next
end
```

Variable	Description	Default
`<email-policy_name>`	Type the name of an email policy. The maximum length is 35 characters.	No default.
`mailfrom <address_str>`	Type the sender email address, such as `FortiWeb@example.com`, that the FortiWeb appliance will use when sending email. The maximum length is 63 characters.	No default.
`mailto1 <recipient_email>`	Type the email address of the first recipient, such as `admin@example.com`, to which the FortiWeb appliance will send email. You must enter one email address for alert email to function. The maximum length is 63 characters.	No default.

Variable	Description	Default
`mailto2 <recipient_email>`	Type the email address of the second recipient, if any, to which the FortiWeb appliance will send alert email. The maximum length is 63 characters.	No default.
`mailto3 <recipient_email>`	Type the email address of the third recipient, if any, to which the FortiWeb appliance will send alert email. The maximum length is 63 characters.	No default.
`smtp-server {<smtp_ipv4> | <smtpfqdn>}`	Type the IP address or fully qualified domain name (FQDN) of the SMTP server, such as `mail.example.com`, that the FortiWeb appliance can use to send email. The maximum length is 63 characters.	No default.
`smtp-port <smtp-port_int>`	Enter the port on the SMTP server that listens for alerts and generated reports from FortiWeb. Valid values are from 1 to 65535.	25
`smtp-auth {enable | disable}`	Enable if the SMTP server requires authentication. Also enable if authentication is not required but is available and you want the FortiWeb appliance to authenticate.	`disable`
`smtp-username <auth_str>`	If you enable smtp-auth {enable | disable}, type the user name that the FortiWeb appliance will use to authenticate itself with the SMTP relay. The maximum length is 63 characters. This field is available only if you enable smtp-auth {enable | disable}.	No default.
`smtp-password <password_str>`	If you enable smtp-auth {enable | disable}, type the password that corresponds with the user name. This field is available only if you enable smtp-auth {enable | disable}.	No default.
`severity {alert | critical | debug | emergency | error | information | notification | warning}`	Select the severity threshold that log messages must meet or exceed in order to cause an email alert.	`emergency`
`interval <interval_int>`	Enter the number of minutes FortiWeb waits to send an additional alert if an alert condition of the specified severity level continues to occur after the initial alert. Valid values are from 1 to 2147483647.	1

Variable	Description	Default
`connection-security {NONE | STARTTLS | SSL/TLS}`	Select one of the following options: • `NONE` — FortiWeb applies no security protocol to email. • `STARTTLS` — Encrypts the connection to the SMTP server using STARTTLS. • `SSL/TLS` — Encrypts the connection to the SMTP server using SSL/TLS.	NONE
attach-compression {enable | disable}	Enable or disable the compression for an alert email policy. With the compression function being enabled, event logs and alerts will be attached to the emails in ZIP format, otherwise they will be attached in TXT format.	`disable`

Example

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

FortiWeb logs messages more severe than a notification. As long as events continue to trigger notification-level log messages, FortiWeb sends an alert email every 10 minutes. (Log messages of other severity levels trigger alert email at their default intervals.) All the related log messages will be attached to the emails in ZIP format.

When the configuration is complete, log in to the web UI to send a sample alert email to test the configuration and the email system.

```
config log email-policy
   edit Email_Policy1
      set mailfrom fortiweb@example.com
      set mailto1 admin@example.com
      set mailto2 analysis@example.com
      set smtp-server mail.example.com
      set smtp-auth enable
      set smtp-username fortiweb
      set smtp-password fortiWebPasswordD2
      set severity notification
      set interval 10
      set attach-compression enable
   next
end
```

Related topics

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

log event-log

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

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

Syntax

```
config log event-log
   set status {enable | disable}
   set analyzer-policy <fortianalyzer-policy_name>
   set cpu-high <percentage_int>
   set mem-high <percentage_int>
   set logdisk-high <percentage_int>
   set trigger-policy <trigger-policy_name>
end
```

Variable	Description	Default
`status {enable | disable}`	Enable to record event log messages. To select the destination and the severity threshold of the stored log messages, used either the `config log disk` or the command.	`enable`
`threshold {50 | 60 | 70 | 80 | 90}`	Select a threshold level as a percentage that will trigger an event log when the actual number of persistent server sessions reaches the defined percentage of the total number of persistent server sessions allowed for the FortiWeb appliance.	`50`
`cpu-high <percentage_int>`	Type a threshold level as a percentage beyond which CPU usage triggers an event log entry. The valid range is from 60 to 99 percent.	`60`
`mem-high <percentage_int>`	Type a threshold level as a percentage beyond which memory usage triggers an event log entry. The valid range is from 60 to 99 percent.	`60`
`logdisk-high <percentage_int>`	Type a threshold level as a percentage beyond which log disk usage triggers an event log entry. The valid range is from 60 to 99 percent.	`60`

Variable	Description	Default
`trigger-policy <trigger-policy_name>`	Type the name of the trigger to apply when the CPU, memory, log disk usage, or number of sessions meets or exceeds the threshold (see `config log trigger-policy`). The maximum length is 35 characters. To display the list of existing trigger policies, type: `set trigger ?`	No default.

Example

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

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

Related topics

- `config log disk`
-
- `config log attack-log`
- `config log traffic-log`
- `diagnose debug application miglogd`
- `diagnose log`

log forti-analyzer

Use this command to configure the FortiWeb appliance to send its log messages to a remote FortiAnalyzer appliance.

You must first define one or more FortiAnalyzer policies using `config log fortianalyzer-policy`.

Logs sent to FortiAnalyzer are controlled by FortiAnalyzer policies and trigger actions that you configure on the FortiWeb appliance, and are associated with various types of violations.

Usually, you should set trigger actions for specific types of violations. Failure to do so will result in the FortiWeb appliance logging every occurrence, which could result in high log volume and reduced system performance. Excessive logging for an extended period of time may cause premature hard disk failure.

Logs stored remotely cannot be viewed from the web UI, and cannot be used by FortiWeb to build reports. If you require these features, record logs locally as well as remotely.

Syntax

```
config log forti-analyzer
   set analyzer-policy <fortianalyzer-policy_name>
   set analyzer-policy <fortianalyzer-policy_name>
   set analyzer-policy <fortianalyzer-policy_name>
end
```

Variable	Description	Default
`fortianalyzer-policy <policy_name>`	Type the name of an existing FortiAnalyzer policy to use when storing log information remotely. The maximum length is 35 characters. To view a list of the existing FortiAnalyzer policies, type: `set fortianalyzer-policy ?`	No default.
`status {enable | disable}`	Enable to record event log messages to FortiAnalyzer if it meets or exceeds the severity level configured in `severity`.	`disable`
`severity {alert | critical | debug | emergency | error | information | notification | warning}`	Select the severity level that a log message must meet or exceed in order to cause the FortiWeb appliance to save it to FortiAnalyzer.	`information`

Example

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

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

Related topics

- config log fortianalyzer-policy

log fortianalyzer-policy

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

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see Permissions on page 74.

Syntax

```
config log fortianalyzer-policy
   edit <policy_name>
      config fortianalyzer-server-list
         edit <entry_index>
            set ip-address <forti-analyzer_ipv4>
            set enc-algorithm {disable | default}
         end
      next
end
```

Variable	Description	Default
`<policy_name>`	Type the name of the new or existing FortiAnalyzer policy. The maximum length is 35 characters. To display a list of the existing policies, type: `edit ?`	No default.
`<entry_index>`	Enter the index number of the individual entry in the table.	No default.
`ip-address <forti-analyzer_ipv4>`	Type the IP address of the remote FortiAnalyzer appliance.	No default.
`enc-algorithm {disable | default}`	Specifies whether FortiWeb transmits logs to the FortiAnalyzer appliance using SSL.	`disable`

Example

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

```
config log fortianalyzer-policy
   edit fa-policy1
      config fortianalyzer-policy
         edit 1
            set ip-address 192.0.2.0
         end
      next
end
config log forti-analyzer
   set fortianalyzer-policy fa-policy1
   set status enable
   set severity error
end
```

Related topics

- `config log forti-analyzer`

log ftp-policy

Use this command to configure a connection to an FTP or TFTP server. The `config log reports` configuration uses this policy to specify a server that FortiWeb sends reports to.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see Permissions on page 74.

Syntax

```
config log ftp-policy
   edit <policy_name>
      set type {ftp | tftp}
      set server <ftp-server_ipv4>
      set ftp_auth {enable | disable}
      set ftp_user <ftp-user_str>
      set ftp_passwd <ftp_pswd>
      set ftp-dir <ftp-dir_str>
end
```

Variable	Description	Default
<policy_name>	Type the name of a new or existing FTP/TFTP policy. The maximum length is 35 characters. To display the list of existing policies, type: edit ?	No default.
type {ftp | tftp}	Specify whether the server is FTP or TFTP.	ftp
server <ftp-server_ipv4>	The IP address of the FTP or TFTP server.	No default.
ftp_auth {enable | disable}	Specify whether the server requires a user name and password for authentication, rather than allowing anonymous connections. Available only if type is ftp.	disable
ftp_user <ftp-user_str>	Enter the user name that FortiWeb uses to authenticate with the server. Available only if ftp_auth is enable.	No default.
ftp_passwd <ftp_pswd>	Enter the password for the specified username. Available only if ftp_auth is enable	No default.
ftp-dir <ftp-dir_str>	Enter the location on the server where FortiWeb stores reports.	No default.

Related topics

- config log reports

log reports

Use this command to configure report profiles.

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

In addition to log files, your FortiWeb appliance requires a report profile to generate a report. A report profile is a group of settings that contains the report name, file format, subject matter, and other aspects that the FortiWeb 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 in the web UI when you click the **Run now** icon in the report profile list. You may want to create one report profile for each type of report that you will generate on demand or periodically, by schedule.

Generating reports can be resource intensive. To avoid email processing performance impacts, you may want to generate reports during times with low traffic volume, such as at night.

The number of results in a section's table or graph varies by the report type.

Ranked reports (top **x**, or top **y** of top **x**) can include a different number of results per cross-section, then combine remaining results under "Others." For example, in "Top Attack Severity by Hour of Day," the report includes the top **x** hours, and their top **y** attacks, then groups the remaining results.

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

Before you generate a report, collect log data that will be the basis of the report. For information on enabling logging to the local hard disk, see `config log attack-log` and `config log disk`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see Permissions on page 74.

Creating a report profile is considerably easier in the web UI. Go to **Log&Report > Report Config**.

Syntax

```
config log reports
   edit <report_name>
      set custom_company "<org_str>"
      set custom_footer_options {custom | report-title}
      set analyzer-policy <fortianalyzer-policy_name>
      set custom_header <header_str>
      set custom_header_logo <filename_hex>
      set custom_title_logo <filename_hex>
      set email_attachment_compress {enable | disable}
      set email_attachment_name "<filename_str>"
      set email_body "<message_str>"
      set email_subject "<subject_str>"
      set filter_string "<log-filter_str>"
      set include_nodata {yes | no}
      set on_demand {enable | disable}
      set output_email {html mht pdf rtf txt}
      set output_email_policy <policy_name>
      set output_file {html mht pdf rtf txt}
      set output_ftp {html pdf rtf txt mht}
      set output_ftp_policy <ftp-policy_name>
      set period_end <time_str> <date_str>
      set period_last_n <n_int>
      set period_start <time_str> <date_str>
      set period_type {last-14-days | last-2-weeks | last-30-days | last-7-
          days | lastmonth | last-n-days | last-n-hours | last-n-weeks |
          last-quarter | last-week | other | this-month | this-quarter |
          this-week | this-year | today | yesterday}
      set report_desc "<comment_str>"
      set report_title <title_str>
```

```
        set Report_attack_activity {attacks-type attacks-url attacks-date-type
            attacks-month-type attacks-day-type attacks-hour-type attacks-type-dev
            attacks-dst-type attacks-dst-ip attacks-type-ip attacks-method-type
            attacks-cat attacks-policy attacks-day attacks-ts attacks-td
            attacks-proto attacks-date-severity attacks-month-severity
            attacks-day-severity attacks-hour-severity attacks-sessionid attacks-
            signature-id attacks-srccounty attacks-type-signature-id attacks-
            fortisandbox attacks-httphost attacks-username}
        set Report_event_activity {ev-all ev-all-cat ev-all-type ev-crit-hour
            ev-crit-day ev-warn-hour ev-warn-day ev-info-hour ev-info-day
            ev-emer-hour ev-emer-day ev-aler-hour ev-aler-day ev-err-hour
            ev-err-day ev-noti-hour ev-noti-day ev-hour ev-hour-cat ev-day
            ev-day-cat ev-stat}
        set Report_traffic_activity {net-pol net-srv net-src net-dst net-src-dst
            net-dst-src net-date-dst net-hour-dst net-day-dst net-month-dst
            net-date-src net-hour-src net-day-src net-month-src net-srccountry
            net-httphost net-username}
        set analyzer-policy <fortianalyzer-policy_name>
        set schedule_type {daily | dates | days | none}
        set schedule_days {sun | mon | tue | wed | thu | fri | sat}
        set schedule_dates <dates_str>
        set schedule_time <time_str>
        set scope_include_summary {yes | no}
        set scope_include_table_of_content {yes | no}
        set scope_top1 <topX_int>
        set scope_top2 <topY_int>
    next
end
```

Variable	Description	Default
<report_name>	Type the name of a new or existing report profile. The maximum length is 63 characters. The profile name will be included in the report header. To display the list of existing report names, type: edit ?	No default.
custom_company "<org_str>"	Type the name of your department, company, or other organization, if any, that you want to include in the report summary. If the text is more than one word or contains special characters, enclose it in double quotes ("). The maximum length is 191 characters. For information on enabling the summary, see scope_include_summary {yes | no}.	No default.

Variable	Description	Default
`custom_footer_options {custom | report-title}`	Select either: • `report-title` — Use <report_name> as the footer text. • `custom` — Provide separate footer text in analyzer-policy <fortianalyzer-policy_name>.	`report-title`
`custom_footer "<footer_str>"`	Type the text, if any, that you want to include at the bottom of each report page. If the text is more than one word or contains special characters, enclose it in double quotes ("). The maximum length is 127 characters. This setting is available only if `custom_footer_options` is `custom`.	No default.
`custom_header <header_str>`	Type the text, if any, that you want to include at the top of each report page. If the text is more than one word or contains special characters, enclose it in double quotes ("). The maximum length is 127 characters.	No default.
`custom_header_logo <filename_hex>`	Type the file name of a custom logo that you have previously uploaded to the FortiWeb appliance. The logo image will be included in the report header. The maximum length is 255 characters.	No default.
`custom_title_logo <filename_hex>`	Type the file name of a custom logo that you have previously uploaded to the FortiWeb appliance. The logo image will be included in the report title. The maximum length is 255 characters.	No default.
`email_attachment_compress {enable | disable}`	Enable to enclose the generated report formats in a compressed archive attached to the email. This field is required if you have enabled email output by enabling one or more of the file formats for email output in output_email {html mht pdf rtf txt}.	`disable`
`email_attachment_name "<filename_str>"`	Type the file name that will be used for the reports attached to the email. The maximum length is 63 characters. This field is required if you have enabled email output by enabling one or more of the file formats for email output in output_email {html mht pdf rtf txt}.	No default.

Variable	Description	Default
`email_body "<message_str>"`	Type the message body of the email. The maximum length is 383 characters. This field is required if you have enabled email output by enabling one or more of the file formats for email output in output_email {html mht pdf rtf txt}.	No default.
`email_subject "<subject_str>"`	Type the subject line of the email. The maximum length is 191 characters. This field is required if you have enabled email output by enabling one or more of the file formats for email output in output_email {html mht pdf rtf txt}.	No default.
`filter_string "<log-filter_str>"`	Type a log message filter string that includes or excludes log messages based upon matching log field values. The maximum length is 1,023 characters. For example syntax, see Example on page 117.	No default.
`include_nodata {yes | no}`	Select whether to include (`yes`) or hide (`no`) reports which are empty because there is no matching log data.	`no`
`on_demand {enable | disable}`	Enable to run the report one time only. After the FortiWeb appliance completes the report, it removes the report profile from its hard disk. Type `disable` to schedule a time to run the report, and to keep the report profile for subsequent use.	`disable`
`output_email {html mht pdf rtf txt}`	Select one or more file types for the report when mailing generated reports.	No default.
`output_email_policy <policy_name>`	If you set a value for `output_email`, type the name of the email policy that contains settings for sending the report by email. The maximum length is 35 characters. For more information on email policies, see `config log email-policy`.	No default.
`output_file {html mht pdf rtf txt}`	Select one or more file types for the report when saving to the FortiWeb hard disk.	`html`
`output_ftp {html pdf rtf txt mht}`	Select one or more file types for the report when FortiWeb sends reports to an FTP or TFTP server.	No default.
`output_ftp_policy <ftp-policy_name>`	Enter the policy that defines a connection to the appropriate server. See `config log ftp-policy`.	No default.

Variable	Description	Default
period_end <time_str> <date_str>	Enter the time and date that define the **end** of the span of time whose log messages you want to use when generating the report. The time format is hh:mm and the date format is yyyy/mm/dd, where: • hh is the hour according to a 24-hour clock • mm is the minute • yyyy is the year • mm is the month • dd is the day This setting appears only when you select a period_type of other.	No default.
period_last_n <n_int>	Enter the number that defines **n** if the period_type contains that variable. The valid range is from 1 to 2,147,483,647. This setting appears only when you select a period_type of last-n-days, last-n-hours, or last-n-weeks.	No default.
period_start <time_str> <date_str>	Enter the time and date that defines the **beginning** of the span of time whose log messages you want to use when generating the report. The time format is hh:mm and the date format is yyyy/mm/dd, where: • hh is the hour according to a 24-hour clock • mm is the minute • yyyy is the year • mm is the month • dd is the day This setting appears only when you select a period_type of other.	No default.

Variable	Description	Default
`period_type {last-14-days | last-2-weeks | last-30-days | last-7-days | lastmonth | last-n-days | last-n-hours | last-n-weeks | last-quarter | last-week | other | this-month | this-quarter | this-week | this-year | today | yesterday}`	Select the span of time whose log messages you want to use when generating the report. If you select `last-n-days`, `last-n-hours`, or `last-nweeks`, you must also define **n** by entering period_last_n <n_int>. If you select other, you must also define the start and end of the report's time range by entering `period_start` and `period_end`. The span of time will be included in the summary, if enabled. For information on enabling the summary, see scope_include_summary {yes | no}.	`last-7-days`
`report_desc "<comment_str>"`	Type a description of the report, if any, that you want to include in the report summary. If the text is more than one word or contains special characters, surround it with double quotes ("). The maximum length is 63 characters. For information on enabling the summary, see scope_include_summary {yes | no}.	No default.
`report_title <title_str>`	Type a title, if any, that you want to include in the report summary. If the text is more than one word or contains special characters, enclose it in double quotes ("). The maximum length is 127 characters. For information on enabling the summary, see scope_include_summary {yes | no}.	No default.

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

Variable	Description	Default
`Report_traffic_activity {net-pol net-srv net-src net-dst net-src-dst net-dst-src net-date-dst net-hour-dst net-day-dst net-month-dst net-date-src net-hour-src net-day-src net-month-src net-srccountry net-httphost net-username}`	Type zero or more options to indicate which charts based upon traffic logs to include in the report. For example, to include “Top Sources By Day of Week”, enter a list of charts that includes `net-day-src`.	No default.
`Report_pci_activity {pci-attacks-date-type pci-attacks-day-type pci-attacks-hour-type pci-attacks-month-type}`	Type zero or more options to indicate which charts based upon PCI attack logs to include in the report.	No default.
`schedule_type {daily | dates | days | none}`	Select when the FortiWeb appliance will automatically run the report. If you reboot the FortiWeb appliance while the report is being generated, report generation resumes after the boot process is complete. If `schedule_type` is `daily`, `dates` or `days`, specify the `schedule_time`, `schedule_days`, or `schedule_dates` when the report will be generated. If `schedule_type` is none, the report will be generated only when you manually initiate it.	`none`
`schedule_days {sun | mon | tue | wed | thu | fri | sat}`	If `schedule_type` is `days`, select the day of the week when the report should be generated.	No default.
`schedule_dates <dates_str>`	If `schedule_type` is `dates`, select the specific date of the month, from 1 to 31, when the report should be generated. Separate multiple dates with spaces.	No default.
`schedule_time <time_str>`	If `schedule_type` is not `none`, select the time of day when the report should be run. The time format is `hh:mm`, where: • `hh` is the hour according to a 24-hour clock • `mm` is the minute	`00:00`

Variable	Description	Default
scope_include_summary {yes | no}	Enter yes to include a summary section at the beginning of the report. The summary includes: • <report_name> • custom_company "<org_str>" • report_desc "<comment_str>" • the date and time when the report was generated using this profile • the span of time whose log messages were used to generate the report, according to period_type	yes
scope_include_table_of_content {yes | no}	Enter yes to include a table of contents at the beginning of the report. The table of contents includes links to each chart in the report.	yes
scope_top1 <topX_int>	Enter **x** number of items (up to 30) to include in the first cross-section of ranked reports. For some report types, you can set the top ranked items for the report. These reports have “Top” in their name, and will always show only the top **x** entries. Reports that do not include “Top” in their name show all information. Changing the values for top field will not affect these reports.	6
scope_top2 <topY_int>	Enter **y** number of items (up to 30) to include in the second cross-section of ranked reports. For some report types, you can set the number of ranked items to include in the report. These reports have “Top” in their name, and will always show only the top **x** entries. Some report types have two levels of ranking: the top **y** sub-entries for each top **x** entry. Reports that do not include “Top” in their name show all information. Changing the values for top field will not affect these reports.	3

Example

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

```
config log reports
   edit "Report_1"
      set Report_attack_activity attacks-type attacks-url attacks-date-type attacks-month-
          type attacks-day-type attacks-hour-type attacks-type-dev attacks-dst-type
```

```
            attacks-dst-ip attacks-type-ip attacks-method-type attacks-cat attacks-policy
            attacks-day attacks-ts attacks-td attacks-proto attacks-date-severity attacks-
            month-severity attacks-day-severity attacks-hour-severity attacks-sessionid
            attacks-signature-id attacks-srccounty attacks-type-signature-id
        set Report_event_activity ev-all ev-all-cat ev-all-type ev-crit-hour ev-crit-day ev-
            warn-hour ev-warn-day ev-info-hour ev-info-day ev-emer-hour ev-emer-day ev-aler-
            hour ev-aler-day ev-err-hour ev-err-day ev-noti-hour ev-noti-day ev-hour ev-
            hour-cat ev-day ev-day-cat ev-stat
        set Report_traffic_activity net-pol net-srv net-src net-dst net-src-dst net-dst-src
            net-date-dst net-hour-dst net-day-dst net-month-dst net-date-src net-hour-src
            net-day-src net-month-src
        set custom_company "Example, Inc."
        set custom_footer_options custom
        set custom_header "A fictitious corporation."
        set custom_title_logo "titlelogo.jpg"
        set filter_string "(and src==\'172.16.1.10\')"
        set include_nodata yes
        set output_file html pdf
        set output_email html
        set output_email_policy log_report_analysis
        set period_type last-n-days
        set report_desc "A sample report."
        set report_title "Report 1"
        set schedule_type days
        set custom_footer "Weekly report for Example, Inc."
        set period_last_n 14
        set schedule_days sat
        set schedule_time 01:00
    next
end
```

Related topics

- config log attack-log
- config log disk
- config log email-policy
- config log ftp-policy

log sensitive

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

This command is relevant only if you have enabled the FortiWeb appliance to keep packet payloads along with their associated log messages. For details, see config log attack-log and config log traffic-log.

To use this command, your administrator account's access control profile must have either w or rw permission to the loggrp area. For more information, see Permissions on page 74.

Syntax

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

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

Example

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

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

Related topics

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

log siem-message-policy

Use this command to configure the FortiWeb appliance to send its log messages to one or more a remote ArcSight SIEM (security information and event management) servers.

You must first define one or more SIEM policies using config log siem-policy.

Logs sent to the ArcSight server are controlled by SIEM policies and trigger actions that you configure on the FortiWeb appliance, and are associated with various types of violations.

Usually, you should set trigger actions for specific types of violations. Failure to do so will result in the FortiWeb appliance logging every occurrence, which could result in high log volume and reduced system performance. Excessive logging for an extended period of time may cause premature hard disk failure.

Logs stored remotely cannot be viewed from the web UI, and cannot be used by FortiWeb to build reports. If you require these features, record logs locally as well as remotely.

Syntax

```
config log siem-message-policy
   set siem-policy <policy_name>
   set severity {alert | critical | debug | emergency | error | information |
       notification | warning}
   set analyzer-policy <fortianalyzer-policy_name>
end
```

Variable	Description	Default
`siem-policy <policy_name>`	Type the name of an existing SIEM policy to use when storing log information remotely. The maximum length is 35 characters. To view a list of the existing SIEM policies, type: `set siem-policy ?`	No default.
`severity {alert | critical | debug | emergency | error | information | notification | warning}`	Select the severity level that a log message must meet or exceed in order to cause the FortiWeb appliance to save it to the ArcSight server.	`information`
`status {enable | disable}`	Enable to record event log messages to the ArcSight server if it meets or exceeds the severity level specified by `severity`.	`disable`

Example

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

```
config log siem-message-policy
   set status enable
   set severity error
   set siem-policy SIEM_Policy1
end
```

Related topics

- `config log siem-policy`

log siem-policy

Use this command to configure a connection to one or more ArcSight SIEM (security information and event management) servers. The policy is used by the `log syslogd` configuration to define the specific ArcSight server on which log messages are stored. For more information, see `config log syslogd`.

Currently, because all SIEM policies send logs using ArcSight CEF (common event format), the value of `type` is always `cef`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see Permissions on page 74.

Syntax

```
config log siem-policy
   edit <policy_name>
      config siem-server-list
         edit <entry_index>
            set type <arcsight-cef | azure-cef>
            set port <port_int>
            set server <siem_ipv4>
         end
      next
end
```

Variable	Description	Default
`<policy_name>`	Type the name of a new or existing SIEM policy. The maximum length is 35 characters. To display the list of existing policies, type: `edit ?`	No default.
`<entry_index>`	Enter the index number of the individual entry in the table.	No default.
`type <arcsight-cef | azure-cef>`	Select whether this configuration connects to an ArcSight server or, if your appliance is deployed on Azure, Azure Event Hub. The Azure CEF policy type requires you to complete Azure event hub settings using the `config system eventhub` CLI command.	`arcsight-cef`
`port <port_int>`	The port where the ArcSight server listens for log output.	`514`
`server <siem_ipv4>`	The IP address of the ArcSight server.	No default.

Example

This example creates `SIEM_Policy1`. FortiWeb contacts the ArcSight server using its IP address, `192.168.1.10`. Communications occur over the standard port number for ArcSight, UDP port `514`. The FortiWeb appliance sends log messages to the server in CEF format.

```
config log siem-policy
   edit SIEM_Policy1
      config siem-server-list
         edit 1
            set type arcsight-cef
            set port 514
            set server 192.168.1.10
         end
      next
end
```

Related topics

- `config log siem-policy`
- `config system dns`
- `config router static`

log syslogd

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

For improved performance, unless necessary, avoid logging highly frequent log types. While logs sent to your Syslog server do not persist in FortiWeb's local RAM, FortiWeb still must use bandwidth and processing resources while sending the log message.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see Permissions on page 74.

Syntax

```
config log syslogd
   set status {enable | disable}
   set facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp |
      kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 |
      local7 | mail | ntp | user}
   set severity {alert | critical | debug | emergency | error | information |
      notification | warning}
   set policy <syslogd-policy_name>
end
```

Variable	Description	Default
`status {enable | disable}`	Enable to send log messages to the Syslog server defined by `config log syslog-policy`. Also configure `facility`, `policy` and `severity`.	`disable`
`facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp | kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | mail | ntp | user}`	Type the facility identifier that the FortiWeb appliance will use to identify itself when sending log messages to the first Syslog server. 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.	`local7`
`severity {alert | critical | debug | emergency | error | information | notification | warning}`	Select the severity level that a log message must meet or exceed in order to cause the FortiWeb appliance to send it to the first Syslog server.	`information`
`policy <syslogd-policy_name>`	If logging to a Syslog server is enabled, type the name of a Syslog policy which describes the Syslog server to which the log message will be sent. The maximum length is 35 characters. For more information on Syslog policies, see `config log syslog-policy`.	No default.

Example

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

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

log syslog-policy

Use this command to configure a connection to one or more Syslog servers. Each policy can specify connections for up to three Syslog servers. The `log syslogd` configuration uses the policy to define the specific Syslog server or servers on which log messages are stored. For more information, see `config log syslogd`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see Permissions on page 74.

Syntax

```
config log syslog-policy
   edit <policy_name>
      config log-server-list
         edit <entry_index>
            set csv {enable | disable}
            set port <port_int>
            set server <syslog_ipv4>
      end
   next
end
```

Variable	Description	Default
`<policy_name>`	Type the name of a new or existing Syslog policy. The maximum length is 35 characters. The name of the report profile will be included in the report header. To display the list of existing policies, type: `edit ?`	No default.
`<entry_index>`	Enter the index number of the individual entry in the table. You can create up to 3 connections.	No default.
`csv {enable | disable}`	Enable if the Syslog server requires the FortiWeb appliance to send log messages in comma-separated value (CSV) format, instead of the standard Syslog format.	`disable`
`port <port_int>`	Type the port number on which the Syslog server listens. The valid range is from 1 to 65,535.	`514`
`server <syslog_ipv4>`	Type the IP address of the Syslog server.	No default.

Example

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

```
config log syslog-policy
   edit Syslog_Policy1
      config log-server-list
         edit 1
            set server 192.168.1.10
            set port 514
```

```
            set csv enable
        end
    next
end
```

Related topics

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

log traffic-log

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

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

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

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

To use this command, your administrator account's access control profile must have either w or rw permission to the loggrp area. For more information, see Permissions on page 74.

Syntax

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

Variable	Description	Default
status {enable | disable}	Enable to record traffic log messages if disk log storage is enabled, and the logs meet or exceed the severity levels selected using config log disk.	disable
packet-log {enable | disable}	Enable to keep packet payloads stored with their associated traffic log message. For information on obscuring sensitive information in packet payloads, see config log sensitive.	disable
message-event {enable | disable}		disable

Example

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

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

Related topics

- `config log attack-log`
- `config log event-log`
- `config log disk`
- `config log sensitive`
- `diagnose debug application miglogd`
- `diagnose log`

log trigger-policy

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

You apply trigger policies to individual conditions that have an associated action and severity, such as attacks and rule violations. A trigger policy has the following components:

- an email policy (contains the details associated with the recipient email account)
- a Syslog policy (contains details required to communicate with the Syslog server)
- a FortiAnalyzer policy (contains the IP address of the remote FortiAnalyzer appliance)

The trigger policy determines whether an email is sent to administrators when a certain condition occurs and whether the log messages associated with the condition are stored on a Syslog server or FortiAnalyzer.

You define the email, Syslog, and FortiAnalyzer policies before you apply the trigger policy to an individual condition. For more information, see `config log email-policy`, `config log syslog-policy`, and `config log fortianalyzer-policy`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For more information, see Permissions on page 74.

Syntax

```
config log trigger-policy
   edit <trigger-policy_name>
        set email-policy <email-policy_name>
        set syslog-policy <syslog-policy_name>
```

```
        set analyzer-policy <fortianalyzer-policy_name>
        set siem-policy <siem-policy_name>
    next
end
```

Variable	Description	Default
<trigger-policy_name>	Type the name of a new or existing trigger policy. The maximum length is 35 characters.	No default.
email-policy <email-policy_name>	Type the name of the email policy to be used with the trigger policy. The maximum length is 35 characters. If the conditions associated with the trigger policy occur, the email policy determines the recipients of the notification email messages associated with the condition. For more information, see config log email-policy.	No default.
syslog-policy <syslog-policy_name>	Type the name of the Syslog policy to be used with the trigger policy. The maximum length is 35 characters. If the conditions associated with the trigger policy occur, the Syslog policy determines which Syslog server the messages are sent to. For more information, see config log syslog-policy.	No default.
analyzer-policy <fortianalyzer-policy_name>	Type the name of an existing FortiAnalyzer policy to be used with the trigger policy. The maximum length is 35 characters. See config log fortianalyzer-policy.	No default.
siem-policy <siem-policy_name>	Type the name of an existing SIEM policy to be used with the trigger policy. The maximum length is 35 characters. See config log siem-policy.	No default.

Example

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

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

Related topics

- config log email-policy
- config log syslog-policy
- config log fortianalyzer-policy
- config log siem-policy
- config waf http-protocol-parameter-restriction
- config waf signature

router policy

Use this command to configure policy routes that redirect traffic away from a static route.

For example, you can divert traffic for intrusion protection scanning (IPS). It is also useful if your FortiWeb protects web servers for different customers (for example, the clients of a Managed Security Service Provider).

Policy routes can direct traffic to a specific network interface and gateway based on the packet's source and destination IP address.

Syntax

```
config router policy
   edit <policy_index>
      set iif <incoming_interface_name>
      set src <source_ip>
      set dst <destination_ip>
      set oif <outgoing_interface_name>
      set gateway <router_ip>
      set priority <priorty_int>
   next
end
```

Variable	Description	Default
<policy_index>	Enter the index number of the policy route. The valid range is from 1 to 4,294,967,295.	No default.
<incoming_interface_name>	Enter the name of the interface, such as port1, on which FortiWeb receives packets it applies this routing policy to.	No default.
src <source_ip>	Enter the source IP address and netmask to match, separated with a space. FortiWeb routes matching traffic through the specified interface and gateway.	0.0.0.0 0.0.0.0

Variable	Description	Default
`dst <destination_ip>`	Enter the destination IP address and netmask to match, separated with a space. FortiWeb routes matching traffic through the specified interface and gateway.	`0.0.0.0 0.0.0.0`
`<outgoing_interface_name>`	Enter the name of the interface, such as `port2`, through which FortiWeb routes packets that match the specified IP address information.	No default.
`gateway <router_ip>`	Enter the IP address of a next-hop router.	`0.0.0.0`
`priority <priorty_int>`	Enter a value between 1 and 200 that specifies the priority of the route. When packets match more than one policy route, FortiWeb directs traffic to the route with the lowest value.	`200`

Related topics

- `config router static`
- `config router setting`

router setting

Use this command to change how FortiWeb handles non-HTTP/HTTPS traffic (for example, SSH and FTP) when it is operating in reverse proxy mode.

When this setting is disabled (the default) and FortiWeb is operating in reverse proxy mode, the appliance drops any non-HTTP/HTTPS traffic.

When this setting is enabled and FortiWeb is operating in reverse proxy mode, the appliance handles non-HTTP/HTTPS protocols in the following ways:

- Any non-HTTP/HTTPS traffic destined for a virtual server on the appliance is dropped.
- For any non-HTTP/HTTPS traffic destined for another destination (for example, a back-end server), FortiWeb acts as a router and forwards it based in its destination address.

This command has no effect when FortiWeb is operating in transparent modes, which allow and forward non-HTTP/HTTPS packets by default.

Use this setting only if necessary. For security and performance reasons, if you have a FortiGate with an Internet/public address virtual IP (VIP) that forwards traffic to your FortiWeb, and your FortiWeb is on the same subnet as your web servers, do not use this setting. Instead, configure the VIP to forward:

- only HTTP/HTTPS to FortiWeb, which forwards it to your servers
- specific traffic such as SSH or SFTP directly to your servers

This avoids latency related to an extra hop. It also avoids accidentally forwarding unscanned protocols.

Routing is best effort. Not all protocols may be supported, such as Citrix Receiver (formerly ICA).

FortiWeb appliances are designed to provide in-depth protection specifically for the HTTP and HTTPS protocols. Because of this, when in **reverse proxy mode**, by default, FortiWeb **does not forward non-HTTP/HTTPS protocols** to your protected web servers. (That is, IP-based forwarding is disabled. Traffic is only forwarded if picked up and scanned by the HTTP reverse proxy.) This provides a secure default configuration by blocking traffic to services that might have been unintentionally left open and should not be accessible to the general public.

In some cases, however, a web server provides more services, not just HTTP or HTTPS. A typical exception is a server that also allows SFTP and SSH access. In these cases, enable routing to allow FortiWeb to route the non-HTTP/HTTPS traffic to the server using the server's IP address. For HTTP/HTTPS services, direct traffic to the IP address of the FortiWeb virtual server, which forwards requests to the back-end server after inspection.

This command has no equivalent in the web UI.

Use the following commands to retrieve information about current static route values:

```
config router setting
   get route static
end
```

Use the following commands to view the current value of `ip-forward`:

```
config router setting
   get route setting
end
```

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `netgrp` area. For more information, see Permissions on page 74.

Syntax

```
config router setting
   set ip-forward {enable | disable}
   set ip6-forward {enable | disable}
end
```

Variable	Description	Default
`ip-forward {enable | disable}`	Enable to forward non-HTTP/HTTPS traffic if its IPv4 IP address matches a static route.	`disable`

Variable	Description	Default
`ip6-forward {enable | disable}`	Enable to forward non-HTTP/HTTPS traffic if its IPv6 IP address matches a static route.	`disable`

Example

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

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

Related topics

- `config router static`
- `config router policy`
- `config router all`

router static

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

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

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

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

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

The FortiWeb appliance examines the packet's destination IP address and compares it to those of the static routes. If more than one route matches the packet, the FortiWeb appliance applies the route with the smallest index number. For this reason, you should give more specific routes a smaller index number than the default route.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `netgrp` area. For more information, see Permissions on page 74.

Syntax

```
config router static
   edit <route_index>
      set device <interface_name>
      set dst <destination_ip>
      set gateway <router_ip>
   next
end
```

Variable	Description	Default
<route_index>	Type the index number of the static route. If multiple routes match a packet, the one with the smallest index number is applied. The valid range is from 1 to 4,294,967,295.	No default.
device <interface_name>	Type the name of the network interface device, such as port1, through which traffic subject to this route will be outbound. The maximum length is 35 characters.	No default.
dst <destination_ip>	Enter the destination IP address and netmask of traffic that will be subject to this route, separated with a space. To indicate all traffic regardless of IP address and netmask (that is, to configure a route to the default gateway), enter 0.0.0.0 0.0.0.0. or ::/0.	0.0.0.0 0.0.0.0
gateway <router_ip>	Enter the IP address of a next-hop router. **Caution:** The gateway IP address must be in the same subnet as the interface's IP address. If you change the interface's IP address later, the new IP address must also be in the same subnet as the interface's default gateway address. Otherwise, all static routes and the default gateway will be lost.	0.0.0.0

Example

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

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

Related topics

- config router setting
- config router policy
- config system interface
- config log syslog-policy
- config server-policy policy
- config system admin
- config system dns
- config system global
- config system snmp community
- config wad website
- execute traceroute
- diagnose network arp
- diagnose network ip
- diagnose network route
- get router all

server-policy allow-hosts

Use this command to configure protected host groups.

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

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

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

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

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

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

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

Protected host groups can be used by:

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

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

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see Permissions on page 74.

Syntax

```
config server-policy allow-hosts
   edit <protected-hosts_name>
      set default-action {allow | deny}
      config host-list
         edit <protected-host_index>
            set action {allow | deny}
            set host {<host_ipv4> | <host_fqdn> | <host_ipv6>}
         next
      end
   next
end
```

Variable	Description	Default
`<protected-hosts_name>`	Type the name of a new or existing group of protected hosts.The maximum length is 35 characters. To display the list of existing groups, type: `edit ?`	No default.
`default-action {allow | deny}`	Select whether to accept or deny HTTP requests whose `Host:` field does **not** match any of the host definitions that you will add to this protected hosts group.	`allow`

Variable	Description	Default
<protected-host_index>	Type the index number of a protected host within its group. The valid range is from 1 to 9,223,372,036,854,775,807. Each host-list can contain up to 64 IP addresses and/or fully qualified domain names (FQDNs).	No default.
action {allow | deny}	Select whether to accept or deny HTTP requests whose `Host:` field matches the host definition in host {<host_ipv4> | <host_fqdn> | <host_ipv6>}.	allow
host {<host_ipv4> | <host_fqdn> | <host_ipv6>}	Type the IP address or FQDN of a virtual or real web host, as it appears in the `Host:` field of HTTP headers, such as `www.example.com`. The maximum length is 255 characters. 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 actual IP address of the web server. For example, if a virtual server 10.0.0.1/24 forwards traffic to the physical server 192.168.1.1, for protected hosts, you would enter: • `10.0.0.1`, the address of the virtual server • `www.example.com`, the domain name that resolves to the virtual server	No default.

Example

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

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

Related topics

- config server-policy policy
- config waf allow-method-exceptions
- config server-policy custom-application application-policy
- config waf input-rule
- config waf signature
- config waf start-pages
- config waf page-access-rule
- config waf hidden-fields-rule

server-policy custom-application application-policy

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

To solve this kind of problem, FortiWeb uses application policy plug-ins that recognize the non-standard application URLs so that the auto-learning profile can work properly.

First create a URL interpreter (see config server-policy custom-application url-replacer) and then use this command to create an application policy to use it.

To use this command, your administrator account's access control profile must have either w or rw permission to the traroutegrp area. For more information, see Permissions on page 74.

Syntax

```
config server-policy custom-application application-policy
   edit analyzer-policy <fortianalyzer-policy_name>
      config rule-list
         edit analyzer-policy <fortianalyzer-policy_name>
            set analyzer-policy <fortianalyzer-policy_name>
            set analyzer-policy <fortianalyzer-policy_name>
         next
      end
   next
end
```

Variable	Description	Default
<policy_name>	Type the name of a new or existing application policy. The maximum length is 35 characters. To display the list of existing policies, type: edit ?	No default.

Variable	Description	Default
<entry_index>	Type the index number of the individual rule in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
plugin-name <url-replacer_name>	Type the name of an existing URL interpreter. The maximum length is 35 characters.	No default.
type {URL_Replacer}	Type the name of the plug-in type. (Currently, only the URL_Replacer option is supported.)	URL_Replacer

Example

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

```
config server-policy custom-application application-policy
   edit replacer-policy1
      config rule-list
         edit 1
            set plugin-name url-replacer1
         next
         edit 2
            set plugin-name url-replacer2
         next
      end
   next
end
```

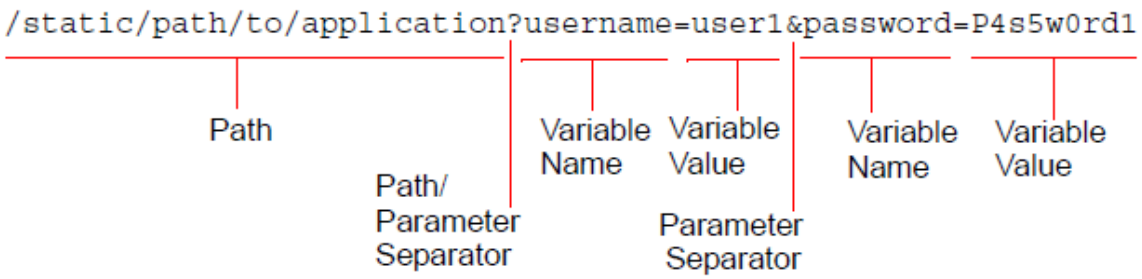
Related topics

- config server-policy custom-application application-policy
- config waf web-protection-profile autolearning-profile

server-policy custom-application url-replacer

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 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 face 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 use this command and `config server-policy custom-application application-policy` to apply 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.

For example, if the URL is:

```
/application/value
```

and the URL replacer settings are:

Setting name	Value
type {pre-defined | custom-defined}	custom-defined
url "<original-url_str>"	(/application/)([^/]+\\.[^/]+)
new-url <new-url_str>	$0
param <value_str>	$1
new-param <replaced-param_name>	setting

then the URL will be interpreted by auto-learning as:

```
/application?setting=value
```

To apply interpret non-standard URLs:

1. Create the custom URL replacer.
2. Add the URL replacer to a custom application policy see `config server-policy custom-application application-policy`).
3. Apply the custom application policy in an auto-learning profile (see `config waf web-protection-profile autolearning-profile`).
4. Finally, apply the auto-learning profiles in a server policy (see `config server-policy policy`).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see Permissions on page 74.

Syntax

```
config server-policy custom-application url-replacer
   edit server-policy custom-application url-replacer
      set type {pre-defined | custom-defined}
      set app-type {jsp | owa-2003}
      set url "<original-url_str>"
      set new-url <new-url_str>
      set param <value_str>
      set new-param <replaced-param_name>
   next
end
```

Variable	Description	Default
<interpreter_name>	Type the name of a new or existing URL interpreter. The maximum length is 35 characters. To display the list of existing URL interpreter, type: edit ?	No default.

Variable	Description	Default
`type {pre-defined | custom-defined}`	Select either: • `pre-defined` — Use one of the predefined URL replacers for well-known web applications, which you select in app-type {jsp | owa-2003}. • `custom-defined` — Define your own URL replacer by configuring url "<original-url_str>", new-url <new-url_str>, param <value_str>, and new-param <replaced-param_name>	`pre-defined`
`app-type {jsp | owa-2003}`	If `type` is `pre-defined`, select which predefined URL interpreter to use, either: • `jsp` — Use the URL replacer designed for Java server pages (JSP) web applications, where parameters are often separated by semi-colons (;). • `owa-2003` — User the URL replacer designed for Microsoft Outlook Web App (OWA) 2003, where user name and directory parameters are often embedded in the URL.	`jsp`
`url "<original-url_str>"`	Type a regular expression, such as `^/(.*)/(.*)$`, matching **all** and **only** the URLs to which the URL replacer should apply. The pattern does not require a backslash (/). However, it must at least match URLs that begin with a slash as they appear in the HTTP header, such as `/index.html`. Do not include the domain name, such as `www.example.com`. This setting is used only if `type` is `custom-defined`. The maximum length is 255 characters. **Note:** Auto-learning consider URLs up to approximately 180 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 so will ignore it. No event log will be created in this case. **Note:** If this URL replacer will be used **sequentially** in its set of URL replacers, instead of being mutually exclusive, this regular expression should match the URL produced by the previous interpreter, **not** the original URL from the request.	No default.

Variable	Description	Default
new-url <new-url_str>	Type either a literal URL, such as /index.html, or a regular expression with a back-reference (such as /$1) defining how the URL will be interpreted. This setting is used only if type is custom-defined. The maximum length is 255 characters. **Note:** Back-references can only refer to capture groups (parts of the expression surrounded with parentheses) within the same URL replacer. Back-references **cannot** refer to capture groups in other URL replacers.	No default.
param <value_str>	Type either the parameter's literal value, such as user1, or a back-reference (such as /$0) defining how the value will be interpreted. This setting is used only if type is custom-defined. The maximum length is 255 characters.	No default.
new-param <replaced-param_name>	Type either the parameter's literal name, such as username, or a back-reference (such as $2) defining how the parameter's name will be interpreted in the auto-learning report. This setting is used only if type is custom-defined. The maximum length is 255 characters. **Note:** Back-references can only refer to capture groups (parts of the expression surrounded with parentheses) within the same URL replacer. Back-references **cannot** refer to capture groups in other URL replacers.	No default.

Example

This example assumes the HTTP request URL from a client is /mary/login.asp. The URL replacer interprets the URL to be /login.asp?username=mary.

```
config server-policy custom-application url-replacer
   edit url-replacer1
      set type custom-defined
      set url ^/(.*)/(.*)$
      set new-url /$1
      set param $0
      set new-param username
   next
end
```

Related topics

- config server-policy custom-application application-policy

server-policy health

Use this command to configure server health checks.

Tests for server responsiveness (called “server health checks” in the web UI) poll web servers that are members of a server pool to determine their availability before forwarding traffic. Server health checks can use TCP, HTTP/HTTPS, ICMP `ECHO_REQUEST` (`ping`), TCP SSL, or TCP half-open.

The FortiWeb appliance polls the server at the frequency set in the interval <seconds_int> 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 back-end server will be unavailable for a long period, such as when a server is undergoing hardware repair, it is experiencing extended downtime, or when you have removed a server from the server pool, you can improve the performance of your FortiWeb appliance by disabling the back-end server, rather than allowing the server health check to continue to check for responsiveness. For details, see `config server-policy server-pool`.

To apply server health checks, select them in a server pool configuration. For details, see `config server-policy server-pool`.

To use this command, your administrator account’s access control profile requires either `w` or `rw` permission to the `traroutegrp` area. For more information, see Permissions on page 74.

Syntax

```
config server-policy health
   edit <health-check_name>
      set trigger-policy <trigger-policy_name>
      set relationship {and |or}
      configure health-list
         edit <entry_index>
            set type {icmp | tcp | http | https | tcp-ssl | tcp-half-open}
            set timeout <seconds_int>
            set retry-times <retries_int>
            set interval <seconds_int>
            set url-path <request_str>
            set method {get | head | post}
            set host <host_str>
            set match-type {response-code | match-content | all}
            set response-code {response-code_int}
            set match-content {match-content_str}
         next
end
```

Variable	Description	Default
<health-check_name>	Type the name of the server health check. The maximum length is 35 characters. To display the list of existing server health checks, type: edit ?	No default.
trigger-policy <trigger-policy_name>	Type the name of the trigger to apply when the health check detects a failed server (see config log trigger-policy). The maximum length is 35 characters. To display the list of existing trigger policies, type: set trigger ?	No default.
relationship {and |or}	• and — FortiWeb considers the server to be responsive when it passes all the tests in the list. • or — FortiWeb considers the server to be responsive when it passes at least one of the tests in the list.	and
<entry_index>	Type the index number of the individual rule in the table. The valid range is from 1 to 16.	No default.

Variable	Description	Default
`type {icmp | tcp | http | https | tcp-ssl | tcp-half-open}`	• `icmp` — Send ICMP type 8 (`ECHO_REQUEST`) and listen for either ICMP type 0 (`ECHO_RESPONSE`) indicating responsiveness, or timeout indicating that the host is not responsive. • `tcp` — Send TCP `SYN` and listen for either TCP `SYN ACK` indicating responsiveness, or timeout indicating that the host is not responsive. • `http` — Send an HTTP request and listen for the code specified by `response-code`, the page content specified by `match-content`, or both the code and the content, or timeout indicating that the host is not responsive. Apply to server pool members only if the **SSL** setting for the member is disabled. • `https` — Send an HTTPS request and listen for the code specified by `response-code`, the page content specified by `match-content`, or both the code and the content, or timeout indicating that the host is not responsive. Apply to server pool members only if the **SSL** setting for the member is enabled. • `tcp-ssl` — Send an HTTPS request. FortiWeb considers the host to be responsive if the SSL handshake is successful, and closes the connection once the handshake is complete. This type of health check requires fewer resources than `http` or `https`. Apply to server pool members only if the **SSL** setting for the member is enabled. • `tcp-half-open` — Send TCP `SYN` and listen for either TCP `SYN ACK` indicating responsiveness, or timeout indicating that the host is not responsive. If the response is `SYN ACK`, send TCP `RST` to terminate the connection. This type of health check requires fewer resources from the pool member than `tcp`.	`ping`
`timeout <seconds_int>`	Type the number of seconds which must pass after the server health check to indicate a failed health check. The valid range is from 1 to 10 seconds.	`3`

Variable	Description	Default
`retry-times <retries_int>`	Type the number of times, if any, a failed health check will be retried before the server is determined to be unresponsive. The valid range is from 1 to 10 retries.	`3`
`interval <seconds_int>`	Type the number of seconds between each server health check. The valid range is from 1 to 10 seconds.	`10`
`url-path <request_str>`	Type the URL, such as `/index.html`, that FortiWeb uses in the HTTP/HTTPS request to verify the responsiveness of the server. If the web server successfully returns this URL, and its content matches the expression specified by `match-content`, FortiWeb considers it to be responsive. Available when `type` is `http` or `https`.	No default.
`method {get | head | post}`	Specify whether the health check uses the HEAD, GET, or POST method. Available when `type` is `http` or `https`.	`get`
`host <host_str>`	Optionally, enter the HTTP host header name of a specific host. This is useful if the pool member hosts multiple web sites (virtual hosting environment). Available when `type` is `http` or `https`.	No default.
`match-type {response-code | match-content | all}`	• `response-code` — If the web server successfully returns the URL specified by `url-path` and the code specified by `response-code`, FortiWeb considers the server to be responsive. • `match-content` — If the web server successfully returns the URL specified by `url-path` and its content matches the `match-content` value, FortiWeb considers the server to be responsive. • `all` — If the web server successfully returns the URL specified by `url-path` and its content matches the `match-content` value, and the code specified by `response-code`, FortiWeb considers the server to be responsive. Available when `type` is `http` or `https`.	`match-content`

Variable	Description	Default
response-code {response-code_int}	Enter the response code that you require the server to return to confirm that it is available, if match-type is response-code or all. Available when type is http or https.	200
match-content {match-content_str}	Enter a regular expression that matches the content that must be present in the HTTP reply to indicate proper server connectivity, if match-type is match-content or all. Available when type is http or https.	No default.

Example

This example configures a server health check that periodically requests the main page of the web site, /index. If a physical server does not successfully return that page (which contains the word “About”) every 10 seconds (the default), and fails the check at least three times in a row, FortiWeb considers it unresponsive and forwards subsequent HTTP requests to other physical servers in the server farm.

```
config server-policy health
   edit status_check1
      set trigger-policy "notification-servers1"
      configure health-list
         edit 1
            set type http
            set retry-times 3
            set url-path "/index"
            set method get
            set match-type match-content
            set regular "About"
   next
end
```

Related topics

- config server-policy server-pool
- config server-policy policy
- config log trigger-policy

server-policy http-content-routing-policy

Use this command to configure HTTP header-based routing.

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 define how FortiWeb routes requests to server pools. They are based on one or more of the following HTTP header elements:

- Host
- URL
- Parameter
- Referer
- cookie
- Header
- Source IP
- X.509 certificate

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

If you have configured request rewriting, configure HTTP content-based routing using the original request URL and/or `Host:` name, as it appears **before** FortiWeb has rewritten it. For more information on rewriting, see `config waf url-rewrite url-rewrite-policy`.

To apply your HTTP-based routes, select them when you configure the server policy (see `config server-policy policy`).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see Permissions on page 74.

Syntax

```
config server-policy http-content-routing-policy
   edit <routing-policy_name>
      set server-pool <server-pool_name>
      config content-routing-match-list
         edit <entry_index>
            set match-object {http-host | http-request | url-parameter | http-
                referer | http-cookie | http-header | source-ip | x509-
                certificate-Subject | x509-certificate-Extension}
            set match-condition {match-begin | match-end | match-sub | match-
                domain | match-dir | match-reg | ip-range | ip-range6 | equal}
            set x509-subject-name {E | CN | OU | O | L | ST | C}
            set match-expression <match-expression_str>
            set name <name_str>
            set name-match-condition {match-begin | match-end | match-sub |
                match-reg | equal}
            set value <value_str>
            set value-match-condition {match-begin | match-end | match-sub |
                match-reg | equal}
            set start-ip <start_ip>
            set end-ip <end_ip>
            set concatenate { and | or }
         next
      end
   next
end
```

Variable	Description	Default
<routing_policy_name>	Type the name of the HTTP content routing policy. The maximum length is 63 characters. To display the list of existing policies, type: `edit ?`	No default.
server-pool <server-pool_name>	Type the name of the server pool to which FortiWeb forwards traffic when the traffic matches rules in this policy. For more information, see `config server-policy server-pool`.	No default.
<entry_index>	Type the index number of the individual rule in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
match-object {http-host | http-request | url-parameter | http-referer | http-cookie | http-header | source-ip | x509-certificate-Subject | x509-certificate-Extension}	Type the type of object that FortiWeb examines for matching values: • `http-host` — `Host:` field • `http-request` — A URL • `url-parameter` — A URL parameter and value • `http-referer` — `Referer:` field • `http-cookie` — A cookie name and value • `http-header` — A header name and value • `source-ip` — An IPv4 address or address range or IPv6 address or address range • `x509-certificate-Subject` — A specified Relative Distinguished Name (RDN) in the X509 certificate `Subject` field. Also specify `x509-subject-name`. • `x509-certificate-Extension` — Additional fields that the extensions field adds to the X509 certificate	No default.

Variable	Description	Default
`match-condition {match-begin | match-end | match-sub | match-domain | match-dir | match-reg | ip-range | ip-range6 | equal}`	Type the type of value to match. Values can be a literal value that appears in the object or a regular expression. The value of `match-object` determines which content types you can specify. If `match-object` is `http-host`, `http-request`, `http-referer`, or `x509-certificate-Extension`: • `match-begin` — The object to match begins with the specified string. • `match-end` — The object to match ends with the specified string. • `match-sub` — The object to match contains the specified string. • `equal` — The object to match is the specified string.	No default.

Variable	Description	Default

	If `match-object` is `http-host` only:
	• `match-domain` — The object to match contains the specified string between the periods in a domain name.
	For example, if `match-expression` is `abc`, the condition matches the following hostnames:
	`dname1.abc.com`
	`dname1.dname2.abc.com`
	However, the same Match Simple String value does not match the following hostnames:
	`abc.com`
	`dname.abc`
	If `match-object` is `http-request` :
	• `match-dir` — The object to match contains the specified string between delimiting characters (slash) in a domain name.
	For example, if `match-expression` is `abc`, the condition matches the following hostnames:
	`test.com/abc/`
	`test.com/dir1/abc/`
	However, the same `match-string` value does not match the following hostnames:
	`test.com/abc`
	`test.abc.com`
	If `match-object` is `source-ip` :
	• `ip-range` — The source IP to match is an IPv4 IP address or within a range of IPv4 IP addresses.
	• `ip-range6` — The source IP to match is an IPv6 IP address or within a range of IPv6 IP addresses.
	If `match-object` is `http-host`, `http-request`, `http-referer`, `source-ip`, or `x509-certificate-Extension`:
	• `match-reg` — The object to match has a value that matches the specified regular expression.
		No default.

Variable	Description	Default
`x509-subject-name {E | CN | OU | O | L | ST | C}`	Enter the attribute type to match. Available when `match-object` is `x509-certificate-Subject`.	No default.
`match-expression <match-expression_str>`	Specifies a value to match in the object element specified by `match-object` and `match-condition`. Examples: • A literal URL, such as `/index.php`, that a matching HTTP request contains. • An expression, such as `^/*.php`, that matches a URL. **Tip:** When you enter a regular expression using the web UI, you can validate its syntax.	No default.
`name <name_str>`	Type the name of the object to match. The value can be a literal value or a regular expression. For example, the name of a cookie embedded by traffic controller software on one of the servers. Available if `match-object` is `url-parameter`, `http-cookie`, or `http-header`.	No default.
`name-match-condition {match-begin | match-end | match-sub | match-reg | equal}`	Type the type of value to match. The value is specified by `name` and can be a literal value that appears in the object or a regular expression. • `match-begin` — The name to match begins with the specified string. • `match-end` — The name to match ends with the specified string. • `match-sub` — The name to match contains the specified string. • `equal` — The name to match is the specified string. • `match-reg` — The name to match matches the specified regular expression.	No default.
`value <value_str>`	Type the object value to match. The value can be a literal value or a regular expression. Available if `match-object` is `url-parameter`, `http-cookie`, or `http-header`.	No default.

Variable	Description	Default
value-match-condition {match-begin | match-end | match-sub | match-reg | equal}	Type the type of value to match. The value is specified by value and can be a literal value or a regular expression. • match-begin — The value to match begins with the specified string. • match-end — The value to match ends with the specified string. • match-sub — The value to match contains the specified string. • equal — The value to match is the specified string. • match-reg — The value to match matches the specified regular expression.	No default.
start-ip <start_ip>	Type the first IP address in a range of IP addresses. Available if match-condition is ip-range or ip-range6.	No default.
end-ip <end_ip>	Type the last IP address in a range of IP addresses. Available if match-object is source-ip	No default.
concatenate { and | or }	• and — A matching request matches this entry in addition to other entries in the HTTP content routing list. • or —A matching request matches this entry or other entries in the list.	and

Example

This HTTP content routing policy routes requests for www.example.com/school to the server pool school-site.

The content routing has three rules: one matches the host (www.example.com), a second matches the sessid cookie, and a third matches the /school URL. In combination, the first and third rules match the request for www.example.com/school.

```
config server-policy http-content-routing-policy
   edit "content_routing_policy1"
      set server-pool school-site
      config content-routing-match-list
         edit 1
            set match-condition match-reg
            set match-expression www.example.com
         next
         edit 2
            set match-object http-cookie
            set name sessid
            set value hash[a-fA-F0-7]*
            set name-match-condition match-reg
            set value-match-condition match-reg
         next
```

```
        edit 3
          set match-object http-request
          set match-expression /school
        next
      end
    next
  end
```

Related topics

- config server-policy server-pool
- config server-policy policy
- config waf url-rewrite url-rewrite-policy

server-policy pattern custom-data-type

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see Permissions on page 74.

Syntax

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

Variable	Description	Default
<custom-data-type_name>	Type the name of the custom data type. The maximum length is 35 characters. To display the list of existing types, type: `edit ?`	No default.
expression <regex_pattern>	Type a regular expression that defines the data type. It should match all data of that type, but nothing else. The maximum length is 2,071 characters.	No default.

Example

This example configures two custom data types.

```
config server-policy pattern custom-data-type
  edit "Level 3 Password-custom"
    set expression "^aaa"
```

```
    next
    edit "Custom Data Type 1"
       set expression "^555"
    next
end
```

Related topics

- config server-policy pattern data-type-group

server-policy pattern custom-global-white-list-group

Use this command to configure objects that will be exempt from scans.

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 use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see Permissions on page 74.

Syntax

```
config server-policy pattern custom-global-white-list-group
   edit <entry_index>
      set status {enable | disable}
      set type {Cookie | Parameter | URL}
      set domain <cookie_fqdn>
      set name <name_str>
      set path <url_str>
      set request-type {plain | regular}
      set request-file <url_str>
   next
end
```

Variable	Description	Default
<entry_index>	Type the index number of the individual rule in the table. The valid range is from 1 to 9,223,372,036,854,775,807.	No default.
status {enable | disable}	Enable to exempt this object from all scans.	enable
type {Cookie | Parameter | URL}	Indicate the type of the object. Depending on your selection, the remaining settings vary.	URL

Variable	Description	Default

domain <cookie_fqdn>	Type the partial or complete domain name or IP address as it appears in the cookie, such as:
	`www.example.com`
	`.google.com`
	`10.0.2.50`
	If clients sometimes access the host via IP address instead of DNS, create white list objects for both.
	This setting is available if `type` is set to `Cookie`.
	Caution: Do not whitelist untrusted subdomains that use vulnerable cookies. It could compromise the security of that domain and its network.
		No default.

name <name_str>	Depending on your selection in `type {Cookie | Parameter | URL}`, either: • type the name of the cookie as it appears in the HTTP request, such as `NID`. • type the name of the parameter as it appears in the HTTP URL or body, such as `rememberme`. This setting is available if `type` is set to `Cookie` or `Parameter`.	No default.
path <url_str>	Type the path as it appears in the cookie, such as `/` or `/blog/folder`. This setting is available if `type` is set to `Cookie`.	No default.
request-type {plain | regular}	Indicate whether the request-file <url_str> field contains a literal URL (`plain`), or a regular expression designed to match multiple URLs (`regular`). This setting is available if `type` is set to `URL`.	`plain`

Variable	Description	Default
request-file <url_str>	Depending on your selection in the request-type {plain | regular} field, enter either: • the literal URL, such as /robots.txt, that the HTTP request must contain in order to match the rule. The URL must begin with a backslash (/). • a regular expression, such as ^/*.html, 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 backslash, such as /index.html. Do not include the domain name, such as www.example.com. This setting is available if type is set to URL.	

Example

This example exempts requests for robots.txt from most scans.

```
config server-policy pattern custom-global-white-list-group
   edit 1
      set request-file /robots.txt
   next
end
```

Related topics

- config waf web-protection-profile inline-protection
- config waf web-protection-profile autolearning-profile

server-policy pattern custom-susp-url

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

To use this command, your administrator account's access control profile must have either w or rw permission to the traroutegrp area. For more information, see Permissions on page 74.

Syntax

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

Variable	Description	Default
<custom-susp-url_name>	Type the name of the custom URL. The maximum length is 35 characters. To display the list of existing URLs, type: edit ?	No default.
expression <url_pattern>	Type either a simple string or a regular expression to defines the custom URL request to check for. The maximum length is 2,071 characters.	No default.

Example

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

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

Related topics

- config server-policy pattern suspicious-url-rule

server-policy pattern custom-susp-url-rule

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

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

To use this command, your administrator account's access control profile must have either w or rw permission to the traroutegrp area. For more information, see Permissions on page 74.

Syntax

```
config server-policy pattern custom-susp-url-rule
   edit <rule_name>
      config type-list
         edit <entry_index>
            set custom-susp-url <suspicious-url_name>
         next
      end
   next
end
```

Variable	Description	Default
<rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: edit ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
custom-susp-url <suspicious-url_name>	Type the name of an existing custom URL already defined using config server-policy pattern custom-susp-url. The maximum length is 35 characters. To display the list of existing rules, type: edit ?	No default.

Example

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

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

Related topics

- config server-policy pattern custom-susp-url

server-policy pattern data-type-group

Use this command to configure data type groups.

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

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

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

Data type groups are used by auto-learning profiles. For details, see `config server-policy policy`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see Permissions on page 74.

Syntax

```
config server-policy pattern data-type-group
   edit <data-type-group_name>
      config type-list
         edit <entry_index>
            set data-type {Address | Canadian_Post_code | Canadian_Province_
                Name | Canadian_SIN | China_Post_Code | Country_Name | Credit_
                Card_Number | Danmark_Postalcode | Dates_and_Times | Email |
                GPA | GUID | ip_address | Indian_Vehicle_Number | Italian_mobile_
                phone | Kuwait_Civil_ID | L1_Password | L2_Password | Markup_or_
                Code | Microsoft_product_key | NINO | Netherlands_Postcode |
                Num | personal_name | Phone | Quebec_Postal_Code | String |
                Swedish_personal_number | Swedish_Postalcode | UAE_land_phone |
                UK_Bank_code | UK_postcode | US_SSN | US_State_Name | US_Street_
                Address | US_Zip_Code | Unix_device_name | Uri | Windows_file_
                name}
         next
      end
   next
end
```

Variable	Description	Default
`<data-type-group_name>`	Type the name of the data type group. The maximum length is 35 characters. To display the list of existing groups, type: `edit ?`	No default.
`<entry_index>`	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.

Variable	Description	Default
`data-type {Address | Canadian_Post_code | Canadian_Province_Name | Canadian_SIN | China_Post_Code | Country_Name | Credit_Card_Number | Danmark_Postalcode | Dates_and_Times | Email | GPA | GUID | ip_address | Indian_Vehicle_Number | Italian_mobile_phone | Kuwait_Civil_ID | L1_Password | L2_Password | Markup_or_Code | Microsoft_product_key | NINO | Netherlands_Postcode | Num | personal_name | Phone | Quebec_Postal_Code | String | Swedish_personal_number | Swedish_Postalcode | UAE_land_phone | UK_Bank_code | UK_postcode | US_SSN | US_State_Name | US_Street_Address | US_Zip_Code | Unix_device_name | Uri | Windows_file_name}`	For each `data-type` entry, enter one of the following predefined data types exactly as shown (available options may vary due to FortiGuard updates): • `Address` — Canadian postal codes and United States ZIP code and ZIP + 4 codes. • `Canadian_Post_code` — Canadian postal codes such as K2H 7B8 or k2h7b8. Does **not** match hyphenations such as K2H-7B8. • `Canadian_Province_Name` — Modern and older names and abbreviations of Canadian provinces in English, as well as some abbreviations in French, such as Quebec, IPE, Sask, and Nunavut. Does **not** detect province names in French, such as Québec. • `Canadian_SIN` — Canadian Social Insurance Numbers (SIN) such as 123-456-789. • `China_Post_Code` — Chinese postal codes such as 610000. • `Country_Name` — Country names, codes, and abbreviations in English characters, such as CA, Cote d'Ivoire, Brazil, Russian Federation, Brunei, and Dar el Salam. • `Credit_Card_Number` — American Express, Carte Blanche, Diners Club, enRoute, Japan Credit Bureau (JCB), Master Card, Novus, and Visa credit card numbers. • `Danmark_Postalcode` — 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. • `Dates_and_Times` — Dates and times in various formats such as +13:45 for time zone offsets, 1:01 AM, 1am, 23:01:01, and 01.01.30 AM for times, and 31.01.2009, 31/01/2009, 01/31/2000, 2009-01-3, 31-01-2009, 1-31-2009, 01 Jan 2009, 01 JAN 2009, 20-Jan-2009 and February 29, 2009 for dates. • `Email` — Email addresses such as admin@example.com • `GPA` — 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 **not** 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. • `GUID` — 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.	No default.

Variable	Description	Default
	• `ip_address` – A public or private IPv4 address, such as 10.0.0.1. Does **not** match IPv6 addresses. • `Indian_Vehicle_Number` — An Indian Vehicle Registration Number, such as mh 12 bj 1780. • `Italian_mobile_phone` — Italian mobile phone numbers with the prefix for international calls, such as +393471234567, or without, such as 3381234567. Does **not** match numbers with a dash or space after the area code, nor VoIP or land lines. • `Kuwait_Civil_ID` — 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. • `L1_Password` — A string of at least 6 characters, with one or more each of lower-case characters, upper-case characters, and digits, such as aBc123. Level 1 passwords are “weak” passwords, generally easier to crack than level 2 passwords. • `L2_Password` — A strong password — string of at least 8 characters, with one or more each of lower-case characters, upper-case characters, digits, and special characters, such as aBc123$%. • `Markup_or_Code` — HTML comments, wiki code, hexadecimal HTML color codes, quoted strings in VBScript and ANSI SQL, SQL statements, and RTF bookmarks such as: • `#00ccff, <!--A comment.-->` • `[link url="http://example.com/url?var=A&var2=B"]` • `SELECT * FROM TABLE` • `{\*\bkmkstart TagAmountText}` Does **not** match ANSI escape codes, which are instead detected as strings. • `Microsoft_product_key` — An alphanumeric key for activation of Microsoft software, such as ABC12-34DEF-GH567-IJK89-LM0NP. Does **not** match keys which are non-hyphenated, nor where letters are not capitalized. • `Netherlands_Postcode` — Netherlands postal codes (“postcodes”) such as 3000 AA or 3000AA. Does **not** match postal codes written in lower-case letters, such as 3000aa. • `NINO` — A United Kingdom National Insurance Number (NINO), such as AB123456D. Does **not** match NINOs written in lower-case letters, such as ab123456d.	

Variable	Description	Default
	• `Num` — Numbers in various monetary, decimal, comma-separated value (CSV) and other formats such as 123, +1.23, $1,234,567.89, 1'235.140, and -123.45e-6. Does **not** detect hexadecimal numbers, which are instead detected as strings or code, and Social Security Numbers, which are instead detected as strings. • `personal_name` – 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 **not** match names written in other languages with accented Latinate characters, hanzu, kanji, or hangul, such as Renée Wächter or 林美. • `Phone` — Australian, United States, and Indian phone numbers in various formats such as (123)456-7890, 1.123.456.7890, 0732105432, and +919847444225. • `Quebec_Postal_Code` — Postal codes written in the style sometimes used by Quebecers, with hyphens between the two parts, such as h2j-3c4 or H2J-3C4. • `String` — Character strings such as alphanumeric words, credit card numbers, United States Social Security Numbers (SSN), UK vehicle registration numbers, ANSI escape codes, and hexadecimal numbers in formats such as user1, 123-45-6789, ABC 123 A, 4125632152365, [32mHello, and 8ECCA04F. • `Swedish_Postalcode` — 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. • `Swedish_personal_number` — Personal identification number ("personnummer") for Sweden, such as 19811116-7845. Must be hyphenated. Does **not** match PINs for persons whose age is 100 or greater. • `UAE_land_phone` — Telephone number for the United Arab Emirates, such as 04 - 3452499 or 04 3452499. Does **not** match phone numbers beginning with 01 or 08. • `UK_Bank_code` — Bank sort codes for the United Kingdom, such as 09-01-29. Must be hyphenated. • `UK_postcode` — Postal codes for the United Kingdom, with or without spaces, such as SW1A 2AA or SW1A2AA. • `Unix_device_name` — Standard Linux or UNIX non-loopback wired Ethernet network interface names, such as eth0. Does **not** match names for any other type of device, such as lo, hdda, or ppp.	

Variable	Description	Default
	• `Uri` — Uniform resource identifiers (URI) such as: http://www.example.com ftp://ftp.example.com mailto:admin@example.com • `US_SSN` — United States Social Security Numbers (SSN) such as 123-45-6789. • `US_State_Name` — United States state names and modern postal abbreviations such as HI and Wyoming. Does **not** detect older postal abbreviations such as FI. or Wyo. • `US_Street_Address` – 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 **not** match: • ZIP + 4 codes that include spaces, or do not have a hyphen (e.g. “10001 - 1111” or “10001 1111”) • city abbreviations of 2 characters (e.g. “NY” instead of “NYC”) • Washington D.C. addresses • multiline addresses on Mac OS X, Linux or Unix computers • unabbreviated state names (e.g. “Delaware”) • addresses ending with the country (e.g. “USA”) • addresses beginning with numbers written as words (e.g. “Seven Main Street” instead of “7 Main Street”) • `US_Zip_Code` — United States ZIP code and ZIP + 4 codes such as 34285-3210. • `Windows_file_name` – A valid windows file name, such as Untitled.txt. Does not match file extensions, or file names without their extensions. To display available options, type: `set data-type ?` **Note:** The web UI displays the regular expressions that define each predefined data type. For details, see the *FortiWeb Administration Guide*.	

Example

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

```
config server-policy pattern data-type-group
   edit data-type-group1
      config type-list
         edit 1
```

```
            set data-type Address
          next
          edit 2
            set data-type Phone
          next
        end
    next
end
```

Related topics

- config waf web-protection-profile autolearning-profile

server-policy pattern suspicious-url-rule

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

Each entry in a suspicious URL group defines a type of URL that the FortiWeb appliance considers to be possibly malicious when gathering data for an auto-learning profile.

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

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

To see the regular expressions used in the predefined suspicious URL rules, in the web UI, go to **Auto Learn > Predefined Pattern > URL Pattern**.

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see Permissions on page 74.

Syntax

```
config server-policy pattern suspicious-url-rule
  edit <rule-group_name>
    config type-list
      edit <entry_index>
        set server-type { Abyss | Apache | Appweb | BadBlue | Blazix |
            Cherokee | ColdFusion | IIS | JBoss | Jetty | Jeus_WebContainer |
            LotusDomino | Tomcat | WebLogic | WebSEAL | WebSiphon | Xerver |
            ZendServer | aolserver  | ghttpd | lighttpd | lilhttpd |
            localweb2000 | mywebserver | ngnix | omnihttpd | samba | squid |
            svn | webshare | xeneo | xitami | zeus | zope}
      next
      end
    set custom-susp-url-rule <rule_name>
    next
```

```
        end
    next
end
```

Variable	Description	Default
<rule-group_name>	Type the name of the suspicious URL rule group. The maximum length is 35 characters. To display the list of existing groups, type: edit ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
server-type { Abyss | Apache | Appweb | BadBlue | Blazix | Cherokee | ColdFusion | IIS | JBoss | Jetty | Jeus_WebContainer | LotusDomino | Tomcat | WebLogic | WebSEAL | WebSiphon | Xerver | ZendServer | aolserver | ghttpd | lighttpd | lilhttpd | localweb2000 | mywebserver | ngnix | omnihttpd | samba | squid | svn | webshare | xeneo | xitami | zeus | zope}	For each rule index, select the type of the web server, application, or servlet. FortiWeb will detect attempts to access URLs that are usually sensitive for that software.	No default.
<rule_name>	Type the name of a custom suspicious URL rule (see config server-policy pattern custom-susp-url-rule).	

Example

This example configures a suspicious URL rule group named suspicious-url-group1 that detects HTTP requests for administratively sensitive URLs for some common web servers that could represent attack attempts and includes a custom suspicious URL rule.

```
config server-policy pattern suspicious-url-rule
   edit suspicious-url-group1
      config type-list
         edit 1
            set server-type Apache
         next
         edit 2
            set server-type Apache
         next
         edit 3
            set server-type Tomcat
         next
```

```
        edit 4
          set server-type WebLogic
        next
      end
      set custom-susp-url-rule "Suspicious URL 1"
      next
end
```

Related topics

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

server-policy persistence-policy

Use this command to configure a persistence method and timeout that you can apply to server pools. The persistence policy applies to all members of the server pool.

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.

To apply a persistence policy, select it when you configure a server pool. For details, see config server-policy server-pool.

To use this command, your administrator account's access control profile must have either w or rw permission to the traroutegrp area. For more information, see Permissions on page 74.

Syntax

```
config server-policy persistence-policy
  edit <persistence-policy_name>
    set type { source-ip | persistent-cookie | asp-sessionid | php-sessionid |
        jsp-sessionid | insert-cookie | http-header | url-parameter | rewrite-
        cookie | embedded-cookie | ssl-session-id }
    set cookie-name <cookie-name_str>
    set timeout <timeout_int>
    set ipv4-netmask <v4mask>
    set ipv6-mask-length <v6mask>
    set http-header <http-header_str>
    set url-parameter <url-parameter_str>
    set cookie-path <cookie-path_str>
    set cookie-domain <cookie-domain_str>
  next
end
```

Variable	Description	Default
<persistence-policy_name>	Type the name of the persistence policy. The maximum length is 63 characters. To display the list of existing persistence policies, type: `edit ?`	No default.

Variable	Description	Default
`type { source-ip | persistent-cookie | asp-sessionid | php-sessionid | jsp-sessionid | insert-cookie | http-header | url-parameter | rewrite-cookie | embedded-cookie | ssl-session-id }`	• `source-ip` — Forwards subsequent requests with the same client IP address and subnet as the initial request to the same pool member. To define how FortiWeb derives the appropriate subnet from the IP address, configure `ipv4-netmask` and `ipv6-mask-length`. • `persistent-cookie` — If an initial request contains a cookie whose name matches the `cookie-name` value, FortiWeb forwards subsequent requests that contain the same cookie value to the same pool member as the initial request. • `asp-sessionid` — 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.) • `php-sessionid` — 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.) • `jsp_sessionid` — FortiWeb forwards subsequent requests with the same JSP session ID as the inital request to the same pool member. (FortiWeb preserves the original cookie name.) • `insert-cookie` — FortiWeb inserts a cookie with the name specified by `cookie-name` 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. Also specify `cookie-path` and `cookie-domain`. • `http-header` — Forwards subsequent requests with the same value for an HTTP header as the initial request to the same pool member. Also configure `http-header`.	`source-ip`

Variable	Description	Default
	• `url-parameter` — Forwards subsequent requests with the same value for a URL parameter as the initial request to the same pool member. Also configure `url-parameter`. • `rewrite-cookie` — If the HTTP response has a `Set-Cookie:` value that matches the value specified by `cookie-name`, FortiWeb replaces the value with a randomly generated cookie value. FortiWeb forwards all subsequent requests with this generated cookie value to the same pool member. • `embedded-cookie` — If the HTTP response contains a cookie with the name specified by `cookie-name`, FortiWeb preserves the original cookie value and adds a randomly generated cookie value and a ~(tilde) as a prefix. FortiWeb forwards all subsequent requests with this cookie and prefix to the same pool member. • `ssl-session-id` — If a cookie in the initial request contains an SSL 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.) For persistence types that use cookies, you can use the `sessioncookie-enforce` setting to maintain persistence for transactions within a session. See `config config server-policy policy`.	
`cookie-name <cookie-name_str>`	Type a value to match or the name of the cookie that FortiWeb inserts. Available only when the persistence type uses a cookie.	No default.

Variable	Description	Default
`timeout <timeout_int>`	Type the maximum amount of time between requests that FortiWeb maintains persistence, in seconds. 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.	`300`
`ipv4-netmask <v4mask>`	Type the IPv4 subnet used for session persistence. For example, if IPv4 Netmask is 255.255.255.255, FortiWeb can forward requests from IP addresses 192.168.1.1 and 192.168.1.2 to different server pool members. If IPv4 Netmask is 255.255.255.0, FortiWeb forwards requests from IP addresses 192.168.1.1 and 192.168.1.2 to the same pool member.	`255.255.255.255`
`ipv6-mask-length <v6mask>`	Type the IPv6 network prefix used for session persistence.	`128`
`http-header <http-header_str>`	Type the name of the HTTP header that the persistence feature uses to route requests.	No default.
`url-parameter <url-parameter_str>`	Type the name of the URL parameter that the persistence feature uses to route requests.	No default.
`cookie-path <cookie-path_str>`	Type a path attribute for the cookie that FortiWeb inserts, if `type` is `insert-cookie`.	No default.
`cookie-domain <cookie-domain_str>`	Specifies a domain attribute for the cookie that FortiWeb inserts, if `type` is `insert-cookie`.	No default.

Example

This example creates the persistence policy `ip-persistence`. When this policy is applied to a server pool, FortiWeb forwards initial requests from an IP address using the load-balancing algorithm configured for the pool. It forwards any subsequent requests with the same client IP address as the initial request to the same pool member. After FortiWeb has not received a request from the IP address for 400 seconds, it forwards any subsequent initial requests from the IP address using the load-balancing algorithm.

```
config server-policy persistence-policy
   edit ip-persistence
```

```
        set type source-ip
        set timeout 400
    next
end
```

Related topics

- config server-policy server-pool

server-policy policy

Use this command to configure server policies.

The FortiWeb appliance applies only one server policy to each connection.

FortiWeb does not use a policy when it is disabled, as indicated by status {enable | disable}.

Policy behavior varies by the operation mode. For details, see the *FortiWeb Administration Guide*.

When you switch the operation mode, FortiWeb deletes server policies from the configuration file if they are not applicable in the current operation mode.

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

- Configure a virtual server and server pool.
- To route traffic based on headers in the HTTP layer, configure one or more HTTP content routing policies.
- To restrict traffic based upon which hosts you want to protect, configure a group of protected host names.
- If you want the FortiWeb appliance to gather auto-learning data, generate or configure an auto-learning profile and its required components.
- If you plan to authenticate users, you need to configure users, user groups, and authentication rules and policy, and include the policy in an inline web protection profile.
- To apply a web protection profile to a server policy, you must first configure them.
- If you want to use the FortiWeb appliance to apply SSL to connections instead of using physical servers, you must also import a server certificate or create a Server Name Indication (SNI) configuration
- If you want the FortiWeb appliance to verify the certificate provided by an HTTP client to authenticate themselves, you must also define a certificate verification rule. If you want to specify whether a client is required to present a personal certificate or not based on the request URL, create a URL-based client certificate group.

For details, see:

- config server-policy allow-hosts
- config server-policy vserver, config server-policy server-pool
- config server-policy http-content-routing-policy
- config user ldap-user, config user local-user, config server-policy custom-application application-policy, config user ntlm-user, config user user-group, config waf http-authen http-authen-rule, config waf http-authen http-authen-policy

- `config waf web-protection-profile inline-protection` (reverse proxy mode or either of the transparent modes), or `config waf web-protection-profile offline-protection` (offline protection mode)
- `config waf web-protection-profile autolearning-profile`
- `config system certificate local`, `config system certificate sni`
- `config system certificate verify`, `config system certificate urlcert`

You can use SNMP traps to notify you of policy status changes, or when a policy enforces your network usage policy. For details, see `config system snmp community`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see Permissions on page 74.

Syntax

```
config server-policy policy
  edit <policy_name>
    set deployment-mode {server-pool | http-content-routing | offline-
        protection | transparent-servers | wccp-servers}
    set vserver <vserver_name>
    set v-zone <bridge_name>
    set data-capture-port <port_int>
    set prefer-current-session {enable |disable}
    set server-pool <server-pool_name>
    set client-real-ip {enable | disable}
    set allow-hosts <hosts_name>
    set block-port <port_int>
    set syncookie {enable | disable}
    set half-open-threshold <packets_int>
    set service <service_name>
    set https-service <service_name>
    set hsts-header {enable | disable}
    set hsts-max-age <timeout_int>
    set certificate <certificate_name>
    set intermediate-certificate-group <CA-group_name>
    set ssl-client-verify <verifier_name>
    set urlcert {enable | disable}
    set urlcert-group <urlcert-group_name>
    set urlcert-hlen
    set client-certificate-forwarding {enable | disable}
    set sni {enable | disable}
    set sni-strict {enable | disable}
    set sni-certificate <sni_name>
    set server-side-sni {enable | disable}
    set ssl-v3 {enable | disable}
    set tls-v10 {enable | disable}
    set tls-v11 {enable | disable}
    set tls-v12 {enable | disable}
    set ssl-pfs {enable | disable}
    set ssl-cipher {medium | high | custom}
    set ssl-custom-cipher {<cipher_1> <cipher2> <cipher3> ...}
    set ssl-rc4-first {enable | disable}
    set ssl-chacha-cipher {enable | disable}
    set ssl-noreg {enable | disable}
    set http-to-https {enable | disable}
    set web-protection-profile <profile_name>
```

```
        set waf-autolearning-profile <profile_name>
        set case-sensitive {enable | disable}
        set comment "<comment_str>"
        set status {enable | disable}
        set monitor-mode {enable | disable}
        set noparse {enable | disable}
        set http-pipeline {enable | disable}
        set sessioncookie-enforce {enable | disable}
        config http-content-routing-list
          edit <entry_index>
            set content-routing-policy-name <content-routing_name>
            set profile-inherit {enable | disable}
            set web-protection-profile <profile_name>
            set is-default {yes | no}
          next
        end
      next
    end
```

Variable	Description	Default
<policy_name>	Type the name of the policy. The maximum length is 63 characters. To display the list of existing policies, type: `edit ?`	No default.

Variable	Description	Default
`deployment-mode {server-pool | http-content-routing | offline-protection | transparent-servers | wccp-servers}`	Specify the distribution method that FortiWeb uses when it forwards connections accepted by this policy. • `server-pool` — 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 server-pool <server-pool_name>. This option is available only if the operating mode is reverse proxy mode. • `http-content-routing` — 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. • `offline-detection` — Allows connections to pass through the FortiWeb appliance and applies an offline protection profile. Also configure server-pool <server-pool_name>. This is the only option available if operating mode is offline protection. • `transparent-servers` — Allows connections to pass through the FortiWeb appliance and applies a protection profile. Also configure server-pool <server-pool_name>. This is the only option available when the operating mode is either true transparent proxy or transparent inspection. • `wccp-servers` — FortiWeb is a Web Cache Communication Protocol (WCCP) client that receives traffic from a FortiGate configured as a WCCP server. Also configure `server-pool`. This is the only option available when the operation mode is WCCP.	No default.
`vserver <vserver_name>`	Type the name of a virtual server that provides the IP address and network interface of incoming traffic that FortiWeb routes and to which the policy applies a protection profile. The maximum length is 35 characters. To display the list of existing virtual servers, type: `edit ?` Available only if the operating mode is reverse proxy.	No default.

Variable	Description	Default
`v-zone <bridge_name>`	Type the name of the bridge that specifies the network interface of the incoming traffic that the policy applies a protection profile to. The maximum length is 15 characters. To display the list of existing bridges, type: `edit ?` Available only if the operating mode is true transparent proxy or transparent inspection.	No default.
`data-capture-port <port_int>`	Type the network interface of incoming traffic that the policy attempts to apply a profile to. The IP address is ignored. Available only if the operating mode is offline inspection.	
`prefer-current-session {enable |disable}`	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. Available only when `deployment-mode` is `http-content-routing`.	`disable`
`server-pool <server-pool_name>`	Type the name of the server pool whose members receive the connections. To display the list of existing servers, type: `edit ?` This field is applicable only if `deployment-mode` is `server-pool`, `offline-protection` or `transparent-servers`. **Caution:** 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 it and cause dropped connections.	No default.

Variable	Description	Default
allow-hosts <hosts_name>	Type the name of a protected hosts group to allow or reject connections based upon whether the `Host:` field in the HTTP header is empty or does or does not match the protected hosts group. The maximum length is 35 characters. To display the list of existing groups, type: `edit ?` If you do not select a protected hosts group, FortiWeb accepts pr blocks requests based upon other criteria in the policy or protection profile, but regardless of the `Host:` field in the HTTP header. **Note:** Unlike HTTP 1.1, HTTP 1.0 does **not** require the `Host:` 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 hosts group.	No default.
client-real-ip {enable | disable}	Enter `enable` to configure FortiWeb to use the source IP address of the client that originated the request when it connects to a back-end server on behalf of that client. By default, when the operation mode is reverse proxy, the source IP for connections between FortiWeb and back-end servers is the address of a FortiWeb network interface. **Note:** To ensure FortiWeb receives the server's response, configure FortiWeb as the server's gateway. Available only if the operating mode is reverse proxy.	`disable`
block-port <port_int>	Type the number of the physical network interface port that FortiWeb uses to send TCP `RST` (reset) packets when a request violates the policy. The valid range varies by the number of physical ports on the NIC. For example, to send TCP `RST` from `port1`, type: `set block-port port1` Available only when the operating mode is offline protection.	No default.

Variable	Description	Default
`syncookie {enable | disable}`	Enable to detect TCP `SYN` flood attacks. For more information, see the *FortiWeb Administration Guide*. Available only when the operating mode is reverse proxy or true transparent proxy.	`disable`
`half-open-threshold <packets_int>`	Enter the maximum number of TCP `SYN` packets, including retransmission, that FortiWeb allows to be sent per second to a destination address. If this threshold is exceeded, the FortiWeb appliance treats the traffic as a DoS attack and ignores additional traffic from that source address. The valid range is from 10 to 10,000 packets. Available only when the operating mode is reverse proxy or true transparent proxy and `syncookie` is enabled.	`8192`
`service <service_name>`	Type the custom or predefined service that defines the port number on which the virtual server receives HTTP traffic. The maximum length is 35 characters. To display the list of existing services, type: `edit ?` Available only when the operating mode is reverse proxy.	No default.
`https-service <service_name>`	Type the custom or predefined service that defines the port number on which the virtual server receives HTTPS traffic. The maximum length is 35 characters. To display the list of existing services, type: `edit ?` Available only when the operating mode is reverse proxy. (For other operation modes, use the server pool configuration to enable SSL inspection instead.)	No default.

Variable	Description	Default
`hsts-header {enable | disable}`	Enable to combat MITM attacks on HTTP by injecting the RFC 6797 strict transport security header into the reply, such as: `Strict-Transport-Security: max-age=31536000; includeSubDomains` 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. Available only if https-service <service_name> is configured.	`disable`
`hsts-max-age <timeout_int>`	Type the time to live in seconds for the HSTS header. Available only if hsts-header {enable | disable} is enabled. The valid range is from 3600 to 31,536,000.	`7776000`
`certificate <certificate_name>`	Type the name of the certificate that FortiWeb uses to encrypt or decrypt SSL-secured connections. The maximum length is 35 characters. To display the list of existing certificates, type: `edit ?` If `sni` is `enable`, FortiWeb uses a Server Name Indication (SNI) configuration instead of or in addition to this server certificate. For more information, see sni {enable | disable}. This option is used only if https-service <service_name> is configured.	No default.
`intermediate-certificate-group <CA-group_name>`	Type the name of an intermediate certificate authority (CA) group, if any, that FortiWeb uses to validate the CA signing chain in a client's certificate. The maximum length is 35 characters. To display the list of existing groups, type: `edit ?` Available only if https-service <service_name> is configured.	No default.

Variable	Description	Default
`ssl-client-verify <verifier_name>`	Type the name of a certificate verifier, if any, to use when an HTTP client presents their personal certificate. (If you do not select one, the client is not required to present a personal certificate.) If the client presents an invalid certificate, the FortiWeb appliance does not allow the connection. To be valid, a client certificate must: • Not be expired • Not be revoked by either the certificate revocation list (CRL) (see `config system certificate verify`) • Be signed by a certificate authority (CA) whose certificate you have imported into the FortiWeb appliance (see the *FortiWeb Administration Guide*); if the certificate has been signed by a chain of intermediate CAs, those certificates must be included in an intermediate CA group (see intermediate-certificate-group <CA-group_name>) • Contain a `CA` field whose value matches the CA certificate • Contain an `Issuer` field whose value matches the `Subject` field in the CA certificate Personal certificates, sometimes also called user certificates, establish the identity of the person connecting to the web site. You can require that clients present a certificate alternatively or in addition to HTTP authentication. For more information, see the *FortiWeb Administration Guide*. The maximum length is 35 characters. To display the list of existing verifiers, type: `edit ?` This option is used only if https-service <service_name> is configured. The client must support SSL 3.0, TLS 1.0, TLS 1.1, or TLS 1.2.	No default.

Variable	Description	Default
	Note: If the connection fails when you have selected a certificate verifier, verify that the certificate meets the web browser's requirements. Web browsers may have their own certificate validation requirements in addition to FortiWeb requirements. For example, personal certificates for client authentication may be required to either: • not be restricted in usage/purpose by the CA, or • contain a `Key Usage` field that contains `Digital Signature` or have a `ExtendedKeyUsage` or `EnhancedKeyUsage` field whose value contains `Client Authentication` If the certificate does **not** satisfy browser requirements, although it may be installed in the browser, when the FortiWeb appliance requests the client's certificate, the browser may not display a certificate selection dialog to the user, or the dialog may not contain that certificate. In that case, verification fails. For browser requirements, see your web browser's documentation.	
`urlcert {enable | disable}`	Specifies whether FortiWeb uses a URL-based client certificate group to determine whether a client is required to present a personal certificate. Available only if https-service <service_name> is configured.	`disable`
`urlcert-group <urlcert-group_name>`	Specifies the URL-based client certificate group that determines whether a client is required to present a personal certificate. If the URL the client requests does not match an entry in the group, the client is not required to present a personal certificate. For information on creating a group, see `config system certificate urlcert`.	No default.
`urlcert-hlen`	Specifies the maximum allowed length for an HTTP request with a URL that matches an entry in the URL-based client certificate group, in kilobytes. FortiWeb blocks any matching requests that exceed the specified size. This setting prevents a request from exceeding the maximum buffer size. Valid values are from 16 to 128.	No default.

Variable	Description	Default
`client-certificate-forwarding {enable | disable}`	Enable to include the X.509 personal certificate presented by the client during the SSL/TLS handshake, if any, in an `X-Client-Cert:` HTTP header when forwarding the traffic to the protected web server. 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.	`disable`
`sni {enable | disable}`	Enable to use a Server Name Indication (SNI) configuration instead of or in addition to the server certificate specified by certificate <certificate_name>. The SNI configuration enables FortiWeb to determine which certificate to present on behalf of the members of a pool based on the domain in the client request. See `config system certificate sni`. If you specify both a SNI configuration and a certificate, FortiWeb uses the certificate specified by certificate <certificate_name> when the requested domain does not match a value in the SNI configuration. If you enable sni-strict {enable | disable}, FortiWeb always ignores the value of certificate <certificate_name>. Available only if https-service <service_name> is configured.	`disable`
`sni-strict {enable | disable}`	Select to configure FortiWeb to ignore the value ofcertificate <certificate_name>when it determines which certificate to present on behalf of server pool members, even if the domain in a client request does not match a value in the specified SNI configuration.	`disable`

Variable	Description	Default
`sni-certificate <sni_name>`	Type the name of the Server Name Indication (SNI) configuration that specifies which certificate FortiWeb uses when encrypting or decrypting SSL-secured connections for a specified domain. The SNI configuration enables FortiWeb to present different certificates on behalf of the members of a pool according to the requested domain. If only one certificate is required to encrypt and decrypt traffic that this policy applies to, specify certificate <certificate_name> instead. Available only if https-service <service_name> is configured.	No default.
`server-side-sni {enable | disable}`	Specifies whether FortiWeb supports Server Name Indication (SNI) for back-end servers that it applies this policy to. Enable this feature when the operating mode is reverse proxy, end-to-end encryption is required, and the back-end web server itself requires SNI support. When the operating mode is true transparent proxy, you enable server-side SNI support using server pool configuration.	`disable`
`ssl-v3 {enable | disable}`	Specifies whether clients can connect securely to FortiWeb using the SSL 3.0 cryptographic protocol. Available only if https-service <service_name> is configured.	`enable`
`tls-v10 {enable | disable}`	Specifies whether clients can connect securely to FortiWeb using the TLS 1.0 cryptographic protocol. Available only if https-service <service_name> is configured.	`enable`
`tls-v11 {enable | disable}`	Specifies whether clients can connect securely to FortiWeb using the TLS 1.1 cryptographic protocol. Available only if https-service <service_name> is configured.	`enable`

Variable	Description	Default
`tls-v12 {enable | disable}`	Specifies whether clients can connect securely to FortiWeb using the TLS 1.2 cryptographic protocol. Available only if https-service <service_name> is configured.	`enable`
`ssl-pfs {enable | disable}`	Specifies whether FortiWeb generates a new public-private key pair when it establishes a secure session with a Diffie–Hellman key exchange. Perfect forward secrecy (PFS) improves security by ensuring that the key pair for a current session is unrelated to the key for any future sessions. Available only if https-service <service_name> is configured.	`disable`
`ssl-cipher {medium | high | custom}`	Specify whether the set of cipher suites that FortiWeb allows creates a medium-security, high-security, or custom configuration. If custom, also specify `ssl-custom-cipher`. For details, see “Supported cipher suites & protocol versions” in the *FortiWeb Administration Guide*. Available only if https-service <service_name> is configured.	`medium`

Variable	Description	Default

`ssl-custom-cipher {<cipher_1> <cipher2> <cipher3> ...}`	Specify one or more cipher suites that FortiWeb allows.
	Separate the name of each cipher with a space. To remove from or add to the list of ciphers, retype the entire list.
	Valid values are:
	`ECDHE-RSA-AES256-GCM-SHA384`
	`ECDHE-ECDSA-AES256-GCM-SHA384`
	`ECDHE-RSA-AES256-SHA384`
	`ECDHE-ECDSA-AES256-SHA384`
	`ECDHE-RSA-AES256-SHA`
	`ECDHE-ECDSA-AES256-SHA`
	`DHE-DSS-AES256-GCM-SHA384`
	`DHE-RSA-AES256-GCM-SHA384`
	`DHE-RSA-AES256-SHA256`
	`DHE-DSS-AES256-SHA256`
	`DHE-RSA-AES256-SHA`
	`DHE-DSS-AES256-SHA`
	`DHE-RSA-CAMELLIA256-SHA`
	`DHE-DSS-CAMELLIA256-SHA`
	`ECDH-RSA-AES256-GCM-SHA384`
	`ECDH-ECDSA-AES256-GCM-SHA384`
	`ECDH-RSA-AES256-SHA384`
	`ECDH-ECDSA-AES256-SHA384`
	`ECDH-RSA-AES256-SHA`
	`ECDH-ECDSA-AES256-SHA`
	`AES256-GCM-SHA384`
	`AES256-SHA256`
	`AES256-SHA`
	`CAMELLIA256-SHA`
	`ECDHE-RSA-DES-CBC3-SHA`
	`ECDHE-ECDSA-DES-CBC3-SHA`
	`EDH-RSA-DES-CBC3-SHA`
	`EDH-DSS-DES-CBC3-SHA`
	`ECDH-RSA-DES-CBC3-SHA`
	`ECDH-ECDSA-DES-CBC3-SHA`
	`DES-CBC3-SHA`
	`ECDHE-RSA-AES128-GCM-SHA256`
	`ECDHE-ECDSA-AES128-GCM-SHA256`
	`ECDHE-RSA-AES128-SHA256`
	`ECDHE-ECDSA-AES128-SHA256`
	`ECDHE-RSA-AES128-SHA`
	`ECDHE-ECDSA-AES128-SHA`
	`DHE-DSS-AES128-GCM-SHA256`
	`DHE-RSA-AES128-GCM-SHA256`
	`DHE-RSA-AES128-SHA256`
	`DHE-DSS-AES128-SHA256`
	`DHE-RSA-AES128-SHA`
	`(continues)`
		`DHE-RSA-SEED-SHA DHE-DSS-SEED-SHA SEED-SHA ECDHE-RSA-RC4-SHA ECDHE-ECDSA-RC4-SHA ECDH-RSA-RC4-SHA ECDH-ECDSA-RC4-SHA RC4-SHA RC4-MD5`

Variable	Description	Default
	DHE-DSS-AES128-SHA DHE-RSA-CAMELLIA128-SHA DHE-DSS-CAMELLIA128-SHA ECDH-RSA-AES128-GCM-SHA256 ECDH-ECDSA-AES128-GCM-SHA256 ECDH-RSA-AES128-SHA256 ECDH-ECDSA-AES128-SHA256 ECDH-RSA-AES128-SHA ECDH-ECDSA-AES128-SHA AES128-GCM-SHA256 AES128-SHA256 AES128-SHA CAMELLIA128-SHA DHE-RSA-SEED-SHA DHE-DSS-SEED-SHA SEED-SHA ECDHE-RSA-RC4-SHA ECDHE-ECDSA-RC4-SHA ECDH-RSA-RC4-SHA ECDH-ECDSA-RC4-SHA RC4-SHA RC4-MD5	
`ssl-rc4-first {enable | disable}`	Specifies whether FortiWeb uses the RC4 cipher when it first attempts to create a secure connection with a client. This option protects against a BEAST (Browser Exploit Against SSL/TLS) attack, a TLS 1.0 vulnerability. Enable only when tls-v10 {enable | disable} is enabled and ssl-cipher {medium | high | custom} is `medium`. Available only if https-service <service_name> is configured.	`enable`
`ssl-chacha-cipher {enable | disable}`	Specifies whether this policy supports the ChaCha-Poly1305 cipher suite.	`disable`
`ssl-noreg {enable | disable}`	Specifies whether FortiWeb ignores requests from clients to renegotiate TLS or SSL. Protects against denial-of-service (DoS) attacks that use TLS/SSL renegotiation to overburden the server. Available only if https-service <service_name> is configured.	`enable`

Variable	Description	Default
`http-to-https {enable | disable}`	Specify enable to automatically redirect all HTTP requests to the HTTPS service with the same URL and parameters. Also configure https-service and ensure service uses port 443 (the default). FortiWeb does not apply the protection profile for this policy (specified by `web-protection-profile`) to the redirected traffic. Available only when the operation mode is reverse proxy.	`disable`
`web-protection-profile <profile_name>`	Type the name of the web protection or detection profile to apply to connections that this policy accepts. The maximum length is 35 characters. To display the list of existing profiles, type: `edit ?`	No default.
`waf-autolearning-profile <profile_name>`	Type the name of the auto-learning profile, if any, to use to discover attacks, URLs, and parameters in your web servers' HTTP sessions. The maximum length is 35 characters. To display the list of existing profiles, type: `edit ?` You can view data gathered using an auto-learning profile in an auto-learning report and use it to generate inline or offline protection profiles. For details, see the *FortiWeb Administration Guide*. This option appears only if `deployment-mode` is `offline-detection`.	No default.
`case-sensitive {enable | disable}`	Enable to differentiate uniform resource locators (URLs) according to upper case and lower case letters for features that act upon the URLs in the headers of HTTP requests, such as start page rules, black list rules, white list rules, and page access rules. For example, when enabled, an HTTP request involving `http://www.`**`E`**`xample.com/` would **not** match protection profile features that specify `http://www.`**`e`**`xample.com` (difference highlighted in bold).	No default.

Variable	Description	Default
`comment "<comment_str>"`	Type a description or other comment. If the comment is more than one word or contains special characters, surround the comment with double quotes ("). The maximum length is 999 characters.	No default.
`status {enable | disable}`	Enable to allow the policy to be used when evaluating traffic for a matching policy. **Note:** You can use SNMP traps to notify you of changes to the policy's status. For details, see `config system snmp community`.	No default.
`monitor-mode {enable | disable}`	Enable to override deny and redirect actions defined in the server protection rules for the selected policy. This setting enables FortiWeb to log attacks without performing the deny or redirect action, and to collect more information to build an auto learning profile for the attack. Disable to allow FortiWeb to perform attack deny/redirect actions as defined by the server protection rules.	`disable`
`noparse {enable | disable}`	Enable this option to apply the server policy as a pure proxy, without parsing the content. In this case, the policy allows all traffic to pass through the FortiWeb appliance without applying any protection rules. See also `diagnose debug application http` and `diagnose debug flow trace`. This option applies to server policy only when the FortiWeb appliance operates in reverse proxy or true transparent proxy mode. **Caution:** Use this only during debugging and for as brief a period as possible. This feature disables many protection features. See also http-parse-error-output {enable | disable} in `config log attack-log`.	`disable`

Variable	Description	Default
`http-pipeline {enable | disable}`	Specifies whether FortiWeb accelerates 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. When FortiWeb is operating in reverse proxy or true transparent proxy mode, it can automatically use HTTP pipelining for requests with the following characteristics: • HTTP version is 1.1 • The Connection general-header field does not include the "close" option (for example, `Connection: close`) • The HTTP method is `GET` or `HEAD`	`enable`
`sessioncookie-enforce {enable | disable}`	• `enable` — When FortiWeb maintains session persistence using cookies, it inserts a cookie in subsequent transactions in a session if the transaction does not contain a control cookie. This option is useful if your environment uses TCP multiplexing, which combines HTTP requests from multiple clients in a single session for load balancing or other purposes. • `disable` — When FortiWeb maintains session persistence using cookies, it tracks or inserts the cookie for the first transaction of a session only. It does not track or insert a cookie in subsequent transactions in the session, even if the transaction does not contain a control cookie. For more information on configuring session persistence, see `config server-policy persistence-policy`.	`disable`
`<entry_index>`	Type the index number of the individual entry in the table.	No default.
`content-routing-policy-name <content-routing_name>`	Type the name of a HTTP content routing policy that this server policy uses. To display the list of existing error pages, type: `edit ?`	No default.
`profile-inherit {enable | disable}`	Enter `enable` to specify that FortiWeb applies the web protection profile for the server policy to connections that match the routing policy.	`disable`

Variable	Description	Default
`is-default {yes | no}`	Type `yes` to specify that FortiWeb applies the protection profile to any traffic that does not match conditions specified in the HTTP content routing policies.	No default.

Example

This example configures a web protection server policy. FortiWeb forwards HTTPS connections received by the virtual server named `virtual_ip1` to a server pool named `apache1`, which contains a single physical server. FortiWeb uses the certificate named `certificate1` during SSL negotiations with the client, then forwards traffic to the server pool.

```
config server-policy policy
   edit "https-policy"
      set deployment-mode server-pool
      set vserver virtual_ip1
      set server-pool apache1
      set web-protection-profile inline-protection1
      set https-service HTTPS
      set certificate certificate1
      set ssl-client-verify
      set case-sensitive disable
      set status enable
   next
end
```

Related topics

- config server-policy allow-hosts
- config system certificate local
- config server-policy http-content-routing-policy
- config server-policy server-pool
- config server-policy service custom
- config server-policy vserver
- config system snmp community
- config system settings
- config system v-zone
- config waf web-protection-profile autolearning-profile
- config waf web-protection-profile inline-protection
- config waf web-protection-profile offline-protection
- diagnose debug application dssl
- diagnose debug application http
- diagnose debug application ssl
- diagnose debug application ustack
- diagnose debug flow filter
- diagnose policy

server-policy server-pool

Use this command to configure server pools.

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 either of the transparent modes do not.)

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 `config server-policy policy` and `config server-policy http-content-routing-policy`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see Permissions on page 74.

Syntax

```
config server-policy server-pool
   edit <server-pool_name>
      set type {offline-protection | reverse-proxy | transparent-servers-for-
          ti | transparent-servers-for-tp | transparent-servers-for-wccp}
      set server-balance {enable | disable}
      set health <health-check_name>
      set lb-algo {least-connections | round-robin | weighted-round-robin | uri-
          hash | full-uri-hash | host-hash | host-domain-hash | src-ip-hash}
      set persistence <persistence-policy_name>
      set comment "<comment_str>"
      config pserver-list
         edit <entry_index>
            set status {disable |enable | maintain}
            set analyzer-policy <fortianalyzer-policy_name>
            set ip {address_ipv4 |address_ipv6}
            set domain <server_fqdn>
            set port <port_int>
            set conn-limit <conn-limit_int>
            set weight <weight_int>
            set health-check-inherit {enable | disable}
            set health <health-check_name>
            set backup-server {enable | disable}
            set ssl {enable | disable}
            set certificate <certificate_name>
            set intermediate-certificate-group <CA-group_name>
            set client-certificate <client-certificate_name>
            set hsts-header {enable | disable}
            set hsts-max-age <timeout_int>
            set certificate-verify <verifier_name>
            set url-cert {enable | disable}
            set urlcert-group <urlcert-group_name>
            set urlcert-hlen
            set sni {enable | disable}
            set sni-strict {enable | disable}
```

```
            set sni-certificate <sni_name>
            set ssl-v3 {enable | disable}
            set tls-v10 {enable | disable}
            set tls-v11 {enable | disable}
            set tls-v12 {enable | disable}
            set ssl-cipher {medium | high | custom}
            set ssl-custom-cipher {<cipher_1> <cipher2> <cipher3> ...}
            set ssl-pfs {enable | disable}
            set ssl-rc4-first {enable | disable}
            set ssl-chacha-cipher {enable | disable}
            set ssl-noreg {enable | disable}
            set server-side-sni {enable | disable}
            set recover <recover_int>
            set  warm-up <warm-up_int>
            set  warm-rate <warm-rate_int>
          next
        end
      next
    end
```

Variable	Description	Default
`<server-pool_name>`	Type the name of the server farm. The maximum length is 63 characters. To display the list of existing servers, type: `edit ?`	No default.
`type {offline-protection | reverse-proxy | transparent-servers-for-ti | transparent-servers-for-tp | transparent-servers-for-wccp}`	Select the current operation mode of the appliance to display the corresponding pool options. For full information on the operating modes, see “How to choose the operation mode” on page 69. For details, see opmode {offline-protection | reverse-proxy | transparent | transparent-inspection | wccp} in `config system settings`.	`reverse-proxy`
`server-balance {enable | disable}`	Specifies whether the pool contains a single server or multiple members. If the value is `enabled`, 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. Available only when `type` is `reverse-proxy`.	`disable`

Variable	Description	Default
	Type the name of a server health check FortiWeb uses to determine the responsiveness of server pool members. The maximum length is 35 characters. When you specify a health check for the pool, by default, all pool members use that health check. To select a different health check for a pool member, in the pool member configuration, specify `disable` for `health-check-inherit` and the health check to use for `health`. To display the list of existing health checks, type: `edit ?`	
`health <health-check_name>`	Available only if `type` is `reverse-proxy` and `server-balance` is enable. **Note:** If a pool member is unresponsive, wait until the server becomes responsive again before disabling its server health check. Server health checks record the up or down status of the server. If you deactivate the server health check while the server is unresponsive, the server health check cannot update the recorded status, and FortiWeb continues to regard the physical server as if it were unresponsive. You can determine the physical server's connectivity status using the **Service Status** widget (see the *FortiWeb Administration Guide*) or an SNMP trap (see `config system snmp community`).	No default.
`backup-server {enable | disable}`	Enter `enable` to configure this pool member as a backup server. FortiWeb only routes connections for the pool to a backup server when all the other members of the server pool fail their server health check. The backup server mechanism does not work if you do not specify server health checks for the pool members. If you select this option for more than one pool member, FortiWeb uses the load balancing algorithm to determine which member to use.	`disable`

Variable	Description	Default
`lb-algo {least-connections | round-robin | weighted-round-robin | uri-hash | full-uri-hash | host-hash | host-domain-hash | src-ip-hash}`	Select the load-balancing algorithms that FortiWeb uses when it distributes new connections among server pool members. • `least-connections` — Distributes new connections to the member with the fewest number of existing, fully-formed connections. • `round-robin` — Distributes new connections to the next member of the server pool, regardless of weight, response time, traffic load, or number of existing connections. Unresponsive servers are avoided. • `weighted-round-robin` — Distributes new connections using the round robin method, except that members with a higher weight value receive a larger percentage of connections. • `uri-hash` — Distributes new TCP connections using a hash algorithm based on the URI found in the HTTP header, excluding hostname. • `full-uri-hash` — Distributes new TCP connections using a hash algorithm based on the full URI string found in the HTTP header. The full URI string includes the hostname and path. • `host-hash` — Distributes new TCP connections using a hash algorithm based on the hostname in the HTTP Request header Host field. • `host-domain-hash` — Distributes new TCP connections using a hash algorithm based on the domain name in the HTTP Request header Host field. • `src-ip-hash` — Distributes new TCP connections using a hash algorithm based on the source IP address of the request. For hash-based methods, if you specify a value for `persistence`, after an initial client request, FortiWeb routes any subsequent requests according to the persistence method. Otherwise, it routes subsequent requests according to the hash-based algorithm. Available only if `type` is `reverse-proxy` and `server-balance` is enable.	`round-robin`

Variable	Description	Default
`persistence <persistence-policy_ name>`	Type the name of the persistence policy that specifies a session persistence method and timeout to apply to the pool. For more information, see `config server-policy persistence-policy`.	No default.
`comment "<comment_str>"`	Type a description or other comment. If the comment is more than one word or contains special characters, surround the comment with double quotes ("). The maximum length is 199 characters.	No default.
`<entry_index>`	Type the index number of the member entry within the server pool. The valid range is from 1 to 9,223,372,036,854,775,807. For round robin-style load-balancing, the index number indicates the order in which FortiWeb distributes connections.	No default.
`status {disable |enable | maintain}`	To specify the status of the pool member, type one of the following values: • `enable` — Specifies that this pool member can receive new sessions from FortiWeb. • `disable` — Specifies that this pool member does not receive new sessions from FortiWeb and FortiWeb closes any current sessions as soon as possible. • `maintain` — Specifies that this pool member does not receive new sessions from FortiWeb but FortiWeb maintains any current connections.	`enable`
`server-type {physical | domain}`	Specify whether to specify the pool member by IP address or domain.	`physical`
`ip {address_ ipv4 |address_ipv6}`	Type the IP address of the web server to include in the pool. **Warning:** Server policies do not apply to features that do not yet support IPv6 to servers specified using IPv6 addresses. Available only if `server-type` is `physical`.	No default.

Variable	Description	Default
`domain <server_fqdn>`	Type the fully-qualified domain name of the web server to include in the pool, such as `www.example.com`. **Warning:** Server policies do not apply features that do not yet support IPv6 to domain servers whose DNS names resolve to IPv6 addresses. **Tip:** 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: • use physical servers instead • ensure highly reliable, low-latency service to a DNS server on your local network Available only if `server-type` is `domain`.	No default.
`conn-limit <conn-limit_int>`	Specifies the maximum number of TCP connections that FortiWeb forwards to this pool member. For no limit, specify `0` (the default value). The valid range is from 0 to 1,048,576.	`0`
`port <port_int>`	Type the TCP port number where the pool member listens for connections. The valid range is from 1 to 65,535.	`80`
`weight <weight_int>`	If the server pool uses the weighted round robin load-balancing algorithm, type the numerical weight of the pool member. Members with a greater weight receive a greater proportion of connections. The valid range is from 1 to 9,999.	`0`
`health-check-inherit {enable | disable}`	• `enable` — Use the health check specified by `health` in the server pool configuration. • `disable` — Use the health check specified by `health` in this pool member configuration.	enable

Variable	Description	Default
`ssl {enable | disable}`	For reverse proxy, offline protection, and transparent inspection modes, specifies whether connections between FortiWeb and the pool member use SSL/TLS. For true transparent proxy and WCCP modes, specifies whether FortiWeb performs SSL/TLS processing for the pool members and connections between FortiWeb and the pool member use SSL/TLS. For offline protection and transparent modes, also configure certificate <certificate_name>. FortiWeb uses the certificate to decrypt and scan connections before passing the encrypted traffic through to the pool members (SSL inspection). For true transparent proxy, also configure certificate <certificate_name> and additional SSL settings as required. FortiWeb handles SSL negotiations and encryption and decryption, instead of the pool member (SSL offloading). (For reverse proxy mode, you can configure SSL offloading for all members of a pool using a server policy. See `config server-policy policy`.) **Note:** When this option is enabled, the pool member must be configured to apply SSL. **Note:** Ephemeral (temporary key) Diffie-Hellman exchanges are not supported if the FortiWeb appliance is operating in transparent inspection or offline protection mode.	No default.
`certificate <certificate_name>`	Type the name of the certificate that FortiWeb uses to decrypt SSL-secured connections. Available only if `ssl` is `enable`. The maximum length is 35 characters. To display the list of existing certificates, type: `edit ?`	No default.

Variable	Description	Default
`intermediate-certificate-group <CA-group_name>`	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. If clients receive certificate warnings that the server certificate configured in certificate <certificate_name> has been signed by an intermediary CA, rather than directly by a root CA or other CA currently trusted by the client, configure this option. 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 the *FortiWeb Administration Guide*. Available only if `type` is `transparent-servers-for-tp` and `ssl` is `enable`. (For reverse proxy mode, configure this setting in the server policy instead. See intermediate-certificate-group <CA-group_name> in `config server-policy policy`.)	No default.
`client-certificate <client-certificate_name>`	Specifies the client certificate that FortiWeb uses to connect to this server pool member. Used when connections to this pool member require a valid client certificate. Available only if `type` is `reverse-proxy` or `transparent-servers-for-tp` and `ssl` is `enable`. To upload a client certificate for FortiWeb, see the *FortiWeb Administration Guide*.	`disable`

Variable	Description	Default
`hsts-header {enable | disable}`	Enable to combat MITM attacks on HTTP by injecting the RFC 6797 strict transport security header into the reply, such as: `Strict-Transport-Security: max-age=31536000; includeSubDomains` 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 a dialog that allows the user to override the certificate mismatch error and continue. Available only if `type` is `transparent-servers-for-tp` and `ssl` is `enable`.	`disable`
`hsts-max-age <timeout_int>`	Type the time to live in seconds for the HSTS header. This setting applies only if `hsts-header` is `enable`.	`7776000`

Variable	Description	Default
certificate-verify <verifier_name>	Type the name of a certificate verifier, if any, to use when an HTTP client presents their personal certificate. (If you do not specify one, the client is not required to present a personal certificate.) However, if `sni` is `enable` and the domain in the client request matches an entry in the specified SNI policy, FortiWeb uses the SNI configuration to determine which certificate verifier to use. Personal certificates, sometimes also called user certificates, establish the identity of the person connecting to the web site. For information on how the client's certificate is verified, see ssl-client-verify <verifier_name> in `config server-policy policy`. You can require that clients present a certificate alternatively or in addition to HTTP authentication (see `config waf http-authen http-authen-rule`). Available only if `type` is `transparent-servers-for-tp` and `ssl` is `enable`. (For reverse proxy mode, configure this setting in the server policy instead. See ssl-client-verify <verifier_name> in `config server-policy policy`.) The maximum length is 35 characters. To display the list of existing verifiers, type: `edit ?` **Note:** The client must support SSL 3.0, TLS 1.0, TLS 1.1, or TLS 1.2.	No default.
url-cert {enable | disable}	Specifies whether FortiWeb uses a URL-based client certificate group to determine whether a client is required to present a personal certificate. Available only if https-service <service_name> is configured.	`disable`

Variable	Description	Default
`urlcert-group <urlcert-group_name>`	Specifies the URL-based client certificate group that determines whether a client is required to present a personal certificate. If the URL the client requests does not match an entry in the group, the client is not required to present a personal certificate. For information on creating a group, see `config system certificate urlcert`.	No default.
`urlcert-hlen`	Specifies the maximum allowed length for an HTTP request with a URL that matches an entry in the URL-based client certificate group, in kilobytes. FortiWeb blocks any matching requests that exceed the specified size. This setting prevents a request from exceeding the maximum buffer size. Valid values are from 16 to 128.	No default.
`client-certificate-forwarding {enable | disable}`	Enter `enable` to configure FortiWeb to include any X.509 personal certificates presented by clients during the SSL/TLS handshake with the traffic it forwards to the pool member. Available only if `type` is `transparent-servers-for-tp` and `ssl` is `enable`.	`disable`
`sni {enable | disable}`	Enable to use a Server Name Indication (SNI) configuration instead of or in addition to the server certificate specified by certificate <certificate_name>. The SNI configuration enables FortiWeb to determine which certificate to present on behalf of the members of a pool based on the domain in the client request. See `config system certificate sni`. If you specify both a SNI configuration and a certificate, FortiWeb uses the certificate specified by certificate <certificate_name> when the requested domain does not match a value in the SNI configuration. If you enable sni-strict {enable | disable}, FortiWeb always ignores the value of certificate <certificate_name>. Available only if `type` is `transparent-servers-for-tp` and `ssl` is `enable`.	`disable`

Variable	Description	Default
`sni-strict {enable | disable}`	Select to configure FortiWeb to ignore the value of certificate <certificate_name> when it determines which certificate to present on behalf of server pool members, even if the domain in a client request does not match a value in the specified SNI configuration.	`disable`
`sni-certificate <sni_name>`	Type the name of the Server Name Indication (SNI) configuration that specifies which certificate FortiWeb uses when encrypting or decrypting SSL-secured connections for a specified domain. The SNI configuration enables FortiWeb to present different certificates on behalf of the members of a pool according to the requested domain. If only one certificate is required to encrypt and decrypt traffic that this policy applies to, specify certificate <certificate_name> instead. Available only if sni {enable | disable} is enabled.	No default.
`ssl-v3 {enable | disable}`	For reverse proxy mode, specifies whether secure connections between FortiWeb and the server pool member can use the SSL 3.0 cryptographic protocol. For true transparent proxy and WCCP modes, specifies whether secure connections between clients and FortiWeb and between FortiWeb and the server pool member can use the SSL 3.0 cryptographic protocol. Available only if `type` is `reverse-proxy`, `transparent-servers-for-tp`, or `transparent-servers-for-wccp`, and `ssl` is `enable`.	`enable`
`tls-v10 {enable | disable}`	For reverse proxy mode, specifies whether secure connections between FortiWeb and the server pool member can use the TLS 1.0 cryptographic protocol. For true transparent proxy and WCCP modes, specifies whether secure connections between clients and FortiWeb and between FortiWeb and the server pool member can use the TLS 1.0 cryptographic protocol. Available only if `type` is `reverse-proxy`, `transparent-servers-for-tp`, or `transparent-servers-for-wccp`, and `ssl` is `enable`.	`enable`

Variable	Description	Default
`tls-v11 {enable | disable}`	For reverse proxy mode, specifies whether secure connections between FortiWeb and the server pool member can use the TLS 1.1 cryptographic protocol. For true transparent proxy and WCCP modes, specifies whether secure connections between clients and FortiWeb and between FortiWeb and the server pool member can use the TLS 1.1 cryptographic protocol. Available only if `type` is `reverse-proxy`, `transparent-servers-for-tp`, or `transparent-servers-for-wccp`, and `ssl` is `enable`.	`enable`
`tls-v12 {enable | disable}`	For reverse proxy mode, specifies whether secure connections between FortiWeb and the server pool member can use the TLS 1.2 cryptographic protocol. For true transparent proxy and WCCP modes, specifies whether secure connections between clients and FortiWeb and between FortiWeb and the server pool member can use the TLS 1.2 cryptographic protocol. Available only if `type` is `reverse-proxy`, `transparent-servers-for-tp`, or `transparent-servers-for-wccp`, and `ssl` is `enable`.	`enable`
`ssl-cipher {medium | high | custom}`	For reverse proxy mode, specifies whether secure connections between FortiWeb and the server pool member use a medium-security, high-security, or custom set of cipher suites. For true transparent proxy and WCCP modes, specifies whether secure connections between clients and FortiWeb and between FortiWeb and the server pool member use a medium-security, high-security, or custom set of cipher suites. If custom, also specify `ssl-custom-cipher`. For details, see “Supported cipher suites & protocol versions” in the *FortiWeb Administration Guide*. Available only if `type` is `reverse-proxy`, `transparent-servers-for-tp`, or `transparent-servers-for-wccp`, and `ssl` is `enable`.	`medium`

Variable	Description	Default

`ssl-custom-cipher {<cipher_1> <cipher2> <cipher3> ...}`	Specify one or more cipher suites that FortiWeb allows.
	Separate the name of each cipher with a space. To remove from or add to the list of ciphers, retype the entire list.
	Valid values are:
	`ECDHE-RSA-AES256-GCM-SHA384`
	`ECDHE-ECDSA-AES256-GCM-SHA384`
	`ECDHE-RSA-AES256-SHA384`
	`ECDHE-ECDSA-AES256-SHA384`
	`ECDHE-RSA-AES256-SHA`
	`ECDHE-ECDSA-AES256-SHA`
	`DHE-DSS-AES256-GCM-SHA384`
	`DHE-RSA-AES256-GCM-SHA384`
	`DHE-RSA-AES256-SHA256`
	`DHE-DSS-AES256-SHA256`
	`DHE-RSA-AES256-SHA`
	`DHE-DSS-AES256-SHA`
	`DHE-RSA-CAMELLIA256-SHA`
	`DHE-DSS-CAMELLIA256-SHA`
	`ECDH-RSA-AES256-GCM-SHA384`
	`ECDH-ECDSA-AES256-GCM-SHA384`
	`ECDH-RSA-AES256-SHA384`
	`ECDH-ECDSA-AES256-SHA384`
	`ECDH-RSA-AES256-SHA`
	`ECDH-ECDSA-AES256-SHA`
	`AES256-GCM-SHA384`
	`AES256-SHA256`
	`AES256-SHA`
	`CAMELLIA256-SHA`
	`ECDHE-RSA-DES-CBC3-SHA`
	`ECDHE-ECDSA-DES-CBC3-SHA`
	`EDH-RSA-DES-CBC3-SHA`
	`EDH-DSS-DES-CBC3-SHA`
	`ECDH-RSA-DES-CBC3-SHA`
	`ECDH-ECDSA-DES-CBC3-SHA`
	`DES-CBC3-SHA`
	`ECDHE-RSA-AES128-GCM-SHA256`
	`ECDHE-ECDSA-AES128-GCM-SHA256`
	`ECDHE-RSA-AES128-SHA256`
	`ECDHE-ECDSA-AES128-SHA256`
	`ECDHE-RSA-AES128-SHA`
	`ECDHE-ECDSA-AES128-SHA`
	`DHE-DSS-AES128-GCM-SHA256`
	`DHE-RSA-AES128-GCM-SHA256`
	`DHE-RSA-AES128-SHA256`
	`DHE-DSS-AES128-SHA256`
	`DHE-RSA-AES128-SHA`
	`(continues)`
		`DHE-RSA-SEED-SHA DHE-DSS-SEED-SHA SEED-SHA ECDHE-RSA-RC4-SHA ECDHE-ECDSA-RC4-SHA ECDH-RSA-RC4-SHA ECDH-ECDSA-RC4-SHA RC4-SHA RC4-MD5`

Variable	Description	Default
	DHE-DSS-AES128-SHA DHE-RSA-CAMELLIA128-SHA DHE-DSS-CAMELLIA128-SHA ECDH-RSA-AES128-GCM-SHA256 ECDH-ECDSA-AES128-GCM-SHA256 ECDH-RSA-AES128-SHA256 ECDH-ECDSA-AES128-SHA256 ECDH-RSA-AES128-SHA ECDH-ECDSA-AES128-SHA AES128-GCM-SHA256 AES128-SHA256 AES128-SHA CAMELLIA128-SHA DHE-RSA-SEED-SHA DHE-DSS-SEED-SHA SEED-SHA ECDHE-RSA-RC4-SHA ECDHE-ECDSA-RC4-SHA ECDH-RSA-RC4-SHA ECDH-ECDSA-RC4-SHA RC4-SHA RC4-MD5	
`ssl-pfs {enable | disable}`	Enable to configure FortiWeb to generate a new public-private key pair when it establishes a secure session with a Diffie–Hellman key exchange. Perfect forward secrecy (PFS) improves security by ensuring that the key pair for a current session is unrelated to the key for any future sessions. Available only if `type` is `transparent-servers-for-tp` and `ssl` is `enable`.	`disable`
`ssl-rc4-first {enable | disable}`	Enable to configure FortiWeb to use the RC4 cipher when it first attempts to create a secure connection with a client. This option protects against a BEAST (Browser Exploit Against SSL/TLS) attack, a TLS 1.0 vulnerability. Enable only when tls-v10 {enable | disable} is `enabled` and ssl-cipher {medium | high | custom} is `medium`.	`enable`
`ssl-chacha-cipher {enable | disable}`	Specifies whether this pool member supports the ChaCha-Poly1305 cipher suite.	`disable`

Variable	Description	Default
`ssl-noreg {enable | disable}`	Select to configure FortiWeb to ignore requests from clients to renegotiate TLS or SSL. Protects against denial-of-service (DoS) attacks that use TLS/SSL renegotiation to overburden the server. Available only if `type` is `transparent-servers-for-tp` and `ssl` is `enable`.	`enable`
`server-side-sni {enable | disable}`	Specifies whether FortiWeb supports Server Name Indication (SNI) for back-end servers that it applies this policy to. Enable this feature when the operating mode is transparent proxy, end-to-end encryption is required, and the back-end web server itself requires SNI support. When the operating mode is reverse proxy, you enable server-side SNI support using the server policy.	`disable`
`recover <recover_int>`	Specifies the number of seconds that FortiWeb waits before it forwards traffic to this pool member after a health check indicates that this server is available again. The default is `0` (disabled). The valid range is 0 to 86,400 seconds. After the recovery period elapses, FortiWeb assigns connections at the rate specified by `warm-rate`. Examples of when the server experiences a recovery and warm-up period: • A server is coming back online after the health check monitor detected it was down. • A network service is brought up before other daemons have finished initializing and therefore the server is using more CPU and memory resources than when startup is complete. To avoid connection problems, specify the separate warm-up rate, recovery rate, or both. **Tip:** During scheduled maintenance, you can also manually apply these limits by setting `status` to `maintain`.	`0`

Variable	Description	Default
`warm-up <warm-up_int>`	Specifies for how long FortiWeb forwards traffic at a reduced rate after a health check indicates that this pool member is available again but it cannot yet handle a full connection load. For example, when the pool member begins to respond but startup is not fully complete. The default is `0` (disabled). The valid range is 0 to 86,400 seconds.	`0`
`warm-rate <warm-rate_int>`	Specifies the maximum connection rate while the pool member is starting up. The default is 10 connections per second. The valid range is 1 to 86,400 connections per second. The warm up calibration is useful with servers that bring up the network service before other daemons are initialized. As these types of servers come online, CPU and memory are more utilized than they are during normal operation. For these servers, you define separate rates based on warm-up and recovery behavior. For example, if `warm-up` is `5` and `warm-rate` is `2`, the maximum number of new connections increases at the following rate: • 1st second — Total of 2 new connections allowed (0+2). • 2nd second — 2 new connections added for a total of 4 new connections allowed (2+2). • 3rd second — 2 new connections added for a total of 6 new connections allowed (4+2). • 4th second — 2 new connections added for a total of 8 new connections allowed (6+2). • 5th second — 2 new connections added for a total of 10 new connections allowed (8+2).	`10`

Example

This example configures a server pool named `server-pool1`. It consists of two physical servers: `172.16.1.10` and `172.16.1.11`.

When both servers are available, FortiWeb forwards connections to the server with the smallest number of connections.

```
config server-policy server-pool
   edit "server-pool1"
      set type reverse-proxy
```

```
      set server-balance enable
      set lb-algo least-connections
      config pserver-list
         edit 1
            set status enable
            set server-type physical
            set ip 172.16.1.10
            set ssl disable
            set port 8081
         next
         edit 2
            set status enable
            set server-type physical
            set ip 172.16.1.11
            set ssl disable
            set port 8082
         next
      end
   next
end
```

Related topics

- config server-policy policy
- config server-policy http-content-routing-policy
- config system certificate local
- config server-policy health
- config server-policy persistence-policy

server-policy service custom

Use this command to configure a custom service.

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

To use this command, your administrator account's access control profile must have either w or rw permission to the traroutegrp area. For more information, see Permissions on page 74.

Syntax

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

Variable	Description	Default
<service_name>	Type the name of the new or existing custom network service, such as SOAP1. The maximum length is 63 characters. To display the list of existing services, type: edit ?	No default.
port <port_int>	Type the port number on which a virtual server will receive TCP/IP connections for HTTP or HTTPS requests. The valid range is from 1 to 65,535.	No default.

Example

This example configures a service definition named SOAP1.

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

Related topics

- config server-policy vserver
- config server-policy policy
- config server-policy custom-application application-policy

server-policy service predefined

Use this command to view a predefined service.

This command only displays predefined services. It **cannot** be used to modify them. If you attempt to edit the port number and protocol, the appliance will discard your settings.

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

To use this command, your administrator account's access control profile must have either w or rw permission to the traroutegrp area. For more information, see Permissions on page 74.

Syntax

```
config server-policy service predefined
   edit analyzer-policy <fortianalyzer-policy_name>
```

```
      show
   next
end
```

Variable	Description	Default
<service_name>	Type the name of a predefined network service, such as HTTP or HTTPS. The maximum length is 35 characters. To display the list of existing services, type: edit ?	No default.

Example

This example shows the default settings for all of the predefined services.

```
config server-policy service predefined
   show
```

Output:

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

Related topics

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

server-policy vserver

Use this command to configure virtual servers.

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

When the FortiWeb appliance receives traffic destined for a virtual server, it can then forward the traffic to a physical server or a server farm. 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 with the physical server's IP address)

Virtual servers can be on the same subnet as physical servers. This configuration creates a one-arm HTTP proxy. For example, the virtual server 10.0.0.1/24 could forward to the physical server 10.0.0.2.

However, this is **not** recommended. Unless your network's routing configuration prevents it, it could allow attackers that are aware of the physical server's IP address to bypass FortiWeb by accessing the physical server directly.

To apply virtual servers, select them within a server policy. For details, see `config server-policy policy`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For more information, see Permissions on page 74.

Syntax

```
config server-policy vserver
   edit <virtual-server_name>
      set status {enable | disable}
      set interface <interface_name>
      set vip <virtual-ip_ipv4mask>
      [set vip6 <virtual-ip_ipv6mask>]
      set use-interface-ip {enable | disable}
   next
end
```

Variable	Description	Default
`<virtual-server_name>`	Type the name of the new or existing virtual server. The maximum length is 63 characters. To display the list of existing servers, type: `edit ?`	`disable`
`status {enable | disable}`	Enable to accept traffic destined for this virtual server.	No default.
`interface <interface_ name>`	Type the name of the network interface or bridge, such as `port1` or `bridge1`, to which the virtual server is bound, and on which traffic destined for the virtual server will arrive. The maximum length is 35 characters. To display the list of existing interfaces, type: `edit ?`	No default.

Variable	Description	Default
`vip <virtual-ip_ipv4mask>`	Type the IPv4 address and subnet of the virtual server.	`0.0.0.0 0.0.0.0`
`vip6 <virtual-ip_ipv6mask>`	Type the IPv6 address and subnet of the virtual server.	`::/0`
`use-interface-ip {enable | disable}`	For FortiWeb-VM on Microsoft Azure, specify whether the virtual server uses the IP address of the specified interface, instead of an IP specified by `vip` or `vip6`.	`disable`

Example

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

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

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

Related topics

- `config system interface`
- `config server-policy policy`
- `config server-policy service custom`
- `execute ping`
- `diagnose network ip`

system accprofile

Use this command to configure access control profiles for administrators.

If you have configured RADIUS queries for authenticating administrators, you can override the locally-selected access profile by using a RADIUS VSA. See `config system admin`.

Access profiles 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 a person 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.

For information on how each access control area correlates to which CLI commands that administrators can access, see Permissions on page 74

To use this command, your administrator account's access control profile must have both `r` and `w` permissions to items in the `admingrp` category.

Syntax

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

Variable	Description	Default
<access-profile_name>	Type the name of the access profile. The maximum length is 35 characters. To display the list of existing profiles, type: `edit ?`	No default.
`admingrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the system administrator configuration. Available only when administrative domains (ADOMs) are disabled. See adom-admin {enable | disable} in `config system global`.	`none`
`authusergrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the HTTP authentication user configuration.	`none`
`learngrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the auto-learning profiles and their resulting auto-learning reports.	`none`
`loggrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the logging and alert email configuration.	`none`
`mntgrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to maintenance commands. Unlike the other rows, whose scope is an area of the configuration, the maintenance access control area does not affect the configuration. Instead, it indicates whether the administrator can perform special system operations such as changing the firmware.	`none`
`netgrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the network interface and routing configuration.	`none`
`sysgrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the basic system configuration (except for areas included in other access control areas such as `admingrp`).	`none`
`traroutegrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the server policy (formerly called traffic routing) configuration.	`none`

Variable	Description	Default
`wadgrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the web anti-defacement configuration.	`none`
`webgrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the web protection profile configuration.	`none`
`wvsgrp {none | r | rw | w}`	Type the degree of access that administrator accounts using this access profile will have to the web vulnerability scanner.	`none`

Example

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

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

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

Related topics

- `config system admin`
- `config server-policy custom-application application-policy`
- Permissions

system admin

Use this command to configure FortiWeb administrator accounts. In its factory default configuration, a FortiWeb appliance has one administrator account, named `admin`. That administrator has permissions that grant full access to the FortiWeb configuration and firmware. After connecting to the web UI or the CLI using the `admin` administrator account, you can configure additional administrator accounts with various levels of access to different parts of the FortiWeb configuration.

Administrators can access the web UI and the CLI through the network, depending on administrator account's trusted hosts, ADOMs, and the administrative access protocols enabled for each of the FortiWeb appliance's network interfaces. For details, see `config system interface`, `config system global`, and Connecting to the CLI on page 61.

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

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see Permissions on page 74.

Syntax

```
config system admin
   edit <administrator_name>
      set accprofile <access-profile_name>
      set accprofile-override {enable | disable}
      set domains <adom_name>
      set password <password_str>
      set email-address <contact_email>
      set first-name <name_str>
      set last-name <surname_str>
      set mobile-number <cell-phone_str>
      set phone-number <phone_str>
      set trusthost1 <management-computer_ipv4mask>
      set trusthost2 <management-computer_ipv4mask>
      set trusthost3 <management-computer_ipv4mask>
      set ip6trusthost1 <management-computer_ipv6mask>
      set ip6trusthost2 <management-computer_ipv6mask>
      set ip6trusthost3 <management-computer_ipv6mask>
      set type {local-user | remote-user}
      set admin-usergroup <remote-auth-group_name>
      set wildcard {enable | disable}
      set sshkey <sshkey_str>
   next
end
```

Variable	Description	Default
<administrator_name>	Type the name of the administrator account, such as admin1 or admin@example.com, that can be referenced in other parts of the configuration. Do not use spaces or special characters except the 'at' symbol (@). The maximum length is 35 characters. To display the list of existing accounts, type: edit ? **Note:** 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.	No default.
accprofile <access-profile_name>	Type the name of an access profile that gives the permissions for this administrator account. See also config system accprofile. The maximum length is 35 characters. You can select **prof_admin**, a special access profile used by the admin administrator account. However, selecting this access profile will **not** confer all of the same permissions of the admin administrator. For example, the new administrator would not be able to reset lost administrator passwords. To display the list of existing profiles, type: edit ? **Tip:** Alternatively, if your administrator accounts authenticate via a RADIUS query, you can assign their access profile through the RADIUS server using RFC 2548 Microsoft Vendor-specific RADIUS Attributes. On the RADIUS server, create an attribute named: ATTRIBUTE FortiWeb-Access-Profile 7 then set its value to be the name of the access profile that you want to assign to this account. Finally, in the CLI, use accprofile-override {enable | disable} to enable the override. 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.	No default.

Variable	Description	Default
`accprofile-override {enable | disable}`	Enable to use the access profile indicated by the RADIUS query response, and ignore accprofile <access-profile_name>. This setting applies only if admin-usergroup <remote-auth-group_name> is configured to use a RADIUS query to authenticate this account. This setting applies only if ADOMs are enabled. See adom-admin {enable | disable} in `config system global`.	`disable`
`domains <adom_name>`	Type the name of an administrative domain (ADOM) to assign and restrict this administrative account to it. This setting applies only if ADOMs are enabled. See adom-admin {enable | disable} in `config system global`.	No default.
`password <password_str>`	Type a password for the administrator account. The maximum length is 32 characters. The minimum length is 1 character. For improved security, the password should be at least 8 characters long, be sufficiently complex, and be changed regularly. This setting applies only when `type` is `local-user`. For accounts defined on a remote authentication server, the FortiWeb appliance will instead query the server to verify whether the password given during a login attempt matches the account's definition.	No default.
`email-address <contact_email>`	Type an email address that can be used to contact this administrator. The maximum length is 35 characters.	No default.
`first-name <name_str>`	Type the first name of the administrator. The maximum length is 35 characters.	No default.
`last-name <surname_str>`	Type the surname of the administrator. The maximum length is 35 characters.	No default.
`mobile-number <cell-phone_str>`	Type a cell phone number that can be used to contact this administrator. The maximum length is 35 characters.	No default.
`phone-number <phone_str>`	Type a phone number that can be used to contact this administrator. The maximum length is 35 characters.	No default.

Variable	Description	Default
`trusthost1 <management-computer_ipv4mask>`	Type the IP address and netmask of a management computer or management LAN from which the administrator is allowed to log in to the FortiWeb appliance. You can specify up to three trusted hosts. To allow login attempts from any IP address, enter `0.0.0.0/0.0.0.0`. If you allow administrators to log in from any IP address, consider choosing a longer and more complex password, and limiting administrative access to secure protocols to minimize the security risk. For information on administrative access protocols, see `config system interface`. **Note:** For improved security, restrict all three trusted host addresses to the IP addresses of computers from which only this administrator will log in.	`0.0.0.0` `0.0.0.0`
`trusthost2 <management-computer_ipv4mask>`	Type a second IP address and netmask of a management computer or management LAN from which the administrator is allowed to log in to the FortiWeb appliance. To allow login attempts from any IP address, enter `0.0.0.0/0.0.0.0`.	`0.0.0.0` `0.0.0.0`
`trusthost3 <management-computer_ipv4mask>`	Type a third IP address and netmask of a management computer or management LAN from which the administrator is allowed to log in to the FortiWeb appliance. To allow login attempts from any IP address, enter `0.0.0.0/0.0.0.0`.	`0.0.0.0` `0.0.0.0`

Variable	Description	Default
ip6trusthost1 <management-computer_ipv6mask>	Type the IP address and netmask of a management computer or management LAN from which the administrator is allowed to log in to the FortiWeb appliance. You can specify up to three trusted hosts. To allow login attempts from any IP address, enter `::/0`. **Caution:** If you allow logins from any IP address, consider choosing a longer and more complex password, and limiting administrative access to secure protocols to minimize the security risk. Unlike IPv4, IPv6 does **not** isolate public from private networks via NAT, and therefore can increase availability of your FortiWeb's web UI/CLI to IPv6 attackers unless you have carefully configured your firewall/FortiGate and routers. For information on administrative access protocols, see `config system interface`. **Note:** For improved security, restrict all three trusted host addresses to the IP addresses of computers from which only this administrator will log in.	`::/0`
ip6trusthost2 <management-computer_ipv6mask>	Type a second IP address and netmask of a management computer or management LAN from which the administrator is allowed to log in to the FortiWeb appliance. To allow login attempts from any IP address, enter `::/0`.	`::/0`
ip6trusthost3 <management-computer_ipv6mask>	Type a third IP address and netmask of a management computer or management LAN from which the administrator is allowed to log in to the FortiWeb appliance. To allow login attempts from any IP address, enter `::/0`.	`::/0`
type {local-user | remote-user}	Select either: • `local-user` — Authenticate this account locally, with the FortiWeb appliance itself. • `remote-user` — Authenticate this account via a remote server such as an LDAP or RADIUS server. Also configure admin-usergroup <remote-auth-group_name>.	No default.

Variable	Description	Default
`admin-usergroup <remote-auth-group_name>`	Type the name of the remote authentication group whose settings the FortiWeb appliance will use to connect to a remote authentication server when authenticating login attempts for this account. The maximum length is 35 characters. To display the list of existing groups, type: `edit ?` For details on configuring remote authentication groups, see `config user admin-usergrp`.	No default.
`wildcard {enable | disable}`	Used when administrator accounts authenticate via a RADIUS query. This setting applies only if the value of `type` is `remote-user`.	No default.
`sshkey <sshkey_str>`	The public key used for connecting to the CLI using a public-private key pair. For more information on connecting to the CLI using a public-private key pair, see “Connecting to the CLI” in the *FortiWeb Administration Guide*.	No default.

Example

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

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

To display all dashboard status and widget settings, enter:

```
config system admin
show
```

Related topics

- config system accprofile
- config system global
- config user admin-usergrp

system advanced

Use this command to configure several system-wide options that determine how FortiWeb scans traffic.

To use this command, your administrator account's access control profile must have either w or rw permission to the sysgrp area. For more information, see Permissions on page 74.

Syntax

```
config system advanced
   set circulate-url-decode {enable | disable}
   set max-cache-size <cache_int>
   set max-dlp-cache-size <percentage_int>
   set max-dos-alert-interval <seconds_int>
   set max-http-argbuf-length {8k-cache | 12k-cache | 32k-cache | 64k-cache}
   set max-http-header-length {8k-cache | 12k-cache}
   set share-ip {enable | disable}
   set upfile-count {8 | 16}
end
```

Variable	Description	Default
circulate-url-decode {enable | disable}	Enable to detect URL-embedded attacks that are obfuscated using recursive URL encoding (that is, multiple levels' worth of URL encoding). Encoded URLs can be legitimately used for non-English URLs, but can also be used to avoid detection of attacks that use special characters. Encoded URLs can now be decoded to scan for these types of attacks. Several encoding types are supported. For example, you could detect the character A that is encoded as either %41, %x41, %u0041, or \t41. Disable to decode only one level's worth of the URL, if encoded.	disable

Variable	Description	Default
`max-cache-size <cache_int>`	Type the maximum size in kilobytes (KB) of the body of the HTTP **response** from the web server that FortiWeb will cache per URL. Responses are cached to improve performance on compression, decompression, and rewriting on often-requested URLs. Valid values range from 32 to 1,024. The default value is 64. Increasing the body cache may decrease performance.	`64`
`max-dlp-cache-size <percentage_int>`	Type the maximum percentage of max-cache-size <cache_int> — the body of the HTTP response from the web server — that FortiWeb buffers and scans. Responses are cached to improve performance on compression, decompression, and rewriting on often-requested URLs.	12
`max-dos-alert-interval <seconds_int>`	Type the maximum amount of time that FortiWeb will converge into a single log message during a DoS attack or padding oracle attack.	`180`
`max-http-argbuf-length {8k-cache | 12k-cache | 32k-cache | 64k-cache}`	Select the maximum buffer size in kilobytes (KB) for each parameter in the HTTP request. The buffer applies regardless of HTTP method, and whether the parameters are in the URL or body. **Caution: Fortinet strongly recommends that you configure FortiWeb to block requests larger than this buffer.** FortiWeb cannot scan parameters that exceed this buffer size and allows them to pass through. To prevent oversize attacks, configure FortiWeb to block oversized parameters using analyzer-policy <fortianalyzer-policy_name> and analyzer-policy <fortianalyzer-policy_name>. Some web applications require very large requests or parameters, and will not work if oversized parameters are blocked. To be sure that hardening the configuration will not disrupt normal traffic, first configure <parameter_name>-action {alert | alert_deny | block-period} to be `alert`. If no problems occur, switch it to `alert_deny`. **Tip:** Increasing the buffer size increases memory consumption slightly, and may decrease performance. Only increase this value if necessary.	`8k-cache`

Variable	Description	Default
`max-http-header-length {8k-cache | 12k-cache}`	Select the maximum buffer size in kilobytes (KB) for the `Cookie:`, `User-Agent:`, `Host:`, `Referer:`, and other headers in the HTTP request. **Caution: Fortinet strongly recommends that you configure FortiWeb to block requests if those headers are larger than this buffer.** FortiWeb cannot scan headers that exceed this buffer size and allows them to pass through. To prevent oversized attacks, configure FortiWeb to block oversized headers using waf http-protocol-parameter-restriction. Some web applications require very large requests, cookies, or parameters, and will not work if oversized parameters or cookies are blocked. To be sure that hardening the configuration will not disrupt normal traffic, first configure <parameter_name>-action {alert | alert_deny | block-period} to be `alert`. If no problems occur, switch it to `alert_deny`. **Tip:** Increasing the buffer size increases memory consumption slightly, and may decrease performance. Only increase this value if necessary.	`8k-cache`
`share-ip {enable | disable}`	Enable to analyze the ID field of IP headers in order to attempt to detect when multiple clients share the same source IP address. To configure the difference between packets' ID fields that FortiWeb will treat as a shared IP, use system ip-detection. Enabling this option is required for features that have a separate threshold for shared IP addresses, such as brute force login prevention. If you disable the option, those features will behave as if there is only a single threshold, regardless of whether the source IP is shared by many clients.	`disable`
`upfile-count {8 | 16}`	Select the maximum number of uploaded files that FortiWeb antivirus will scan before deciding to pass or block the request.	`8`

Related topics

- `config server-policy policy`
- `config system certificate local`
- `config system global`
- `config system ip-detection`
- `config waf brute-force-login`

- config waf application-layer-dos-prevention
- config waf http-protocol-parameter-restriction

system antivirus

Use this command to configure system-wide FortiGuard Antivirus scan settings.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
config system antivirus
   set default-db {basic | extended}
   set scan-bzip2 {enable | disable}
   set uncomp-size-limit <limit_int>
   set uncomp-nest-limit <limit_int>
end
```

Variable	Description	Default
`default-db {basic | extended}`	Select which of the antivirus signature databases to use when scanning HTTP `POST` requests for trojans, either: • `basic` — 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. • `extended` — Select to use all signatures, regardless of whether the viruses or greyware are currently spreading.	`basic`
`scan-bzip2 {enable | disable}`	Enable to scan archives that are compressed using the BZIP2 algorithm. **Tip:** Scanning BZIP2 archives can be very CPU-intensive. To improve performance, block the BZIP2 file type, then disable this option.	`enable`

Variable	Description	Default
`uncomp-size-limit <limit_int>`	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 `config waf file-uncompress-rule`. **Caution:** Unless you configure otherwise, compressed requests that are too large for this buffer will pass through FortiWeb **without** scanning or rewriting. **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 max-http-body-length <limit_int>. 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 valid range is from 1 to 30720 KB (30 MB).	5000
`uncomp-nest-limit <limit_int>`	Type the maximum number of allowed levels of compression ("nesting") that FortiWeb will attempt to decompress.	`12`

Related topics

- `config system global`

system autoupdate override

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

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see Permissions on page 74.

Syntax

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

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

Related topics

- `config system autoupdate schedule`

system autoupdate schedule

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

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

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

FortiWeb appliances connect to the FDN by connecting to the Fortinet Distribution Server (FDS) nearest to the FortiWeb appliance based on its configured time zone.

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

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see Permissions on page 74.

Syntax

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

```
    set day {Sunday | Monday | Tuesday | Wednesday | Thursday | Friday |
        Saturday}
end
```

Variable	Description	Default
`status {enable | disable}`	Enable to periodically request signature updates from the FDN.	`disable`
`frequency {daily | every | weekly}`	Select the frequency with which the FortiWeb appliance will request signature updates.	`every`
`time <time_str>`	Type the time at which the FortiWeb appliance will request signature updates. The time format is `hh:mm`, where: • `hh` is the hour according to a 24-hour clock • `mm` is the minute	`00:00`
`day {Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday}`	Select which day of the week that the FortiWeb appliance will request signature updates. This option applies only if `frequency` is `weekly`.	`Monday`

Example

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

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

Related topics

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

system autoupdate tunneling

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

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

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

Variable	Description	Default
`status {enable | disable}`	Enable to connect to the FDN through a web proxy.	`disable`
`address {<proxy_fqdn> | <proxy_ipv4>}`	Type either the IP address or fully qualified domain name (FQDN) of the web proxy. The maximum length is 63 characters.	No default.
`port <port_int>`	Type the port number on which the web proxy listens for connections. The valid range is from 0 to 65,535.	`0`
`username <proxy-user_str>`	If the proxy requires authentication, type the FortiWeb appliance's login name on the web proxy.The maximum length is 49 characters.	No default.
`password <proxy-password_str>`	If the proxy requires authentication, type the password for the FortiWeb appliance's login name on the web proxy. The maximum length is 49 characters.	No default.

Example

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

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

Related topics

- `config system autoupdate schedule`

system backup

Use this command to configure automatic backups of the system configuration to an FTP or SFTP server. You can either run the backup immediately or schedule it to run periodically.

The backup can include all uploaded files such as error pages, WSDL files, certificates, and private keys. Fortinet recommends that if you have many such files, that you include them in the backup. This saves you valuable time if you need to restore the configuration in an emergency.

Fortinet strongly recommends that you password-encrypt this backup, and store it in a secure location. This backup 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.

To restore a backup, see `execute backup full-config`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see Permissions on page 74.

Syntax

```
config system backup
   edit <backup_name>
      set config-type {full-config |cli-config | waf-config}
      set encryption {enable | disable}
      set encryption-passwd <password_str>
      set ftp-auth {enable | disable}
      set ftp-user <user_str>
      set ftp-passwd <password_str>
      set ftp-dir "<directory-path_str>"
      set ftp-server {<server_ipv4> | <server_fqdn>}
      set protocol-type {ftp | sftp}
      set schedule_type {now | days}
      set schedule_days {sun mon tue wed thu fri sat}
      set schedule_time <time_str>
   next
end
```

Variable	Description	Default
`<backup_name>`	Type the name of the backup configuration. The maximum length is 59 characters. To display the list of existing backups, type: `edit ?`	No default.

Variable	Description	Default
`config-type {full-config |cli-config | waf-config}`	Select either: • `full-config` — Include both the configuration file and other uploaded files, such a certificate and error page files, in the backup. • `cli-config` — Include only the configuration file in the backup. • `waf-config` — Include only the web protection profiles in the backup.	`cli-config`
`encryption {enable | disable}`	Enable to encrypt the backup file using 128-bit AES and a password. **Caution:** Unlike when downloading a backup from the web UI to your computer, this **does** include all certificates and private keys. Fortinet strongly recommends that you password-encrypt this backup, and store it in a secure location.	`disable`
`encryption-passwd <password_str>`	Type the password that will be used to encrypt the backup file. This field appears only if you enable encryption {enable | disable}.	
`ftp-auth {enable | disable}`	Enable if the server requires that you provide a user name and password for authentication, rather than allowing anonymous connections. When enabled, you must also configure ftp-user <user_str> and ftp-passwd <password_str>. Disable for FTP servers that allow anonymous uploads.	`disable`
`ftp-user <user_str>`	Type the user name that the FortiWeb appliance will use to authenticate with the server. The maximum length is 127 characters. This variable is not available unless `ftp-auth` is `enable`.	No default.
`ftp-passwd <password_str>`	Type the password corresponding to the account specified in ftp-user <user_str>. The maximum length is 127 characters. This variable is not available unless `ftp-auth` is `enable`.	No default.
`ftp-dir "<directory-path_str>"`	Type the directory path on the server where you want to store the backup file. The maximum length is 127 characters.	No default.

Variable	Description	Default
`ftp-server {<server_ipv4> | <server_fqdn>}`	Type either the IP address or fully qualified domain name (FQDN) of the server. The maximum length is 127 characters.	No default.
`protocol-type {ftp | sftp}`	Select whether to connect to the server using FTP or SFTP.	`ftp`
`schedule_type {now | days}`	Select one of the schedule types: • `now` — Use this to initiate the FTP backup immediately upon ending the command sequence. • `days` — Enter this to allow you to set days and a time to run the backup automatically. You must also configure `schedule_days` and `schedule_time`.	`now`
`schedule_days {sun mon tue wed thu fri sat}`	Select one or more days of the week when you want to run a periodic backup. Separate each day with a blank space. For example, to back up the configuration on Monday and Friday, type: `set schedule_days mon,fri` This command is available only if `schedule_type` is `days`.	No default.
`schedule_time <time_str>`	Type the time of day to run the backup. The time format is `hh:mm`, where: • `hh` is the hour according to a 24-hour clock • `mm` is the minute This command is available only if `schedule_type` is `days`.	`00:00`

Example

This example configures a scheduled, full configuration backup every Sunday and Friday at 1:15 AM. The FortiWeb appliance authenticates with the FTP server using an account named `fortiweb1` and its password, `P@ssword1`. It does not encrypt the backup file.

```
config system backup
   edit "Scheduled_Backup"
      set config-type full-config
      set protocol-type ftp
      set ftp-auth enable
      set ftp-user fortiweb1
      set ftp-passwd P@ssword1
      set ftp-server 172.20.120.01
      set ftp-dir "/config-backups"
      set schedule_type days
      set schedule_days sun,fri
```

```
      set schedule_time 01:15
   next
end
```

Related topics

- `execute restore config`
- `execute backup cli-config`

system certificate ca

Use this command to show the names of certificates for a certificate authority (CA). You use the web UI to upload these certificates.

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

CA certificates are not used directly, but must first be grouped in order to be selected in a certificate verification rule. For details, see `config system certificate ca-group`.

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see Permissions on page 74.

Syntax

```
show system certificate ca
```

Example

```
config system certificate ca
   edit "CA_Cert_1"
   next
   edit "CA_Cert_2"
   next
end
```

Related topics

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

system certificate ca-group

Use this command to group certificate authorities (CA).

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see Permissions on page 74.

Syntax

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

Variable	Description	Default
`<ca-group_name>`	Type the name of a certificate authority (CA) group. The maximum length is 35 characters.	No default.
`<ca_index>`	Type the index number of a CA within its group. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
`name <ca_name>`	Type the name of a previously uploaded CA certificate. The maximum length is 35 characters.	No default.

Example

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

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

Related topics

- `execute certificate ca`
- `config system certificate local`
- `config system certificate verify`

system certificate crl

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

To ensure that your FortiWeb appliance validates only certificates that have not been revoked, you should periodically upload a current certificate revocation list, which may be provided by certificate authorities (CA).

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see Permissions on page 74.

Syntax

```
config system certificate crl
   edit <crl_name>
      set url <crl_str>
   next
end
```

Variable	Description	Default
`<crl_name>`	Type the name of a CRL. The maximum length is 35 characters.	No default.
`url <crl_str>`	If you did not upload a CRL file, but instead will query for it from an HTTP or OCSP server, enter the URL of the CRL. The maximum length is 127 characters.	No default.

Related topics

- `execute certificate ca`
- `config system certificate local`
- `config system certificate verify`

system certificate intermediate-certificate

Use this command to show the names of uploaded intermediate CA certificate. You upload these certificates using the web UI.

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see Permissions on page 74.

Syntax

```
show system certificate intermediate-certificate
```

Example

```
config system certificate intermediate-certificate
   edit "Inter_Cert_1"
   next
   edit "Inter_Cert_2"
   next
   edit "Inter_Cert_3"
   next
end
```

Related topics

- execute certificate inter-ca
- config system certificate intermediate-certificate-group
- config server-policy policy

system certificate intermediate-certificate-group

Use this command to group intermediate CA certificates.

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see Permissions on page 74.

Syntax

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

Variable	Description	Default
<intermediate-ca-group_name>	Type the name of an intermediate certificate authority (CA) group. The maximum length is 35 characters.	No default.
<intermediate-ca_index>	Type the index number of an intermediate CA within its group. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
name <ca_name>	Type the name of a previously uploaded intermediate CA certificate. The maximum length is 35 characters.	No default.

Related topics

- execute certificate inter-ca
- config system certificate intermediate-certificate
- config server-policy policy

system certificate local

Use this command to edit the comment associated with a server certificate that is stored locally on the FortiWeb appliance.

You can also configure settings for a certificate that works with an HSM (hardware security module). For more information on HSM integration, see `execute system hsm info` and the *FortiWeb Administration Guide*.

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

- administrators connect to the web UI (HTTPS connections only)
- web clients use SSL or TLS to connect to a virtual server, if you have enabled SSL off-loading in the policy (HTTPS connections and reverse proxy mode)
- web clients use SSL or TLS to connect to a physical server (HTTPS connections and true transparent mode)

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

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

- For connections to the web UI, the FortiWeb appliance presents its default certificate.

The FortiWeb appliance's default certificate does not appear in the list of local certificates. It is used only for connections to the web UI and cannot be removed.

- For SSL off-loading or SSL decryption, upload certificates that do **not** belong to the FortiWeb appliance, but instead belong to the protected hosts. Then, select which one the FortiWeb appliance will use when configuring the SSL option in a policy or server farm.

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see Permissions on page 74.

Syntax

```
config system certificate local
  edit system certificate local
    set comment "<comment_str>"
    set status {na | ok | pending}
    set type {certificate | csr}
    set flag {0 | 1}
    set is-hsm {no | yes}
    set partition-number <partition_name>
```

```
    next
  end
```

Variable	Description	Default
`<certificate_name>`	Type the name of a certificate file. The maximum length is 35 characters.	No default.
`comment "<comment_str>"`	Type a description or other comment. If the comment contains more than one word or contains an apostrophe, surround the comment in double quotes (`"`). The maximum length is 127 characters.	No default.
`status {na | ok | pending}`	Indicates the status of an imported certificate: • `na` indicates that the certificate was successfully imported, and is currently selected for use by the FortiWeb appliance. • `ok` indicates that the certificate was successfully imported but is not selected as the certificate currently in use. To use the certificate, select it in a policy or server farm. • `pending` indicates that the certificate request was generated, but must be downloaded, signed, and imported before it can be used as a local certificate.	No default.
`type {certificate | csr}`	Indicates whether the file is a certificate or a certificate signing request (CSR).	No default.
`flag {0 | 1}`	Indicates if a password was saved. This is used by FortiWeb for backwards compatibility.	No default.
`is-hsm {no | yes}`	Specifies whether you configured the CSR for this certificate to work with an integrated HSM.	`no`
`partition-number <partition_name>`	Enter the name of the HSM partition you selected when you created the CSR for this certificate.	No default.

Example

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

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

Related topics

- `execute certificate local`
- `config server-policy policy`
- `config server-policy server-pool`

system certificate sni

In some cases, the members of a server pool or a single pool member host multiple secure websites that use different certificates. Use this command to create a Server Name Indication (SNI) configuration that identifies the certificate to use by domain.

You can select a SNI configuration in a server policy only when the operating mode is 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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see Permissions on page 74.

Syntax

```
config system certificate sni
   edit <sni_name>
      config members
         edit <entry_index>
            set domain <server_fqdn>
            set local-cert <local-cert_name>
            set inter-group <intermediate-cagroup_name>
            set verify <certificate_verificator_name>
         end
      next
end
```

Variable	Description	Default
`<sni_name>`	Type the name of an Server Name Indication (SNI) configuration.	No default.
`<entry_index>`	Type the index number of an SNI configuration entry. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
`domain <server_fqdn>`	Type the domain of the secure website (HTTPS) that uses the certificate specified by `local-cert <local-cert_name>`.	No default.
`local-cert <local-cert_name>`	Type the name of the server certificate that FortiWeb uses to encrypt or decrypt SSL-secured connections for the website specified by `domain <server_fqdn>`.	

Variable	Description	Default
`inter-group <intermediate-cagroup_name>`	Type 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-cert <local-cert_name>. If clients receive certificate warnings that an intermediary CA has signed the server certificate configured in `local-cert`, rather than by a root CA or other CA currently trusted by the client directly, configure this option. 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 the *FortiWeb Administration Guide*.	
`verify <certificate_verificator_name>`	Type 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.) 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 alternatively or in addition to HTTP authentication (see `config waf http-authen http-authen-rule`). To display the list of existing verifiers, type: `edit ?` **Note:** The client must support SSL 3.0 or TLS 1.0.	

Related topics

- `config system certificate local`
- `config system certificate intermediate-certificate-group`
- `config system certificate verify`

system certificate urlcert

Use this command to configure the URL-based client certificate feature for a server policy or server pool. This feature allows you to require a certificate for some requests and not for others. Whether a client is required to present a personal certificate or not is based on the requested URL and the rules you specify in the URL-based client certificate group.

A URL-based client certificate group specifies the URLs to match and whether the matched request is required to present a certificate or exempt from presenting a certificate.

When the URL-based client certificate feature is enabled, clients are not required to present a certificate if the request URL is specified as exempt in the URL-based client certificate group rule or URL of the request does not match a rule.

Syntax

```
config system certificate urlcert
   edit <url-cert-group_name>
      config list
         edit <entry_index>
            set url <url_str>
            set require {enable | disable}
         end
      next
end
```

Variable	Description	Default
`<url-cert-group_name>`	Enter the name for the URL-based client certificate group.	No default.
`<entry_index>`	Type the index number of an URL-based client certificate group entry.	No default.
`url <url_str>`	Enter a URL to match. When the URL of a client request matches this value and the value of `require` is `enable`, FortiWeb requires the client to present a private certificate.	No default.
`require {enable | disable}`	Specifies whether client requests with the URL specified by `url` are required to present a personal certificate. When you select `disable`, FortiWeb does not require client requests with the specified URL to present a personal certificate.	No default.

Related topics

- `config server-policy policy`
- `config server-policy server-pool`

system certificate verify

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

To apply a certificate verification rule, select it in a policy. For details, see `config server-policy policy`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For more information, see Permissions on page 74.

Syntax

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

Variable	Description	Default
`<certificate_ verificator_name>`	Type the name of a certificate verifier. The maximum length is 35 characters.	No default.
`ca <ca-group_name>`	Type the name of a CA group, if any, that you want to use to authenticate client certificates. The maximum length is 35 characters.	No default.
`crl <crl_name>`	Type the name of a certificate revocation list, if any, to use to verify the revocation status of client certificates. The maximum length is 35 characters.	No default.

Related topics

- `config system certificate ca-group`
- `config system certificate crl`
- `config server-policy policy`
- `config server-policy server-pool`

system conf-sync

Use this command to configure non-HA configuration synchronization settings.

This command configures, but does **not** execute, the synchronization. To do this, use the web UI.

This command works only when administrative domains (ADOMs) are disabled.

This type of synchronization is used between FortiWeb appliances that are not part of a native FortiWeb high availability (HA) pair, such as when you need to clone the configuration once, or when HA is provided by an external device.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
config system conf-sync
   set ip <remote-fortiweb_ipv4>
   set password <password_str>
   set sync-type {full-sync | partial-sync}
   set server-port <port_int>
end
```

Variable	Description	Default
ip <remote-fortiweb_ipv4>	Type the IP address of the remote FortiWeb appliance that you want to synchronize with the local FortiWeb appliance.	0.0.0.0
password <password_str>	Type the administrator password for the remote FortiWeb appliance. The maximum length is 63 characters.	No default.

Variable	Description	Default

`sync-type {full-sync | partial-sync}`	Select one of the synchronization types.
	For all operation modes except WCCP, `full-sync` updates the entire configuration of the peer FortiWeb appliance **except for** the following items:
	• Network interface used for synchronization (prevents sync from accidentally breaking connectivity with future syncs)
	• Administrator accounts
	• Access profiles
	• HA settings
	For the WCCP operation mode, `full-sync` updates the entire configuration **except for** the following items:
	• `config system interface`
	• `config route static`
	• `config route policy`
	• `config system wccp`
	• Administrator accounts
	• Access profiles
	• HA settings
	For all operation modes, `partial-sync` updates the configuration of the peer FortiWeb appliance, **except for** the following items:
	`router ...`
	`server-policy health`
	`server-policy http-content-routing-policy`
	`server-policy persistence-policy`
	`server-policy policy`
	`server-policy server-pool`
	`server-policy service custom`
	`server-policy service predefined`
	`server-policy vserver`
	`system ...`
		`partial-sync`

`server-port <port_int>`	Type the port number of the remote (peer) FortiWeb appliance that is used to connect to the local appliance for configuration synchronization. The valid range is from 1 to 65,535. **Caution:** The port number used with this command must be different than the port number used with `config system global` command or the submitting operation will fail.	`955`

Related topics

- config system settings
- config system global

system console

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

To use this command, your administrator account's access control profile must have either w or rw permission to the sysgrp area. For more information, see Permissions on page 74.

Syntax

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

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

Example

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

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

Related topics

- config system admin

system dns

Use this command to configure the FortiWeb appliance with its local domain name, and the IP addresses of the domain name system (DNS) servers that the FortiWeb appliance will query to resolve domain names such as www.example.com into IP addresses.

FortiWeb appliances require connectivity to DNS servers for DNS lookups. Use either the DNS servers supplied by your Internet service provider (ISP) or the IP addresses of your own DNS servers. You must provide unicast, non-local addresses for your DNS servers. Local host and broadcast addresses will not be accepted.

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

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

Variable	Description	Default
`primary <dns_ipv4>`	Type the IP address of the primary DNS server.	`8.8.8.8`
`secondary <dns_ipv4>`	Type the IP address of the secondary DNS server.	`0.0.0.0`

Variable	Description	Default
`domain <local-domain_str>`	Type the name of the local domain to which the FortiWeb appliance belongs, if any. The maximum length is 127 characters. This field is optional. It will not appear in the `Host:` field of HTTP headers for client connections to protected web servers. **Note:** You can also configure the host name. For details, see system global on page 256.	No default.

Example

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

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

Related topics

- `config log syslog-policy`
- `config router static`
- `config system interface`
- `config system global`
- `config server-policy policy`

system eventhub

When FortiWeb-VM is deployed on Azure, use this command to manually configure the FortiWeb appliance to send log messages to Azure Event Hubs.

Alternatively, you can create the configuration automatically using a PowerShell script. For more information, see the *FortiWeb-VM for Azure Install Guide*.

When the event hub configuration is complete, FortiWeb sends health logs to Azure Event Hub.

If you also create a corresponding Azure CEF SIEM policy (see `config log siem-policy`), FortiWeb also sends security logs to Azure Event Hubs.

This command is available for FortiWeb-VM running on Microsoft Azure only.

You can use the Azure classic portal to obtain the values that the `config system eventhub` settings require. For detailed instructions, see the *FortiWeb-VM for Azure Install Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
config system eventhub
   set status {enable | disable}
   set appliance_id <subscription_str>
   set policy_saskey <primary-key_str>
   set policy_name <policy-name_str>
   set eventhub_name <ehub-name_str>
   set servicebus_namespace <servicebus-namespace_str>
end
```

Variable	Description	Default
`status {enable | disable}`	Enter `enable` to activate the Azure event hub configuration.	`disable`
`appliance_id <subscription_str>`	Enter the subscription (ID) that has the access to the Azure Event Hub	No default.
`policy_saskey <primary-key_str>`	Enter the primary shared access key that the specified policy (by `policy_name <policy-name_str>`) uses for Shared Access Signature authentication on the Azure Event Hub.	No default.
`policy_name <policy-name_str>`	Enter the name of the Shared Access policy created for the Azure Event Hub.	No default.
`eventhub_name <ehub-name_str>`	Enter the name of the Azure Event Hub that is associated with the specified service bus (by `servicebus_namespace <servicebus-namespace_str>`).	No default.
`servicebus_namespace <servicebus-namespace_str>`	Enter the Service Bus Namespace that the Event Hub is created at.	No default.

Related topics

- `log siem-policy`
- `config system eventhub`

system fail-open

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 port3 + port4
- FortiWeb port3 + port4 and port5 + port6
- FortiWeb port5 + port6
- FortiWeb 3000E/4000E: port9 + port10, port11 + port12, port13 + port14, or port15 + port16
- FortiWeb port5 + port6 and port7 + port8
- FortiWeb port5 + port6 and port7 + port8
- FortiWeb port5 + port6

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.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
config system fail-open
   set port3-port4 {poweroff-bypass | poweroff-cutoff}
end
```

Variable	Description	Default
port3-port4 {poweroff-bypass | poweroff-cutoff}	Select either: • poweroff-bypass — Behave like a wire when powered off, allowing connections to pass directly through from one port to the other, bypassing policy and profile filtering. • poweroff-keep — Interrupt connectivity when powered off. **Note:** The name of this setting varies by which ports are wired together for bypass in your specific hardware model.	poweroff-bypass

Related topics

- config system ha

system fips-cc

Use this command to enable and configure Federal Information Processing Standards (FIPS) and Common Criteria (CC) compliant mode.

When the FIPS-CC certification process is complete, a separate document will provide detailed information about this command.

system firewall address

Use this command to configure IP addresses and address ranges that FortiWeb's built-in stateful firewall uses. You use the address configuration in a firewall policy (see config system firewall firewall-policy.)

Syntax

```
config system firewall address
   edit <firewall-address_name>
        set type {ip-netmask | ip-range}
        set ip-netmask <firewall-address_ipv4mask>
        set ip-address-value <firewall-address_ipv4>
end
```

Variable	Description	Default
<firewall-address_name>	Enter a name that identifies this firewall address configuration.	No default.

Variable	Description	Default
type {ip-netmask | ip-range}	Select how this configuration specifies a firewall address or addresses: • ip-netmask — A single IP address and netmask. • ip-range — A single IP address or a range of IP addresses.	ip-range
ip-netmask <firewall-address_ipv4mask>	Enter an IPv4 address and subnet mask, separated by a forward slash (/). For example, 192.0.2.2/24. Available when type is ip-netmask.	No default.
ip-address-value <firewall-address_ipv4>	Enter a single IP address or a range of addresses. For example, 172.22.14.1, or 172.22.14.1-172.22.14.255. Available when type is ip-range.	No default.

Related topics

- config system firewall firewall-policy
- config system firewall service

system firewall service

Use this command to configure the protocols and ports that FortiWeb's built-in stateful firewall uses. You use the service configuration in a firewall policy (see config system firewall firewall-policy.)

Syntax

```
config system firewall service
   edit <firewall-service_name>
        set protocol {TCP | UDP | ICMP}
        set source-port-min <source-port-min_int>
        set source-port-max <source-port-max_int>
        set destination-port-min <source-port-min_int>
        set destination-port-max <source-port-max_int>
end
```

Variable	Description	Default
<firewall-service_name>	Enter a name that identifies this firewall service configuration.	No default.
protocol {TCP | UDP | ICMP}	Select the protocol for this firewall service configuration.	TCP

Variable	Description	Default
source-port-min <source-port-min_int>	Enter the start port in the range of source ports for this firewall service.	0
source-port-max <source-port-max_int>	Enter the end port in the range of source ports for this firewall service	65535
destination-port-min <source-port-min_int>	Enter the start port in the range of destination ports for this firewall service.	0
destination-port-max <source-port-max_int>	Enter the end port in the range of destination ports for this firewall service	65535

Related topics

- config system firewall address
- config system firewall firewall-policy

system firewall firewall-policy

Use this command to configure the policies that FortiWeb's built-in stateful firewall uses to determine which traffic to allow and deny.

The firewall policy uses address and service configurations that you create separately (see config system firewall address and config system firewall service.)

Syntax

```
config system firewall firewall-policy
   set default-action {deny | accept}
   edit <entry_index>
        set in-interface <incoming_interface_ name>
        set out-interface <outgoing_interface_ name>
        set src-address <firewall-address_name>
        set dest-address <firewall-address_name>
        set service <firewall-service_name>
        set action {deny | accept}
end
```

Variable	Description	Default
`default-action {deny | accept}`	• `deny` — Firewall blocks traffic that does not match a policy rule. However, administrative access is still allowed on network interfaces for which it has been configured. • `accept` — Firewall allows traffic that does not match a policy rule.	`accept`
`<entry_index>`	Enter the index number of the policy rule in the table.	No default.
`in-interface <incoming_ interface_ name>`	Enter the name of the interface (for example, `port1`) on which FortiWeb receives packets it applies this firewall policy rule to.	No default.
`out-interface <outgoing_ interface_ name>`	Enter the name of the interface (for example, `port2`) through which FortiWeb routes packets it applies this firewall policy rule to.	No default.
`src-address <firewall-address_name>`	Enter the name of the firewall address configuration that specifies the source IP address or addresses to which this policy applies. For information on creating firewall address configurations, see `config system firewall address`.	No default.
`dest-address <firewall-address_name>`	Enter the name of the firewall address configuration that specifies the source IP address or addresses to which this policy rule applies. For information on creating firewall address configurations, see `config system firewall address`.	No default.
`service <firewall-service_name>`	Enter the name of the firewall service configuration that specifies the protocols and ports to which this policy rule applies. For information on creating firewall service configurations, see `config system firewall service`.	No default.
`action {deny | accept}`	• `deny` — Firewall blocks traffic that matches this policy rule. However, administrative access is still allowed on network interfaces for which it has been configured. • `accept` — Firewall allows traffic that matches this policy rule.	`deny`

Example

This example configures a firewall policy to deny any HTTP services but coming from specified sources.

```
config system firewall address
   edit "alloowed_source"
```

```
      set type ip-range
      set ip-address-value 172.22.203.100-172.22.203.115
end
config system firewall address
   edit "site1"
      set type ip-netmask
      set ip-netmask 206.11.0.2/24
end
config system firewall service
   edit "http"
      set protocol TCP
      set destination-port-min 80
      set destination-port-max 80
end
config system firewall firewall-policy
   set default-action deny
   edit "http_allowed"
      set in-interface port1
      set out-interface port2
      set src-address allowed_source
      set dest-address site1
      set service http
      set action accept
end
```

Related topics

- config system firewall address
- config system firewall service

system fortigate-integration

FortiGate appliances can maintain a list of source IPs that it prevents from interacting with the network and protected systems. You can configure FortiWeb to receive this list of IP addresses at intervals you specify. Then, you configure an inline protection profile to detect the IP addresses in the list and take an appropriate action.

This feature is available only if the operating mode is reverse proxy or true transparent proxy.

This command configures a FortiGate appliance that provides banned source IPs. To configure FortiWeb to detect the quarantined IP addresses and take the appropriate action, configure the FortiGate Quarantined IPs settings in an inline protection profile. (See `config waf web-protection-profile inline-protection`.)

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
config system fortigate-integration
   set address <address_ipv4>
   set port <port_int>
   set protocol {HTTP | HTTPS}
   set username <username_str>
```

```
    set password <password_str>
    set schedule-frequency <schedule-frequency_int>
    set flag {enable | disable}
  end
```

Variable	Description	Default
`address <address_ipv4>`	Enter the FortiGate IP address that is used for administrative access.	No default.
`port <port_int>`	Specify the port that the FortiGate uses for administrative access via HTTPs. In most cases, this is port 443.	`80`
`protocol {HTTP | HTTPS}`	Specify whether the FortiGate and FortiWeb communicate securely using HTTPS.	`HTTP`
`username <username_str>`	Enter the name of the administrator account that FortiWeb uses to connect to the FortiGate.	No default.
`password <password_str>`	Enter the password for the FortiGate administrator account that FortiWeb uses.	No default.
`schedule-frequency <schedule-frequency_int>`	Enter how often FortiWeb checks the FortiGate for an updated list of banned source IP addresses, in hours. The valid range is 1 to 5.	`1`
`flag {enable | disable}`	Enables or disables the transmission of quarantined source IP address information from the specified FortiGate.	`disable`

Related topics

- `config waf file-upload-restriction-policy`
- `config log reports`
- `get system fortisandbox-statistics`

system fortisandbox

Use this command to configure FortiWeb to submit all files that match your upload restriction rules to FortiSandbox.

FortiSandbox evaluates whether the file poses a threat and returns the result to FortiWeb. If FortiSandbox determines that the file is malicious, FortiWeb performs the following tasks:

- Generates an attack log message that contains the result.
- For 10 minutes after it receives the FortiSandbox results, takes the action specified by the file upload restriction policy. During this time, it does not re-submit the file to FortiSandbox.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
config system fortisandbox
   set type {fsa | cloud}
   set server <server_ipv4>
   set ssl {enable | disable}
   set cache-timeout <timeout_int>
   set email <email_str>
   set interval <interval_int>
end
```

Variable	Description	Default
`type {fsa | cloud}`	Specifies whether FortiWeb submits files that match the upload restriction rules to a FortiSandbox physical appliance (or FortiSandbox-VM) or to FortiSandbox Cloud. The FortiSandbox Cloud option requires you to register your FortiWeb and a FortiWeb FortiGuard Sandbox Cloud Service subscription.	`fsa`
`server <server_ipv4>`	Enter the IP address of the FortiSandbox to send files to. Available only when `type` is `fsa`.	No default.
`ssl {enable | disable}`	Enter `enable` to communicate with the specified FortiSandbox using SSL.	`disable`
`cache-timeout <timeout_int>`	Enter how long FortiWeb waits before it clears the hash table entry for an uploaded file that was evaluated by FortiSandbox, in hours. Valid values are from 1 to 168. FortiWeb stores file evaluation results from FortiSandbox in a hash table. Whenever a client uploads a file, FortiWeb looks for a table entry that matches it. If there is a matching entry, FortiWeb takes action based on the stored result. If there is no matching entry, FortiWeb sends the file to FortiSandbox for evaluation.	`72`
`email <email_str>`	Enter the email address that FortiSandbox sends weekly reports and notifications to.	No default.
`interval <interval_int>`	Enter a number that specifies how often FortiWeb retrieves statistics from FortiSandbox, in minutes.	`5`

Example

This example creates a connection to a FortiSandbox at 192.0.2.2 that retrieves statistics at the default interval (5 minutes) and sends a weekly report to admin@example.com.

```
config system fortisandbox
   set server 192.0.2.2
   set ssl enable
   set email admin@example.com
end
```

Related topics

- config waf file-upload-restriction-policy
- config log reports
- get system fortisandbox-statistics

system global

Use this command to configure system-wide settings such as language, display refresh rate and listening ports of the web UI, the time zone and host name of the FortiWeb appliance, and NTP time synchronization.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
config system global
   set admin-port <port_int>
   set admin-sport <port_int>
   set admintimeout <minutes_int>
   set adom-admin {enable | disable}
   set anypktstream {enable | disable}
   set auth-timeout <milliseconds_int>
   set certificate <certificate_name>
   set cli-signature {enable | disable}
   set confsync-port <port_int>
   set dh-params {1024 | 1536 | 2048 | 3072 | 4096 | 6144 | 8192}
   set dst {enable | disable}
   set high-compatibility-mode {enable | disable}
   set hostname <host_name>
   set hsm {enable | disable}
   set ie6workaround {enable | disable}
   set language {english |japanese | simch | trach}
   set maintainer-user {enable | disable}
   set no-sslv3 {enable | disable}
   set ntpserver {<ntp_fqdn> | <ntp_ipv4>}
   set ntpsync {enable | disable}
   set pre-login-banner {enable | disable}
   set refresh <seconds_int>
   set single-admin-mode {enable | disable}
   set strong-password {enable | disable}
```

```
    set syncinterval <minutes_int>
    set timezone <time-zone-code_str>
    set tftp {enable | disable}
    set ssh-fips {enable | disable}
end
```

Variable	Description	Default
admin-port <port_int>	Type the port number on which the FortiWeb appliance listens for HTTP access to the web UI. The valid range is from 1 to 65,535.	80
admin-sport <port_int>	Type the port number on which the FortiWeb appliance listens for HTTPS (SSL-secured) access to the web UI. The valid range is from 1 to 65,535.	443
admintimeout <minutes_int>	Type the amount of time in minutes after which an idle administrative session with the web UI or CLI will be automatically logged out. The valid range is from 1 to 480 minutes (8 hours). To improve security, do not increase the idle timeout.	5
adom-admin {enable | disable}	Enable to be able to restrict administrator accounts to specific administrative domains. See also domains <adom_name> in config system admin. **Note:** After you type end, if this setting is enabled, the CLI will terminate your session and restructure the configuration to use ADOMs. Global settings will remain in the global configuration scope, but objects that are configurable separately per ADOM such as services are moved to the root ADOM. To continue by configuring additional ADOMs, log in again, then go to Defining ADOMs on page 86.	disable
anypktstream {enable | disable}	Enable to configure FortiWeb to scan partial TCP connections. In some cases, FortiWeb is deployed after a client has already created a connection with a back-end server. If this option is disabled, FortiWeb ignores any traffic that is part of a pre-existing session.	disable

Variable	Description	Default
`auth-timeout <milliseconds_int>`	Type the number of milliseconds that FortiWeb will wait for the remote authentication server to respond to its query. The valid range is from 1 to 60,000 (60 seconds). If administrator logins often time out, and FortiWeb is configured to query an external RADIUS or LDAP server, increasing this value may help. This setting only affects remote authentication queries for **administrator** accounts. To configure the query connection timeout for end-user accounts, use auth-timeout <timeout_int> in the HTTP authentication policy instead.	`2000`
`cli-signature {enable | disable}`	Enable to be able to enter custom attack signatures via the CLI. Typically, attack signatures should be entered using the web UI, where you can verify syntax and test matching of your regular expression. If you are sure that your expression is correct, you can enable this option to enter your custom signature via the CLI.	`disable`
`confsync-port <port_int>`	Type the port number the local FortiWeb uses to listen for a remote (peer) FortiWeb. Used when you have configured FortiWeb to synchronize its configuration. The valid range is from 1 to 65,535. **Caution:** The port number must be different than the port number set using `config server-policy custom-application application-policy`.	`8333`
`dh-params {1024 | 1536 | 2048 | 3072 | 4096 | 6144 | 8192}`	Specifies the key length that FortiWeb presents in Diffie-Hellman exchanges. Most web browsers require a key length of at least 2048.	`2048`
`dst {enable | disable}`	Enable to automatically adjust the FortiWeb appliance's clock for daylight savings time (DST).	`disable`
`high-compatibility-mode {enable | disable}`	Enable to accelerate SSL transport.	

Variable	Description	Default
`hostname <host_name>`	Type the host name of this FortiWeb appliance. Host names may include US-ASCII letters, numbers, hyphens, and underscores. The maximum length is 35 characters. Spaces and special characters are not allowed. The host name of the FortiWeb appliance is used in several places. • It appears in the **System Information** widget on the **Status** tab of the web UI, and in the router all CLI command. • It is used in the command prompt of the CLI. • It is used as the SNMP system name. For information about SNMP, see `config system snmp sysinfo`. The **System Information** widget and the router all CLI command will display the full host name. However, if the host name is longer than 16 characters, the CLI and other places display the host name in a truncated form ending with a tilde (~) to indicate that additional characters exist, but are not displayed. For example, if the host name is FortiWeb1234567890, the CLI prompt would be `FortiWeb123456789~#`. **Note:** You can also configure the local domain name. For details, see `config system dns`.	`FortiWeb`
`hsm {enable | disable}`	Specifies whether the settings you use to integrate FortiWeb with an HSM (hardware security module) are displayed in the web UI.	`disable`
`ie6workaround {enable | disable}`	Enable to use the work around for a navigation bar freeze issue caused by using the web UI with Microsoft Internet Explorer 6.	`disable`

Variable	Description	Default
`language {english |japanese | simch | trach}`	Select which language to use when displaying the web UI. The display's web pages will use UTF-8 encoding, regardless of which language you choose. UTF-8 supports multiple languages, and allows all of them to be displayed correctly, even when multiple languages are used on the same web page. For example, your organization could have web sites in both English and simplified Chinese. Your FortiWeb administrators prefer to work in the English version of the web UI. They could use the web UI in English while writing rules to match content in both English and simplified Chinese **without** changing this setting. Both the rules and the web UI will display correctly, as long as all rules were input using UTF-8. Usually, your text input method or your management computer's operating system should match the display, and also use UTF-8. If they do not, you may not be able to correctly display both your input and the web UI at the same time. For example, your web browser's or operating system's default encoding for simplified Chinese input may be GB2312. However, you **usually** should switch it to be UTF-8 when using the web UI, **unless** you are writing regular expressions that must match HTTP client's requests, and those requests use GB2312 encoding. For more information on language support in the web UI and CLI, see Language support & regular expressions on page 80. **Note:** This setting does **not** affect the display of the CLI.	`english`
`maintainer-user {enable | disable}`	Specifies whether the maintainer administrator account is enabled. The maintainer account is enabled by default and allows you to reset the password for the admin account using a console connection	`enable`

Variable	Description	Default
`no-sslv3 {enable | disable}`	Enable to disable support for SSL 3.0 connections to the web UI. Protects against a POODLE (Padding Oracle On Downgraded Legacy Encryption) attack. To disable access to back-end servers via SSL 3.0, use `config server-policy policy` or `config server-policy server-pool`.	`enable`
`ntpserver {<ntp_fqdn> | <ntp_ipv4>}`	Type the IP address or fully qualified domain name (FQDN) of a Network Time Protocol (NTP) server or pool, such as `pool.ntp.org`, to query in order to synchronize the FortiWeb appliance's clock. The maximum length is 63 characters. For more information about NTP and to find the IP address of an NTP server that you can use, see: http://www.ntp.org/	No default.
`ntpsync {enable | disable}`	Enable to automatically update the system date and time by connecting to a NTP server. Also configure ntpserver {<ntp_fqdn> | <ntp_ipv4>}, syncinterval <minutes_int> and timezone <time-zone-code_str>.	`disable`
`pre-login-banner {enable | disable}`	Enable to add a login disclaimer message for administrators logging in to FortiWeb. This disclaimer is a statement that a user accepts or declines. It is useful for environments such as corporations that are governed by strict usage policies for forensics and legal reasons. For information on modifying the disclaimer, see `config system replacemsg`.	`disable`
`refresh <seconds_int>`	Type the automatic refresh interval, in seconds, for the web UI's **System Status Monitor** widget. The valid range is from 0 to 9,223,372,036,854,775,807 seconds. To disable automatic refreshes, type `0`.	`80`

Variable	Description	Default
`single-admin-mode {enable | disable}`	Enable to allow only one administrator account to be logged in at any given time. This option may be useful to prevent administrators from inadvertently overwriting each other's changes. When multiple administrators simultaneously modify the same part of the configuration, they each edit a copy of the current, saved state of the configuration item. As each administrator makes changes, FortiWeb does **not** update the other administrators' working copies. Each administrator may therefore make conflicting changes without being aware of the other. The FortiWeb appliance will only use whichever administrator's configuration is saved last. If only one administrator can be logged in at a time, this problem cannot occur. Disable to allow multiple administrators to be logged in. In this case, administrators should communicate with each other to avoid overwriting each other's changes.	`disable`
`strong-password {enable | disable}`	Enable to enforce strong password rules for administrator accounts. If the password entered is not strong enough when a new administrator account is created, the FortiWeb appliance displays an error and prompts to enter a stronger password. Strong passwords have the following characteristics: • are between 8 and 16 characters in length • contain at least one upper case and one lower case letter • contain at least one numeric • contain at least one non-alphanumeric character	`disable`
`syncinterval <minutes_int>`	Type how often, in minutes, the FortiWeb appliance should synchronize its time with the Network Time Protocol (NTP) server. The valid range is from 1 to 1440 minutes. To disable time synchronization, type `0`.	`60`
`tftp {enable | disable}`	Specifies whether FortiWeb can perform backups, restoration, firmware updates and other tasks using TFTP.	`enable`

Variable	Description	Default
timezone <time-zone-code_str>	Type the two-digit code for the time zone in which the FortiWeb appliance is located. The valid range is from 00 to 74. To display a list of time zone codes, their associated the GMT time zone offset, and contained major cities, type set timezone ?.	00
ssh-fips {enable | disable}	A setting used with Federal Information Processing Standards (FIPS) and Common Criteria (CC) compliant mode. When the FIPS-CC certification process is complete, a separate document will provide detailed information about this command.	disable

Example

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

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

For an example that includes a host name, see config system dns.

Related topics

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

system ha

Use this command to configure the FortiWeb appliance to act as a member of a high availability (HA) cluster in order to improve availability.

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 your 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 `config server-policy custom-application application-policy`.

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))
- Redundant network topology: if the active appliance fails, physical network cabling and routes must redirect web traffic to the standby appliance
- At least one physical port on both HA appliances connected directly, via crossover cables, or through switches

FortiWeb-VM now 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.

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, standby, or slave), which assumes the role of the active appliance and begins processing connections **only** if the active appliance fails.

For more information on HA, including troubleshooting, failover behavior, synchronized data, and network topology, see the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
config system ha
   set mode {active-passive | standalone}
   set group-id <group_int>
   [set group-name <pair-name_str>]
   set priority <level_int>
   set override {enable | disable}
   set hbdev <interface_name>
   [set hbdev-backup <interface_name>]
   set hb-interval <milliseconds_int>
   set hb-lost-threshold <seconds_int>
   set arps <arp_int>
   set arp-interval <seconds_int>
   [set monitor {<interface_name> ...}]
   set boot-time <limit_int>
   set ha-mgmt-status { enable | disable}
   set ha-mgmt-interface <interface_name>
```

```
end
```

Variable	Description	Default
`mode {active-passive | standalone}`	Select one of the following: • `active-passive` — Form an HA group with another FortiWeb appliance. The appliances operate together, with the standby assuming the role of the active appliance if it fails. • `standalone` — Operate each appliance independently. **Note:** To avoid connectivity issues, do not use config system ha to remove an appliance from an HA cluster. Instead, use `config ha disconnect`, which removes the appliance from the cluster and changes the HA mode to standalone.	`standalone`
`group-id <group_int>`	Type a number that identifies the HA pair. **Both members of the HA pair must have the same group ID.** If you have more than one HA pair on the same network, each HA pair must have a different group ID. Changing the group ID changes the cluster's virtual MAC address. The valid range is 0 to 63.	`0`
`group-name <pair-name_str>`	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.	No default.
`priority <level_int>`	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 `config ha manage`.) This setting is optional. The smaller the number, the higher the priority. The valid range is 0 to 9. **Note:** By default, unless you enable override {enable | disable}, uptime is more important than this setting. For details, see the *FortiWeb Administration Guide*.	`5`

Variable	Description	Default
`override {enable | disable}`	Enable to make priority <level_int> a more important factor than uptime when selecting the primary appliance.	`disable`
`hbdev <interface_name>`	Select which port 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). The maximum length is 15 characters. Connect this port to the same port number on the other member of the HA cluster. (e.g., If you select `port3` for the primary heartbeat link, connect port3 on **this** appliance to port3 on the **other** appliance.) 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. 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. **Tip:** If enough ports are available, you can select both a primary heartbeat interface and a secondary heartbeat interface (hbdev-backup <interface_name>) 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.) **Note:** If a switch is used to connect the heartbeat interfaces, the heartbeat interfaces must be reachable by Layer 2 multicast.	No default.

Variable	Description	Default
`hbdev-backup <interface_name>`	Select a secondary, standby port 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). It must **not** be the same network interface as hbdev <interface_name>. The maximum length is 15 characters. Connect this port to the same port number on the other member of the HA cluster. (e.g., If you select `port4` for the secondary heartbeat link, connect port4 on **this** appliance to port4 on the **other** appliance.) 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.	No default.

Variable	Description	Default
arps <arp_int>	Type the number of times that the FortiWeb appliance will broadcast 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 different 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 arp-interval <seconds_int>. Normally, you do not need to change this setting. Exceptions include: • 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. • 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. The valid range is 1 to 16.	3

Variable	Description	Default
`arp-interval <seconds_int>`	Type the number of seconds to wait between each broadcast of ARP packets. Normally, you do not need to change this setting. Exceptions include: • 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. • 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. The valid range is from 1 to 20.	1
`hb-interval <milliseconds_int>`	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. This part of the configuration is synchronized between the active appliance and standby appliance. The valid range is 1 to 20 (that is, between 100 and 2,000 milliseconds). **Note:** Although this setting is synchronized between the main and standby appliances, you should initially configure both appliances with the same hb-interval <milliseconds_int> to prevent inadvertent failover from occurring before the initial synchronization.	1

Variable	Description	Default
`hb-lost-threshold <seconds_int>`	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. This part of the configuration is synchronized between the main appliance and standby appliance. Normally, you do not need to change this setting. Exceptions include: • 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. • 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. The valid range is from 1 to 60. **Note:** Although this setting is synchronized between the main and standby appliances, you should initially configure both appliances with the same hb-lost-threshold <seconds_int> to prevent inadvertent failover from occurring before the initial synchronization. **Note:** You can use SNMP traps to notify you when a failover is occurring. For details, see `config system snmp community`.	3

Variable	Description	Default
`monitor {<interface_name> ...}`	Type the name of one or more network interfaces that each directly correlate with a physical link. These ports will be monitored for link failure. Separate the name of each network interface with a space. To remove from or add to the list of monitored network interfaces, retype the entire list. Port monitoring (also called interface monitoring) monitors physical network ports to verify that they are functioning properly and linked to their networks. If the physical port fails or the cable becomes disconnected, a failover occurs. You can monitor physical interfaces, but **not** VLAN subinterfaces or 4-port switches. **Note:** To prevent an unintentional failover, do not configure port monitoring **until** 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.	No default.
`boot-time <limit_int>`	Type the maximum number of seconds that a appliance will wait for a heartbeat or synchronization connection after the appliance returns online. If this limit is exceeded, the appliance will assume that the other unit is unresponsive, and assume the role of the main appliance. Due to the default heartbeat and synchronization intervals, as long as the HA pair are cabled directly together, the default value is usually sufficient. If the HA heartbeat link passes through other devices, such as routers and switches, however, a larger value may be needed. You may notice this especially when updating the firmware. The valid range is from 1 to 100 seconds.	`30`

Variable	Description	Default
ha-mgmt-status { enable | disable}	Specifies whether the network interface you select provides administrative access to this appliance when it is a member of the HA cluster. When this option is selected, you can access the configuration for this cluster member using the IP address of the specified network interface. The interface configuration, including administrative access and other settings, is not synchronized with other cluster members. You cannot configure routing for the port you select. To allow your management computer to connect with the web UI and CLI, ensure it is on the same subnet as the port. (Alternatively, you can configure a source IP NAT on the router or firewall that modifies the management computer's source IP.) You can configure up to 8 reserved management ports in each HA cluster.	disable
ha-mgmt-interface <interface_name>	Specifies the network interface that provides administrative access to this appliance when it is a member of the HA cluster.	No default.

Example

This example configures a FortiWeb appliance as one appliance in an active-passive HA pair whose group ID is 1. The primary heartbeat occurs over port3, and the secondary heartbeat link is over port4. Priority is more important than uptime when electing the main appliance. The appliance will wait 30 seconds after boot time for a heartbeat or synchronization before assuming that it should be that main appliance. Aside from the heartbeat link, failover can also be triggered by port monitoring of port1 and port2.

```
config system ha
   set mode active-passive
   set group-id 1
   set priority 6
   set override enable
   set hbdev port3
   set hbdev-backup port4
   set arps 3
   set arp-interval 2
   set hb-interval 1
   set hb-lost-threshold 3
   set monitor port1 port2
   set boot-time 30
end
```

Related topics

- config system interface
- config system fail-open
- config system global
- diagnose debug application hasync
- diagnose debug application hatalk
- diagnose system ha status
- diagnose system ha mac
- execute ha disconnect
- execute ha manage
- execute ha synchronize
- get system status

system hsm info

Use this command to edit the configuration that allows FortiWeb to work with SafeNet Luna SA HSM (hardware security module). The HSM integration allows FortiWeb to retrieve a per-connection, SSL session key instead of loading the local private key and certificate.

Because the HSM configuration requires you to upload a server certificate, you can create it using the web UI only. After you create the configuration in the web UI, this command allows you to edit it.

For detailed information on integrating HSM with FortiWeb, see the *FortiWeb Administration Guide*.

Before you can show or edit HSM configuration in the CLI and access HSM settings in the web UI, use the following command to enable the HSM settings:

```
config system global
   set hsm enable
```

Syntax

```
config system hsm info
   set ip <hsm_ipv4>
   set port <port_int>
   set timeout <timeout_int>
   set filename <filename_str>
   set action {register | unregister}
end
```

Variable	Description	Default
`ip <hsm_ipv4>`	Enter the IP address of the HSM.	No default.
`port <port_int>`	Enter the port where FortiWeb establishes an NTLS connection with the HSM.	`1792`
`timeout <timeout_int>`	Enter a timeout value for the connection between HSM and FortiWeb.	No default.
`filename <filename_str>`	Shows the name of the server certificate file from the HSM. You cannot edit this option using the CLI.	No default.
`action {register | unregister}`	Enter `register` to register FortiWeb as a client of the HSM.	No default.

Related topics

- `config system global`
- `config system hsm partition`
- `config system certificate local`

system hsm partition

Use this command to edit information about the partition that the FortiWeb HSM client is assigned to. The partition settings are part of the configuration that allows FortiWeb to work with SafeNet Luna SA HSM (hardware security module).

Before you can show or edit HSM configuration in the CLI and access HSM settings in the web UI, use the following command to enable the HSM settings:

```
config system global
   set hsm enable
```

For additional HSM integration settings, see `config system hsm info`.

For detailed information on integrating HSM with FortiWeb, see the *FortiWeb Administration Guide*.

Syntax

```
config system hsm partition
   edit <partition_name>
      set password <password_int>
```

```
end
```

Variable	Description	Default
<partition_name>	Enter the name of a partition that the FortiWeb HSM client is assigned to.	No default.
password <password_int>	Enter the partition password.	No default.

Related topics

- config system global
- config system hsm info
- config system certificate local

system interface

Use this command to configure:

- the network interfaces associated with the physical network ports of the FortiWeb appliance,
- VLAN subinterfaces or 802.3ad link aggregates associated with physical network interfaces

Both the network interfaces and VLAN subinterfaces can include administrative access.

You can restrict which IP addresses are permitted to log in as a FortiWeb administrator through the network interfaces and VLAN subinterfaces. For details, see config system admin.

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

You can use SNMP traps to notify you when a network interface's configuration changes, or when a link is brought down or brought up. For details, see config system snmp community.

To use this command, your administrator account's access control profile must have either w or rw permission to the netgrp area. For more information, see Permissions on page 74.

Syntax

```
config system interface
  edit <interface_name>
    set status {up | down}
    set type {aggregate | physical | vlan}
    set algorithm {layer2 | layer2_3 | layer3_4}
```

```
        set allowaccess {http https ping snmp ssh telnet FWB-manager}
        set ip6-allowaccess {http https ping snmp ssh telnet FWB-manager}
        set wccp {enable | disable}
        set description "<comment_str>"
        set interface <interface_name>
        set intf {<port_name> ...}
        set ip <interface_ipv4mask>
        [set ip6 <interface_ipv6mask>]
        set mode {static | dhcp}
        set vlanid <vlan-id_int>
        set lacp-speed {fast | slow}
        set mtu <mtu_int>
        set azure-endpoint
        [config secondaryip]
          edit <entry_index>
            set ip {interface_ipv4mask | interface_ipv6mask}
          next
        end
    next
end
```

Variable	Description	Default
`<interface_name>`	Type the name of a network interface. The maximum length is 15 characters.	No default.
`status {up | down}`	Enable (select `up`) to bring up the network interface so that it is permitted to receive and/or transmit traffic. **Note:** This administrative status from this command is **not** the same as its detected physical link status. For example, even though you have used config system interface to configure port1 with `set status up`, if the cable is physically unplugged, `diagnose hardware nic list port1` may indicate correctly that the link is down (`Link detected: no`).	`up`

Variable	Description	Default
`algorithm {layer2 | layer2_3 | layer3_4}`	Select the connectivity layers that will be considered when distributing frames among the aggregated physical ports. • **layer2** — 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. • **layer2_3** — 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. • **layer3_4** — 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.	layer2

Variable	Description	Default
allowaccess {http https ping snmp ssh telnet FWB-manager}	Type the IPv4 protocols that will be permitted for administrative connections to the network interface or VLAN subinterface. Separate each protocol with a space. To remove from or add to the list of permitted administrative access protocols, retype the entire list. • ping — Allow ICMP ping responses from this network interface. • http — Allow HTTP access to the web UI. **Caution:** HTTP connections are **not** secure and can be intercepted by a third party. To reduce risk to the security of your FortiMail appliance, enable this option only on network interfaces connected directly to your management computer. • https — Allow secure HTTP (HTTPS) access to the web UI. • snmp — Allow SNMP access. For more information, see config system snmp community. **Note:** This setting only configures which network interface will **receive** SNMP queries. To configure which network interface will **send** traffic, see config system snmp community. • ssh — Allow SSH access to the CLI. • telnet — Allow Telnet access to the CLI. **Caution:** Telnet connections are **not** secure. • FWB-manager — Allow FortiWeb Manager to use this interface to administer this appliance. **Caution:** Enable administrative access only on network interfaces or VLAN subinterfaces that are connected to trusted private networks or directly to your management computer. If possible, enable only secure administrative access protocols such as HTTPS or SSH. Failure to restrict administrative access could compromise the security of your FortiWeb appliance. Consider allowing ping only when troubleshooting.	ping https ssh

Variable	Description	Default
`ip6-allowaccess {http https ping snmp ssh telnet FWB-manager}`	Type the IPv6 protocols that will be permitted for administrative connections to the network interface or VLAN subinterface. Separate each protocol with a space. To remove from or add to the list of permitted administrative access protocols, retype the entire list. • `ping` — Allow ICMP ping responses from this network interface. • `http` — Allow HTTP access to the web UI. **Caution:** HTTP connections are **not** secure and can be intercepted by a third party. To reduce risk to the security of your FortiMail appliance, enable this option only on network interfaces connected directly to your management computer. • `https` — Allow secure HTTP (HTTPS) access to the web UI. • `snmp` — Allow SNMP access. For more information, see `config system snmp community`. **Note:** This setting only configures which network interface will **receive** SNMP queries. To configure which network interface will **send** traffic, see `config system snmp community`. • `ssh` — Allow SSH access to the CLI. • `telnet` — Allow Telnet access to the CLI. **Caution:** Telnet connections are **not** secure. • `FWB-manager` — Allow FortiWeb Manager to use this interface to administer this appliance. **Caution:** Enable administrative access only on network interfaces or VLAN subinterfaces connected to trusted private networks or directly to your management computer. If possible, enable only secure administrative access protocols such as HTTPS or SSH. Failure to restrict administrative access could compromise the security of your FortiWeb appliance. Consider allowing ping only when troubleshooting.	`ping`
`wccp {enable | disable}`	Specify whether FortiWeb uses the interface to communicate with a FortiGate unit configured as a WCCP server. Available only when the operation mode is WCCP.	`disable`
`description "<comment_str>"`	Type a description or other comment. If the comment is more than one word or contains an apostrophe, surround the comment with double quotes (`"`). The maximum length is 63 characters.	No default.

Variable	Description	Default
`interface <interface_name>`	Type the name of the network interface with which the VLAN subinterface will be associated. The maximum length is 15 characters. This field is available only if `type` is `vlan`.	No default.
`intf {<port_name> ...}`	Type the names of 2 physical network interfaces or more that will be combined into the aggregate link. Only physical network interfaces may be aggregated. The maximum length is 15 characters each. This field is available only if `type` is `vlan`.	No default.
`ip <interface_ipv4mask>`	Type the IPv4 address and netmask of the network interface, if any. The IP address must be on the same subnet as the network to which the interface connects. Two network interfaces cannot have IP addresses on the same subnet. The default setting for port1 is `192.168.1.99` with a netmask of 255.255.255.0. Other ports have no default.	Varies by the interface.
`ip6 <interface_ipv6mask>`	Type the IPv6 address and netmask of the network interface, if any. The IP address must be on the same subnet as the network to which the interface connects. Two network interfaces cannot have IP addresses on the same subnet.	`::/0`
`lacp-speed {fast | slow}`	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: • **SLOW** — Every 30 seconds. • **FAST** — Every 1 second. **Note:** 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.	`slow`
`type {aggregate | physical | vlan}`	Indicates whether the interface is directly associated with a physical network port, or is instead a VLAN subinterface or link aggregate. The default varies by whether you are editing a network interface associated with a physical port (`physical`) or creating a new subinterface/aggregate (`vlan` or `aggregate`).	Varies by the interface.

Variable	Description	Default
`mode {static | dhcp}`	Specify whether the interface obtains its IPv4 address and netmask using DHCP. You can configure only one network interface to acquire its address via DHCP.	`static`
`vlanid <vlan-id_int>`	Type the VLAN ID of packets that belong to this VLAN subinterface. • If one physical network port (that is, a VLAN trunk) will handle multiple VLANs, create multiple VLAN subinterfaces on that port, one for each VLAN ID that will be received. • If multiple, different physical network ports will handle the same VLANs, on each of the ports, create VLAN subinterfaces that have the same VLAN IDs. The VLAN ID is part of the tag that is inserted into each Ethernet frame in order to identify traffic for a specific VLAN. VLAN header addition is handled automatically, and does not require that you adjust the maximum transmission appliance (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 either of the transparent modes would typically add or remove a tag when forwarding traffic among members of the VLAN, but would **not** route tagged traffic to a different VLAN ID. In contrast, a FortiWeb 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 WSDL-based routing. For the maximum number of interfaces, including VLAN subinterfaces, see the *FortiWeb Administration Guide*. This field is available only when `type` is `vlan`. The valid range is between 1 and 4094 and must match the VLAN ID added by the IEEE 802.1q-compliant router or switch connected to the VLAN subinterface.	`0`
`<entry_index>`	Type the index number of the individual entry in the table.	No default.

Variable	Description	Default
`ip {interface_ipv4mask | interface_ipv6mask}`	Type an additional IPv4 or IPv6 address and netmask for the network interface. Available only when `ip-src-balance` or `ip6-src-balance` is enabled. For more information, see `config system network-option`.	No default.
`mtu <mtu_int>`	Enter the maximum transmission unit (MTU) that the interface supports. Valid values are 512 to 9216 (for IPv4) or 1280 to 9216 (for IPv6). You cannot specify an MTU for a VLAN interface that is larger than the MTU of the corresponding physical interface.	`1500`
`azure-endpoint`	A setting related to FortiWeb-VM on the Microsoft Azure cloud computing platform. You cannot edit this setting.	No default.

Example

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

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

Example

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

```
config system interface
   edit "vlan_100"
      set type vlan
      set ip 10.0.1.1 255.255.255.0
      set status up
      set vlanid 100
      set interface port1
   next
end
```

Related topics

- config system v-zone
- config router static
- config server-policy vserver
- config system snmp community
- config system admin
- config system ha
- config system network-option
- execute ping
- diagnose hardware nic
- diagnose network ip
- diagnose network sniffer

system ip-detection

Use this command to configure how FortiWeb analyzes 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.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
config system ip-detection
   set share-ip-detection-level {low | medium | high}
end
```

Variable	Description	Default
`share-ip-detection-level {low | medium | high}`	Select how different packets' ID fields can be before FortiWeb detects that the IP is shared by multiple clients.	`low`

Related topics

- config system advanced

system network-option

Use this command to configure system-wide TCP connection options.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `netgrp` area. For more information, see Permissions on page 74.

Syntax

```
config system network-option
   set tcp-timestamp {enable | disable}
   set tcp-tw-recycle {enable | disable}
   set ip-src-balance {enable | disable}
   set ip6-src-balance {enable | disable}
   set tcp-buffer {default | high | max}
   set arp_ignore {enable | disable}
   set loopback-mtu <loopback-mtu_int>
   set tcp-usertimeout <tcp-usertimeout_int>
   set tcp-keepcnt <tcp-keepcnt_int>
   set tcp-keepidle <tcp-keepidle_int>
   set tcp-keepintvl <tcp-keepintvl_int>
   set loopback-tso-gso {enable | disable}
end
```

Variable	Description	Default
`tcp-timestamp {enable | disable}`	Enable to both: • verify whether clients' TCP timestamps are sequential • include TCP timestamps in packets from FortiWeb Disabling this option can be useful when multiple clients are in front of a source NAT gateway such as a FortiGate. If it applies source NAT but forwards packets to FortiWeb **without** modifying the TCP timestamp, packets received from that source IP will appear to FortiWeb to have an unstable timestamp. FortiWeb will therefore drop out-of-sequence packets. Disabling therefore prevents packets dropped due to this cause, and can improve performance in that case. **Caution:** Disabling this option affects FortiWeb's dynamic calculation of TCP retransmission timeout (RTO) and therefore round trip time (RTT). If you disable the timestamp when it is not necessary, this can result in decreased application performance.	`enable`

Variable	Description	Default
`tcp-tw-recycle {enable | disable}`	Enable to quickly recycle sockets that are ready to close (i.e. in the `TIME_WAIT` state per the TCP RFC). This option can be useful in networks with both sustained high load and bursts of new connection requests. If all sockets are busy, new connection requests may be refused. Enabling this option frees sockets more quickly. **Caution:** Enabling this option can cause issues with external load balancers and HA failover if they are not expecting the connection to close quickly. This can result in decreased application performance. Generally, it is safer to wait for sockets to safely close before they are reused.	`disable`
`ip-src-balance {enable | disable}`	Enable to allow FortiWeb to connect to the back-end servers using more than one IPv4 address. FortiWeb uses a round-robin load-balancing algorithm to distribute the connections among the available IP addresses. To specify the additional IP addresses, see `config system interface`. This option is useful for performance testing when the number of concurrent connections between FortiWeb and a back-end server exceeds the number of ports that a single IP can provide.	`disable`
`ip6-src-balance {enable | disable}`	Enable to allow FortiWeb to connect to the back-end servers using more than one IPv6 address. FortiWeb uses a round-robin load-balancing algorithm to distribute the connections among the available IP addresses. To specify the additional IP addresses, see `config system interface`.	`disable`
`tcp-buffer {default | high | max}`	Specify `high` or `max` to increase the size of the TCP buffer. This option is useful when amount of traffic between a server pool member and FortiWeb is significantly larger than traffic between FortiWeb and the client.	`default`
`arp_ignore {enable | disable}`	Specify how FortiWeb responds to ARP requests. • `disable` – Reply for any local target IP address, configured on any interface. • `enable` – Reply only if the target IP address is local address configured on the incoming interface.	`disable`

Variable	Description	Default
`loopback-mtu <loopback-mtu_int>`	If the operation mode is true transparent proxy, specify a global MTU for v-zones. **Caution:** If this value is smaller than a v-zone's MTU, this value replaces the larger value in the v-zone configuration. Available only when the operation mode is true transparent proxy.	`65536`
`tcp-usertimeout <tcp-usertimeout_int>`	Enter how long FortiWeb waits before it closes the connection with a client that is not sending any data or responding with ACK to keepalive packets, in seconds.	`120`
`tcp-keepcnt <tcp-keepcnt_int>`	Used only if no value is specified for `tcp-usertimeout`. Fortinet recommends that you always specify a `tcp-usertimeout` value.	`3`
`tcp-keepidle <tcp-keepidle_int>`	Enter how long FortiWeb waits before it sends a client or server that keeps a connection with FortiWeb open without sending data a keepalive packet, in seconds.	`60`
`tcp-keepintvl <tcp-keepintvl_int>`	Enter how often FortiWeb sends a keepalive packet to a client that keeps a connection open without sending data, in seconds.	`20`
`loopback-tso-gso {enable | disable}`	Used for debugging.	`disable`

Example

This example assigns additional IP addresses to port1. FortiWeb uses a round-robin load-balancing algorithm to distribute connections to back-end servers among the available IP addresses.

```
config system network-option
   set ip-src-balance enable
end

config system interface
   edit "port1"
      set type physical
      set ip 192.168.183.71/24
      set allowaccess https ping ssh snmp http telnet
      config secondaryip
         edit 1
            set ip 192.168.183.72/24
         next
         edit 2
            set ip 192.168.183.73/24
         next
      end
```

```
    next
end
```

Related topics

- config system interface
- execute ping
- diagnose network ip
- diagnose network sniffer

system raid

Use this command to configure the RAID level.

Currently, only RAID level 1 is supported, and only on the following models shipped with FortiWeb 4.0 MR1 or later:

- FortiWeb-1000B
- FortiWeb-1000C
- FortiWeb-1000D
- FortiWeb-3000C
- FortiWeb-3000D
- FortiWeb-3000E
- FortiWeb-4000C
- FortiWeb-4000D
- FortiWeb-4000E

On older appliances that have been upgraded to FortiWeb 4.0 MR1, RAID cannot be activated.

Back up the data regularly. RAID is not a substitute for regular backups. RAID 1 (mirroring) is designed to improve hardware fault tolerance, but cannot negate all risks.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

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

Variable	Description	Default
`level {raid1}`	Type the RAID level. Currently, only RAID level 1 is supported.	`raid1`

Example

This example sets RAID level 1.

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

Related topics

- `execute create-raid level`
- `execute create-raid rebuild`
- `diagnose hardware raid list`

system replacemsg

Use this command to customize the following FortiWeb HTML pages:

- Pages that FortiWeb presents to clients when it authenticates users.

  FortiWeb uses these pages when you configure a site publishing configuration to use HTML form authentication for its client authentication method. For more information, see `config waf site-publish-helper rule`.
- The error page FortiWeb uses to respond to an HTTP request that violates a policy that responds to violations with the action alert and deny or period block.
- The “Server Unavailable!” page that FortiWeb returns to the client when none of the server pool members are available either because they are disabled or in maintenance more, or they have failed the configured health check.

When you specify the HTML code for the web pages using the `buffer` setting, you enter the complete HTML code with changes, even if you are only changing a word or fixing a typographical error. The web UI provides a more convenient editing method that allows you to see the effect of your changes as you edit.

FortiWeb uses these pages for all server policies. If you require a page content that is customized for a specific policy, create an ADOM that contains the custom pages for that policy.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
config system replacemsg
   edit {url-block | server-inaccessible | login | token | rsa-login | rsa-
       challenge | pre-login-disclaimer}
      set buffer <buffer_str>
      set code <code_int>
      set set format {html | none | text}
      set set group {alert | site-publish}
      set set header {8 bit | HTTP | no header type}
end
```

Variable	Description	Default
`{url-block | server-inaccessible | login | token | rsa-login | rsa-challenge | pre-login-disclaimer}`	Enter one of the following options to specify the page to modify: • url-block — Attack block page • server-inaccessible — Server unavailable message • login — Authentication login page • token — Token authentication page • rsa-login — RSA SecurID authentication page • rsa-challenge — RSA SecurID challenge page • pre-login-disclaimer — a login disclaimer message for administrators logging in to FortiWeb	No default
`buffer <buffer_str>`	Enter the HTML content for the page. Because the code for an web page is usually more than one word and contains special characters, surround it with double quotes (").	Preset HTML content
`code <code_int>`	If you are editing the `url-block` item, specify the HTTP page return code as an integer. You cannot edit this setting for other HTML pages.	`500`
`set format {html | none | text}`	Specifies the format of the replacement message. Currently, all messages are HTML. Cannot be changed from the default.	`html`
`set group {alert | site-publish}`	Specifies whether the replacement page is used for security features (blocking and server unavailable) or site publishing feature. Cannot be changed from the default.	`alert` (`url-block`, `server-inaccessible`) site-publish (`login`, `token`, `rsa-login`, `rsa-challenge`)
`set header {8 bit | HTTP | no header type}`	Specifies the header type for the message. Cannot be changed from the default.	`HTTP`

Related topics

- `config system replacemsg-image`

system replacemsg-image

Use this command to add images that the FortiWeb HTML web pages can use. These pages are the ones that FortiWeb uses for blocking, authentication, and unavailable servers.

You cannot edit the images that FortiWeb provides by default.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
config system replacemsgimage
   edit <image_name>
      set image-type {gif | jpg | png | tiff}
      set image-base64 <image_code>
end
```

Variable	Description	Default
`<image_name>`	Specify the name of the image to add.	No default
`image-type {gif | jpg | png | tiff}`	Specify the image file format of the image to add.	No default
`image-base64 <image_code>`	Specify the HTTP page return code as clear text, Base64-encoded. Ensure the value has the following properties: • Its length is divisible by 4 (a rule of Base64 encoding) • It begins with characters that identify its format (for example, R0lGO for GIF, iVBORw0K for PNG) • The format matches the value of `image-type`	No default

Related topics

- `config system replacemsg`

system settings

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

You will usually set the operation mode once, during installation. Exceptions include if you install the FortiWeb appliance in offline protection mode for evaluation purposes, before deciding to switch to another mode for more feature support in a permanent deployment.

Back up your configuration before changing the operation mode. Changing modes deletes any policies not applicable to the new mode, TCP SYN flood protection settings, all static routes, all V-zone (bridge) IPs, and all VLANs. You 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.

The physical topology must match the operation mode. You may need to re-cable your deployment after changing this setting. For details, see the *FortiWeb Installation Guide*.

There are four operation modes:

- **Reverse proxy** — Requests are destined for a virtual server's network interface and IP address on the FortiWeb appliance. The FortiWeb appliance applies the first applicable policy, then forwards permitted traffic to a real web server. The FortiWeb appliance logs, blocks, or modifies violations according to the matching policy and its protection profile. **Most features are supported.**
- **Offline protection** — Requests are destined for a real web server instead of the FortiWeb appliance; traffic is duplicated to the FortiWeb through a span port. The FortiWeb appliance monitors traffic received on the virtual server'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. The FortiWeb appliance 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 to the web server and client to attempt to terminate the connection. It does **not** otherwise modify traffic. (It cannot, for example, apply SSL, load-balance connections, or support user authentication.)

Unlike in reverse proxy mode or true transparent proxy mode, actions other than **Alertcannot** 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 paths.

Most organizations do **not** permanently deploy their FortiWeb appliances in offline protection mode. Instead, they will use offline protection as a way to learn about their web servers' protection requirements and to form some of the appropriate configuration during a transition period, after which they will switch to one of the operation modes that places the appliance inline between all clients and all 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 some protection features that cannot be supported in a span port topology used with offline detection.

- **True transparent proxy** — Requests are destined for a real web server instead of the FortiWeb appliance. The FortiWeb appliance **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. The FortiWeb appliance logs, blocks, or modifies violations according to the matching policy and its protection profile. **No changes to the IP address scheme of the network are required.** This mode supports user authentication via HTTP but **not** HTTPS.
- **Transparent inspection** — Requests are destined for a real web server instead of the FortiWeb appliance. The FortiWeb appliance **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. The FortiWeb appliance logs or blocks traffic according to the matching policy and its protection profile, but does **not** otherwise modify it. (It cannot, for example, apply 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.

The default operation mode is reverse proxy.

Feature support varies by operation mode. For details, see the *FortiWeb Administration Guide*.

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
config system settings
   set opmode {offline-protection | reverse-proxy | transparent | transparent-
       inspection | wccp}
   set gateway <router_ipv4>
   set stop-guimonitor {enable | disable}
   set enable-cache-flush {enable | disable}
   set fast-forward {enable | disable}
end
```

Variable	Description	Default
`opmode {offline-protection | reverse-proxy | transparent | transparent-inspection | wccp}`	Select the operation mode of the FortiWeb appliance. If you have not yet adjusted the physical topology to suit the new operation mode, see the *FortiWeb Administration Guide*. You may also need to reconfigure IP addresses, VLANs, static routes, bridges, policies, TCP `SYN` flood prevention, and virtual servers, and on your web servers, enable or disable SSL. **Note:** If you select `offline-protection`, you can configure the port from which TCP `RST` (reset) commands are sent to block traffic that violates a policy. For details, see block-port <port_int>.	`reverse-proxy`
`gateway <router_ipv4>`	Type the IPv4 address of the default gateway. This setting is visible only if `opmode` is either `transparent` or `transparent-inspection`. FortiWeb will use the `gateway` setting to create a corresponding static route under router static with the first available index number. Packets will egress through `port1`, the hard-coded management network interface for the transparent operation modes.	`none`
`stop-guimonitor {enable | disable}`	Enable to configure FortiWeb to stop checking whether the process that generates the web UI (httpsd) is defunct (that is, a defunct or zombie process). In some cases, a process that has completed execution can still have an entry in the process table, which can create a resource leak. When this setting is disabled, FortiWeb checks the process and stops and reloads the web UI if it determines that the process is defunct.	`disable`
`enable-cache-flush {enable | disable}`	Enable to configure FortiWeb to clear its cache memory every 45 minutes and generate an event log message for the action.	`disable`
`fast-forward {enable | disable}`	Specifies whether FortiWeb activity is restricted to load balancing.	`disable`

Related topics

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

system snmp community

Use this command to configure the FortiWeb appliance's SNMP agent to belong to an SNMP version 1 or 2c community, and to select which events cause the FortiWeb appliance to generate SNMP traps.

To configure the SNMP agent as a member of a SNMP version 3 community, see `config system snmp user`.

The FortiWeb appliance's simple network management protocol (SNMP) agent allows queries for system information can send traps (alarms or event messages) to the computer that you designate as its SNMP manager. In this way you can use an SNMP manager to monitor the FortiWeb appliance. You can add the IP addresses of up to eight SNMP managers to each community, which designate the destination of traps and which IP addresses are permitted to query the FortiWeb appliance.

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.

You can add up to three SNMP communities. Each community can have a different configuration for queries and traps, and the set of events which trigger a trap. Use SNMP traps to notify the SNMP manager of a wide variety of types of events. Event types range from basic system events, such as high usage of resources, to when an attack type is detected or a specific rule is enforced by a policy.

Before you can use SNMP, you must activate the FortiWeb appliance's SNMP agent (see `config system snmp sysinfo`) and add it as a member of at least one community. You must also enable SNMP access on the network interface through which the SNMP manager will connect. (See `config system interface`.)

On 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 the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
config system snmp community
   edit <community_index>
      set status {enable | disable}
      set name <community_str>
      set events {cpu-high | intf-ip | log-full | mem-low | netlink-down-
          status | netlink-up-status | policy-start | policy-stop | pserver-
          failed | sys-ha-hbfail | sys-mode-change | waf-access-attack | waf-
          amethod-attack | waf-blogin-attack |waf-hidden-fields | waf-pvalid-
          attack | waf-signature-detection | waf-url-access-attack | waf-spage-
          attack}
      set query-v1-port <port_int>
      set query-v1-status {enable | disable}
      set query-v2c-port <port_int>
      set query-v2c-status {enable | disable}
      set trap-v1-lport <port_int>
      set trap-v1-rport <port_int>
      set trap-v1-status {enable | disable}
      set trap-v2c-lport <port_int>
```

```
        set trap-v2c-rport <port_int>
        set trap-v2c-status {enable | disable}
        config hosts
           edit <snmp-manager_index>
              set ip {manager_ipv4 | manager_ipv6>
           next
        end
     next
  end
```

Variable	Description	Default
<community_index>	Type the index number of a community to which the FortiWeb appliance belongs. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
status {enable | disable}	Enable to activate the community. This setting takes effect only if the SNMP agent is enabled. For details, see config system snmp sysinfo.	disable
name <community_str>	Type the name of the SNMP community to which the FortiWeb appliance and at least one SNMP manager belongs. The maximum length is 35 characters. 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.	No default.

Variable	Description	Default
events {cpu-high | intf-ip | log-full | mem-low | netlink-down-status | netlink-up-status | policy-start | policy-stop | pserver-failed | sys-ha-hbfail | sys-mode-change | waf-access-attack | waf-amethod-attack | waf-blogin-attack |waf-hidden-fields | waf-pvalid-attack | waf-signature-detection | waf-url-access-attack | waf-spage-attack}	Type one or more of the following SNMP event names in order to cause the FortiWeb appliance to send traps when those events occur. Traps will be sent to the SNMP managers in this community. Also enable traps. • cpu-high — CPU usage has exceeded 80%. • intf-ip — A network interface's IP address has changed. See config system interface. • log-full — Local log disk space usage has exceeded 80%. If the space is consumed and a new log message is triggered, the FortiWeb appliance will either drop it or overwrite the oldest log message, depending on your configuration. See config log disk. • mem-low — Memory (RAM) usage has exceeded 80%. • netlink-down-status — A network interface has been brought down (disabled). This could be due to either an administrator changing the network interface's settings, or due to HA executing a failover. • netlink-up-status — A network interface has been brought up (enabled).This could be due to either an administrator changing the network interface's settings, or due to HA executing a failover. • policy-start — A policy was enabled. See config server-policy policy. • policy-stop — A policy was disabled. See config server-policy policy. • pserver-failed — A server health check has determined that a physical server that is a member of a server farm is now unavailable. See config server-policy policy. • sys-ha-hbfail — An HA failover is occurring. See config system ha. • sys-mode-change — The operation mode was changed. See config system settings.	No default.

Variable	Description	Default
	• `waf-access-attack` — FortiWeb enforced a page access rule. See `config waf page-access-rule`. • `waf-amethod-attack` — FortiWeb enforced an allowed methods restriction. See `config waf web-protection-profile inline-protection`, `config waf web-protection-profile offline-protection`, and `config waf allow-method-exceptions`. • `waf-blogin-attack` — FortiWeb detected a brute force login attack. See `config waf brute-force-login`. • `waf-hidden-fields` — FortiWeb detected a hidden fields attack. • `waf-pvalid-attack` — FortiWeb enforced an input/parameter validation rule. See `config waf parameter-validation-rule`. • `waf-signature-detection` — FortiWeb enforced a signature rule. See `config waf signature`. • `waf-url-access-attack` — FortiWeb enforced a URL access rule. See `config waf url-access url-access-rule`. • `waf-spage-attack` — FortiWeb enforced a start page rule. See `config waf start-pages`.	
`query-v1-port <port_int>`	Type the port number on which the FortiWeb appliance will listen for SNMP v1 queries from the SNMP managers of the community. The valid range is from 1 to 65,535.	`161`
`query-v1-status {enable | disable}`	Enable to respond to queries using the SNMP v1 version of the SNMP protocol.	`enable`
`query-v2c-port <port_int>`	Type the port number on which the FortiWeb appliance will listen for SNMP v2c queries from the SNMP managers of the community. The valid range is from 1 to 65,535.	`161`
`query-v2c-status {enable | disable}`	Enable to respond to queries using the SNMP v2c version of the SNMP protocol.	`enable`
`trap-v1-lport <port_int>`	Type the port number that will be the source (also called local) port number for SNMP v1 trap packets. The valid range is from 1 to 65,535.	`162`
`trap-v1-rport <port_int>`	Type the port number that will be the destination (also called remote) port number for SNMP v1 trap packets. The valid range is from 1 to 65,535.	`162`

Variable	Description	Default
`trap-v1-status {enable | disable}`	Enable to send traps using the SNMP v1 version of the SNMP protocol.	`enable`
`trap-v2c-lport <port_int>`	Type the port number that will be the source (also called local) port number for SNMP v2c trap packets. The valid range is from 1 to 65,535.	`162`
`trap-v2c-rport <port_int>`	Type the port number that will be the destination (also called remote) port number for SNMP v2c trap packets. The valid range is from 1 to 65,535.	`162`
`trap-v2c-status {enable | disable}`	Enable to send traps using the SNMP v2c version of the SNMP protocol.	`enable`
`<snmp-manager_index>`	Type the index number of an SNMP manager for the community. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
`ip {manager_ipv4 | manager_ipv6>`	Type the IP address of the SNMP manager that, if traps and/or queries are enabled in this community: • will receive traps from the FortiWeb appliance • will be permitted to query the FortiWeb appliance SNMP managers have read-only access. To allow any IP address using this SNMP community name to query the FortiWeb appliance, enter `0.0.0.0`. **Note:** Entering `0.0.0.0` effectively disables traps if there are no other host IP entries, because there is no specific destination for trap packets. If you do not want to disable traps, you must add at least one other entry that specifies the IP address of an SNMP manager.	No default.

Example

For an example, see `config system snmp sysinfo`.

Related topics

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

system snmp sysinfo

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

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

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 the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

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

Variable	Description	Default
`contact-info <contact_str>`	Type the contact information for the administrator or other person responsible for this FortiWeb appliance, such as a phone number or name. The contact information can contain only letters (a-z, A-Z), numbers, hyphens (-) and underscores (_). The maximum length is 35 characters.	No default.
`description <description_str>`	Type a description of the FortiWeb appliance. The string can contain only letters (a-z, A-Z), numbers, hyphens (-) and underscores (_). The maximum length is 35 characters.	No default.
`location <location_str>`	Type the physical location of the FortiWeb appliance. The string can contain only letters (a-z, A-Z), numbers, hyphens (-) and underscores (_). The maximum length is 35 characters.	No default.
`status {enable | disable}`	Enable to activate the SNMP agent, enabling the FortiWeb appliance to send traps and/or receive queries for the communities in which you have enabled queries and/or traps. This setting enables queries only if SNMP administrative access is enabled on one or more network interfaces. For details, see `config system interface`.	`disable`

Example

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

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

```
config system snmp sysinfo
   set contact-info 'admin_example_com'
   set description 'FortiWeb-1000B'
   set location 'Rack_2'
   set status enable
end
config system snmp community
   edit 1
      set status enable
      set name public
      set events {cpu-high mem-low sys-ha-hbfail}
      set query-v1-status disable
      set query-v2c-port 161
      set query-v2c-status enable
      set trap-v1-status disable
      set trap-v2c-lport 162
      set trap-v2c-rport 162
      set trap-v2c-status enable
      config hosts
         edit 1
            set interface port3
            set ip 172.168.1.20
         next
      end
   next
end
config system interface
   edit port3
      set allowaccess ping https ssh snmp
   next
end
```

Related topics

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

system snmp user

Use this command to configure the FortiWeb appliance's SNMP agent to belong to an SNMP version 3 community, and to select which events cause the FortiWeb appliance to generate SNMP traps.

To configure the SNMP agent as a member of a SNMP version version 1 or 2c community and for more information on the SNMP agent, see config system snmp community.

To use this command, your administrator account's access control profile must have either w or rw permission to the sysgrp area. For more information, see Permissions on page 74.

Syntax

```
config system snmp user
   edit name <community_str>
      set status {enable | disable}
      set security-level { noauthnopriv | authnopriv | authpriv >
      set auth-proto {sha1 | md5}
      set auth-pwd <auth-password_str>
      set priv-proto {aes | des}
      set priv-pwd <priv-password_str>
      set query-status {enable | disable}
      set query-port <port_int>
      set trap-status {enable | disable}
      set trapport-local <port_int>
      set trapport-remote <port_int>
      set trapevent {cpu-high | intf-ip | log-full | mem-low | netlink-down-
          status | netlink-up-status | policy-start | policy-stop | pserver-
          failed | sys-ha-hbfail | sys-mode-change | waf-access-attack | waf-
          amethod-attack | waf-blogin-attack |waf-hidden-fields | waf-pvalid-
          attack | waf-signature-detection | waf-url-access-attack | waf-spage-
          attack}
      config hosts
         edit <snmp-user_index>
            set ip <manager_ipv4>
         next
      end
   next
end
```

Variable	Description	Default
`name <community_str>`	Type the name of the SNMP community to which the FortiWeb appliance and at least one SNMP manager belongs. The maximum length is 35 characters. The FortiWeb appliance does not respond to SNMP managers whose query packets do not contain a matching community name. Similarly, trap packets from the FortiWeb appliance include the community name, and an SNMP manager may not accept the trap if its community name does not match.	No default.
`status {enable | disable}`	Enable to activate the community. This setting takes effect only if the SNMP agent is enabled. For details, see `config system snmp sysinfo`.	`disable`

Variable	Description	Default
`security-level { noauthnopriv | authnopriv | authpriv >`	Type the security level. • `noauthnopriv` — No additional authentication or encryption compared to SNMP v1 and v2. • `authnopriv` — The SNMP manager needs to provide the password specified in this community configuration. Also specify `auth-proto` and `auth-pwd`. • `authpriv` — Adds both authentication and encryption. Also specify `auth-proto`, `auth-pwd`, `priv-proto`, and `priv-pwd`. Ensure that the SNMP manager and FortiWeb use the same protocols and passwords.	No default.
`auth-proto {sha1 | md5}`	If the `security-level` option includes authentication, specify the authentication protocol.	`sha1`
`auth-pwd <auth-password_str>`	If the `security-level` option includes authentication, specify the authentication password.	No default.
`priv-proto {aes | des}`	If the `security-level` option is `authprivuser_name`, specify the encryption protocol.	`aes`
`priv-pwd <priv-password_str>`	If the `security-level` option is `authprivuser_name`, specify the encryption password.	No default.
`query-status {enable | disable}`	Enable to respond to queries using the SNMP v3 version of the SNMP protocol.	`enable`
`query-port <port_int>`	Type the port number on which the FortiWeb appliance listens for SNMP v3 queries from the SNMP managers of the community. The valid range is from 1 to 65,535.	`161`
`trap-status {enable | disable}`	Enable to send traps using the SNMP v3 version of the SNMP protocol.	`enable`
`trapport-local <port_int>`	Type the port number that is the source (also called local) port number for SNMP v3 trap packets. The valid range is from 1 to 65,535.	`162`
`trapport-remote <port_int>`	Type the port number that is the destination (also called remote) port number for SNMP v3 trap packets. The valid range is from 1 to 65,535.	`162`

Variable	Description	Default
`trapevent {cpu-high | intf-ip | log-full | mem-low | netlink-down-status | netlink-up-status | policy-start | policy-stop | pserver-failed | sys-ha-hbfail | sys-mode-change | waf-access-attack | waf-amethod-attack | waf-blogin-attack |waf-hidden-fields | waf-pvalid-attack | waf-signature-detection | waf-url-access-attack | waf-spage-attack}`	Type the name of one or more the SNMP events. When FortiWeb detects the specified events, it sends traps to the SNMP managers in this community. Also enable `trap-status`. • `cpu-high` — CPU usage has exceeded 80%. • `intf-ip` — A network interface's IP address has changed. See `config system interface`. • `log-full` — Local log disk space usage has exceeded 80%. If the space is consumed and a new log message is triggered, the FortiWeb appliance will either drop it or overwrite the oldest log message, depending on your configuration. See `config log disk`. • `mem-low` — Memory (RAM) usage has exceeded 80%. • `netlink-down-status` — A network interface has been brought down (disabled). This could be due to either an administrator changing the network interface's settings, or due to HA executing a failover. • `netlink-up-status` — A network interface has been brought up (enabled).This could be due to either an administrator changing the network interface's settings, or due to HA executing a failover. • `policy-start` — A policy was enabled. See `config server-policy policy`. • `policy-stop` — A policy was disabled. See `config server-policy policy`. • `pserver-failed` — A server health check has determined that a physical server that is a member of a server farm is now unavailable. See `config server-policy policy`. • `sys-ha-hbfail` — An HA failover is occurring. See `config system ha`. • `sys-mode-change` — The operation mode was changed. See `config system settings`.	No default.

Variable	Description	Default
	• `waf-access-attack` — FortiWeb enforced a page access rule. See `config waf page-access-rule`. • `waf-amethod-attack` — FortiWeb enforced an allowed methods restriction. See `config waf web-protection-profile inline-protection`, `config waf web-protection-profile offline-protection`, and `config waf allow-method-exceptions`. • `waf-blogin-attack` — FortiWeb detected a brute force login attack. See `config waf brute-force-login`. • `waf-hidden-fields` — FortiWeb detected a hidden fields attack. • `waf-pvalid-attack` — FortiWeb enforced an input/parameter validation rule. See `config waf parameter-validation-rule`. • `waf-signature-detection` — FortiWeb enforced a signature rule. See `config waf signature`. • `waf-url-access-attack` — FortiWeb enforced a URL access rule. See `config waf url-access url-access-rule`. • `waf-spage-attack` — FortiWeb enforced a start page rule. See `config waf start-pages`.	
`<snmp-user_index>`	Type the index number of an SNMP user for the community. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
`ip <manager_ipv4>`	Type the IP address of the SNMP manager that can do the following when you enable traps, queries, or both in this community: • Receive traps from the FortiWeb appliance • Query the FortiWeb appliance SNMP managers have read-only access. To allow any IP address using this SNMP community name to query the FortiWeb appliance, enter `0.0.0.0`. **Note:** Entering `0.0.0.0` effectively disables traps if there are no other host IP entries, because there is no specific destination for trap packets. If you do not want to disable traps, add at least one other entry that specifies the IP address of an SNMP manager.	No default.

Example

For an example, see `config system snmp sysinfo`.

Related topics

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

system v-zone

Use this command to configure bridged network interfaces, also called v-zones.

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

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.

For FortiWeb-VM, you must create vSwitches **before** you can configure a bridge. See the *FortiWeb-VM Install Guide* for details.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `netgrp` area. For more information, see Permissions on page 74.

Syntax

```
config system v-zone
   edit <bridge_name>
      set interfaces {<interface_name> <interface_name> ...}
      set monitor {enable | disable}
      set mtu <mtu_int>
      set use-interface-macs {<interface_name> <interface_name> ...}
   next
end
```

Variable	Description	Default
<bridge_name>	Type the name of the bridge. The maximum length is 15 characters. To display the list of existing bridges, type: edit ?	No default.

Variable	Description	Default
`interfaces {<interface_name> <interface_name> ...}`	Type the names of two or more network interfaces that currently have no IP address of their own, nor are members of another bridge, and therefore could be members of this bridge. Separate each name with a space. The maximum length is 35 characters.	No default.
`mtu <mtu_int>`	Enter the maximum transmission unit (MTU) that the bridge supports. When you specify the MTU for a bridge, FortiWeb automatically sets the MTU for the v-zone members to the same value. Valid values are 512 to 9216 (for IPv4) or 1280 to 9216 (for IPv6).	`1500`
`monitor {enable | disable}`	Specifies whether FortiWeb automatically brings down all members of this v-zone if one member goes down.	`disable`
`use-interface-macs {<interface_name> <interface_name> ...}`	Enter the names of network interfaces that are members of the bridge and send and transmit traffic using the MAC address of their corresponding FortiWeb network interface. When the operation mode is true transparent proxy, by default, traffic to the back-end servers preserves the MAC address of the source. If you are using FortiWeb with front-end load balancers that are in a high availability cluster that uses multiple bridges, this mechanism can cause switching problems on failover. When the v-zone uses the MAC address of the FortiWeb network interface instead, a failover does not interrupt the flow of traffic. Available only when the operation mode is true transparent proxy.	No default.

Example

This example configures a true bridge between port3 and port4. The bridge has no virtual network interface, and so it cannot respond to pings.

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

Related topics

- config system interface
- config system settings

system wccp

Use this command to configure FortiWeb as a Web Cache Communication Protocol (WCCP) client. This configuration allows a FortiGate configured as a WCCP server to redirect HTTP and HTTPS traffic to FortiWeb for inspection.

If your WCCP configuration includes multiple WCCP clients, the WCCP server can balance the traffic load among the clients. In addition, it detects when a client fails and redirects sessions to clients that are still available.

WCCP was originally designed to provide web caching with load balancing and fault tolerance and is described by the Web Cache Communication Protocol Internet draft.

This feature requires the operation mode to be WCCP. See system settings on page 290.

For information on connecting and configuring your network devices for WCCP mode, see the *FortiWeb Administration Guide*.

For detailed information on configuring FortiGate and other Fortinet devices to act as a WCCP service group, see the FortiGate WCCP topic in the *FortiOS Handbook*.

Syntax

```
config system wccp
  edit service-id <service-id_int>
    set cache-id <cache-id_ipv4>
    set router-list <router-list_ipv4>
    set group-address <group-address_ipv4>
    set authentication {enable | disable}
    set password <passwd_str>
    set cache-engine-method {GRE | L2}
    set ports <ports_int>
    set primary-hash [src-ip | dst-ip | src-port | dst-port}
    set priority <priority_int>
    set protocol <priority_int>
    set assignment-weight <assignment-weight_int>
    set assignment-bucket-format {ciso-implementation | wccp-v2}
    set return-to-sender {enable | disable}
  end
```

Variable	Description	Default
service-id <service-id_int>	Enter the service ID of the WCCP service group that this WCCP client belongs to. For HTTP traffic, the service ID is 0. For other types of traffic (for example, HTTPS), the valid range is 51 to 255. (Do not use 1 to 50, which are reserved by the WCCP standard.)	51

Variable	Description	Default
`cache-id <cache-id_ipv4>`	Enter the IP address of the FortiWeb interface that communicates with the WCCP server. Ensure that the WCCP protocol is enabled for the specified network interface. See `config system settings`.	No default.
`router-list <router-list_ipv4>`	Enter the IP addresses of the WCCP servers in the WCCP service group. You can specify up to 8 servers. To configure more than 8 WCCP servers, use Group Address instead.	No default.
`group-address <group-address_ipv4>`	Enter the IP addresses of the clients for multicast WCCP configurations. The multicast address allows you to configure a WCCP service group with more than 8 WCCP clients. The valid range of multicast addresses is 224.0.0.0 to 239.255.255.255.	No default.
`authentication {enable | disable}`	Specify whether communication between the WCCP server and client is encrypted using the MD5 cryptographic hash function.	`disable`
`password <passwd_str>`	Enter the password used by the WCCP server and clients. All servers and clients in the group use the same password. The maximum password length is 8 characters. Available only when `authentication` is `enabled`.	No default.
`cache-engine-method {GRE | L2}`	Enter how the FortiGate unit transmits traffic to FortiWeb. • `GRE` – The WCCP server encapsulates redirected packets within a generic routing encapsulation (GRE) header. The packets also have a WCCP redirect header. • `L2` – The WCCP server overwrites the original MAC header of the IP packets and replaces it with the MAC header for the WCCP client.	`GRE`

Variable	Description	Default
`ports <ports_int>`	Enter the port numbers of the sessions that this client inspects. The valid range is 0 to 65535. Enter 0 to specify all ports.	`80`
`primary-hash [src-ip | dst-ip | src-port | dst-port}`	Enter the hashing scheme that the WCCP server uses in combination with `assignment-weight` to direct traffic, when the WCCP service group has more than one WCCP client. Specify one or more of the following values: • `src-ip` – Source IP address • `dst-ip` – Destination IP address • `src-port` – Source port • `dst-port` – Destination port	`src-ip dst-ip`
`priority <priority_int>`	Enter a value that specifies the priority that this service group has. If more than one service group is available to scan the traffic specified by `ports` and `protocol`, the WCCP server transmits all the traffic to the service group with the highest `priority` value.	`0`
`protocol <priority_int>`	Enter the protocol of the network traffic the WCCP service group transmits. For TCP sessions, enter `6`. Valid values are 0 to 255.	`6`
`assignment-weight <assignment-weight_int>`	Enter a value that the WCCP server uses in combination with `primary-hash` to direct traffic, when the WCCP service group has more than one WCCP client. The valid range is 0 to 255.	`0`
`assignment-bucket-format {ciso-implementation | wccp-v2}`	Enter the hash table bucket format for the WCCP cache engine. • `cisco-implementation` – Source IP address • `wccp-v2` – Web Cache Communication Protocol version 2	`ciso-implementation`
`return-to-sender {enable | disable}`	Specify whether FortiWeb routes traffic back to the client instead of the WCCP server.	`disable`

Example

This example configures FortiWeb as a WCCP client that belongs to the WCCP service group 52 and specifies the interface used for WCCP client functionality (172.22.80.100) and the WCCP server (172.22.80.1).

```
config system wccp
   edit service-id 52
      set cache-id 172.22.80.100
      set router-list 172.22.80.1
      set ports 80 443
      set primary-hash src-ip dst-ip
```

Related topics

- config system settings
- config system interface

user admin-usergrp

Use this command to configure LDAP or RADIUS remote authentication groups that can be used when configuring a FortiWeb administrator account.

Before you can add a remote authentication group, you must first define at least one query for either LDAP or RADIUS accounts. See config user ldap-user or config server-policy custom-application application-policy.

To use this command, your administrator account's access control profile must have either w or rw permission to the authusergrp area. For more information, see Permissions on page 74.

Syntax

```
config user admin-usergrp
   edit <group_name>
      config members
         edit <entry_index>
            set type {ldap | radius}
            set ldap-name <query_name>
            set radius-name <query_name>
         next
      end
   next
end
```

Variable	Description	Default
<group_name>	Type the name of the remote authentication group. The maximum length is 35 characters.	No default.

Variable	Description	Default
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
type {ldap | radius}	Select the protocol used for the query, either LDAP or RADIUS.	ldap
ldap-name <query_name>	Type the name of an existing LDAP account query. The maximum length is 35 characters. To display the list of existing queries, type: edit ?	No default.
radius-name <query_name>	Type the name of an existing RADIUS account query. The maximum length is 35 characters. To display the list of existing queries, type: edit ?	No default.

Example

This example creates a remote authentication group using an existing LDAP user query named LDAP Users 1. Because remote authentication groups use LDAP queries by default, the LDAP query type is not explicitly configured.

```
config user admin-usergrp
   edit "Admin LDAP"
      config members
         edit 0
            set ldap-name "LDAP Users 1"
         next
      end
   next
end
```

Related topics

- config system admin
- config user ldap-user
- config server-policy custom-application application-policy
- get system logged-users

user kerberos-user

Use this command to specify a Kerberos Key Distribution Center (KDC) that FortiWeb can use to obtain a Kerberos service ticket for web applications on behalf of clients.

Because FortiWeb determines the KDC to use based on the realm of the web application, you do not have to specify the KDC in the site publish rule.

For more information, see `config waf site-publish-helper rule` and the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For more information, see Permissions on page 74.

Syntax

```
config user kerberos-user
   edit <kdc_name>
      set realm <realm_str>
      set server <kdc-server_ip>
      set port <kdc-port_ip>
      set status <kdc_status>
   next
end
```

Variable	Description	Default
`<kdc_name>`	Enter the name of the Key Distribution Center (KDC).	No default.
`realm <realm_str>`	Enter the domain of the domain controller (DC) that the Key Distribution Center (KDC) belongs to.	No default.
`server <kdc-server_ip>`	Enter the IP address of the KDC. In most cases, the KDC is located on the same server as the DC.	No default.
`port <kdc-port_ip>`	Enter the port the KDC uses to listen for requests.	No default.
`status <kdc_status>`	Specify whether the KDC configuration is enabled.	`enable`

Related topics

- `config waf site-publish-helper rule`
- `config waf site-publish-helper keytab_file`

user ldap-user

Use this command to configure queries that can be used for remote authentication of either FortiWeb administrators or end users via an LDAP server.

To apply LDAP queries to end users, select a query in a user group that is then selected within an authentication rule, which is in turn selected within an authentication policy, which is ultimately selected within an inline protection profile used for web protection. For details, see `config user user-group`.

To apply LDAP queries to administrators, select a query in an admin group and reference that group in a system administrator configuration. For details, see `config user admin-usergrp`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For more information, see Permissions on page 74.

Syntax

```
config user ldap-user
   edit <ldap-query_name>
      set bind-type {anonymous | simple | regular}
      set common-name-id <cn-attribute_str>
      set distinguished-name <search-dn_str>
      set filter <query-filter_str>
      set group_authentication {enable | disable}
      set group_dn <group-dn_str>
      set group-type {edirectory | open-ldap | windows-ad}
      set password <bind-password_str>
      set port <port_int>
      set protocol {ldaps | starttls}
      set server <ldap_ipv4>
      set ssl-connection {enable | disable}
      set username <bind-dn_str>
   next
end
```

Variable	Description	Default
`<ldap-query_name>`	Type the name of the LDAP user query. The maximum length is 35 characters. To display the list of existing queries, type: `edit ?`	No default.
`bind-type {anonymous | simple | regular}`	Select one of the following LDAP query binding styles: • simple — Bind using the client-supplied password and a bind DN assembled from the common-name-id <cn-attribute_str>, distinguished-name <search-dn_str>, and the client-supplied user name. • `regular` — Bind using a bind DN and password that you configure in username <bind-dn_str> and password <bind-password_str>. • `anonymous` — Do not provide a bind DN or password. Instead, perform the query without authenticating. Select this option only if the LDAP directory supports anonymous queries.	`simple`

Variable	Description	Default
common-name-id <cn-attribute_str>	Type the identifier, often cn, for the common name (CN) attribute whose value is the user name. The maximum length is 63 characters. Identifiers may vary by your LDAP directory's schema.	No default.
distinguished-name <search-dn_str>	Type the distinguished name (DN) such as ou=People,dc=example,dc=com, that, when prefixed with the common name, forms the full path in the directory to user account objects. The maximum length is 255 characters.	No default.
filter <query-filter_str>	Type an LDAP query filter string, if any, that will be used to filter out results from the query's results based upon any attribute in the record set. The maximum length is 255 characters. This option is valid only when bind-type is regular.	No default.
group_authentication {enable | disable}	Enable to only include users that are members of an LDAP group. Also configure group-type {edirectory | open-ldap | windows-ad} and group_dn <group-dn_str>. This option is valid only when bind-type is regular.	enable
group_dn <group-dn_str>	Type the distinguished name of the LDAP user group, such as ou=Groups,dc=example,dc=com. The maximum length is 255 characters. This option is valid only when group_authentication is enabled.	No default.
group-type {edirectory | open-ldap | windows-ad}	Select the schema that matches your server's LDAP directory. 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. This option is valid only when group_authentication is enabled.	open-ldap
password <bind-password_str>	Type the password of the username <bind-dn_str>. The maximum length is 63 characters. 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 bind-type is anonymous or simple.	No default.

Variable	Description	Default
port <port_int>	Type the port number where the LDAP server listens. The valid range is from 1 to 65,535. The default port number varies by your selection in ssl-connection: port 389 is typically used for non-secure connections or for STARTTLS-secured connections, and port 636 is typically used for SSL-secured (LDAPS) connections.	389
protocol {ldaps | starttls}	Select whether to secure the LDAP query using LDAPS or STARTTLS. You may need to reconfigure port <port_int> to correspond to the change in protocol. This field is applicable only if ssl-connection is enable.	ldaps
server <ldap_ipv4>	Type the IP address of the LDAP server.	0.0.0.0
ssl-connection {enable | disable}	Enable to connect to the LDAP servers using an encrypted connection, then select the style of the encryption in protocol.	enable
username <bind-dn_str>	Type the bind DN, such as cn=FortiWebA,dc=example,dc=com, of an LDAP user account with permissions to query the distinguished-name <search-dn_str>. The maximum length is 255 characters. 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 bind-type is anonymous or simple.	No default.

Example

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

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

```
        set group-authentication disable
    next
end
```

Related topics

- config user user-group
- config system admin
- config user admin-usergrp

user local-user

Use this command to configure locally defined user accounts.

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

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For more information, see Permissions on page 74.

Syntax

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

Variable	Description	Default
`<local-user_name>`	Type a name that can be referenced in other parts of the configuration. To display the list of existing accounts, type: `edit ?` Do not use spaces or special characters. The maximum length is 35 characters. **Note:** This is **not** the user name that the person must provide when logging in to the CLI or web UI.	No default.
`username <user_str>`	Type the user name that the client must provide when logging in, such as `user1` or `user1@example.com`. The maximum length is 63 characters.	No default.

Variable	Description	Default
password <password_str>	Type the password for the local user account. The maximum length is 63 characters.	No default.

Example

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

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

Related topics

- config user user-group

user ntlm-user

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

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

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

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

To use this command, your administrator account's access control profile must have either w or rw permission to the authusergrp area. For more information, see Permissions on page 74.

Syntax

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

Variable	Description	Default
<ntlm-query_name>	Type the name of the NTLM user query. The maximum length is 35 characters. To display the list of existing queries, type: edit ?	No default.
port <port_int>	Type the port number where the NTLM server listens. The valid range is from 1 to 65,535.	445
server <ntlm_ipv4>	Type the IP address of the NTLM server.	No default.

Example

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

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

Related topics

- config user user-group

user radius-user

Use this command to configure RADIUS queries used to authenticate end-users and/or administrators.

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

To incorporate RADIUS users, they must be in a user group selected within an authentication rule, which is in turn selected within an authentication policy. For details, see `config server-policy custom-application application-policy`.

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 `config system accprofile`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For more information, see Permissions on page 74.

Syntax

```
config user radius-user
  edit <radius-query_name>
    set secret <password_str>
    set server <radius_ipv4>
    set server-port <port_int>
    set auth-type {default | chap | ms_chap | ms_chap_v2 | pap}
    set nas-ip <nas_ipv4>
    set secondary-secret <password_str>
    set secondary-server <radius2-ipv4>
    set secondary-server-port <port_int>
  next
end
```

Variable	Description	Default
`<radius-query_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. To display the list of existing queries, type: `edit ?` **Note:** This is the name of the query only, **not** the administrator or end-user's account name/login, which is defined by either <administrator_name> or username <user_str>.	No default.
`secret <password_str>`	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, but is allowed to be up to 63 characters.	No default.
`server <radius_ipv4>`	Type the IP address of the RADIUS server to query for users.	`0.0.0.0`

Variable	Description	Default
`server-port <port_int>`	Type the port number where the RADIUS server listens. The valid range is from 1 to 65,535.	`1812`
`auth-type {default | chap | ms_chap | ms_chap_v2 | pap}`	Type the authentication method. The `default` option uses PAP, MS-CHAP-V2, and CHAP, in that order.	`default`
`nas-ip <nas_ipv4>`	Type the NAS IP address and called station ID (see RFC 2548 Microsoft Vendor-specific RADIUS Attributes). If you do not enter an IP address, the IP address of the network interface that the FortiWeb appliance uses to communicate with the RADIUS server is applied.	`0.0.0.0`
`secondary-secret <password_str>`	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, but is allowed to be up to 63 characters.	No default.
`secondary-server <radius2-ipv4>`	Type the IP address of the secondary RADIUS server.	No default.
`secondary-server-port <port_int>`	Type the port number where the secondary RADIUS server listens. The valid range is from 1 to 65,535.	`1812`

Related topics

- `config user admin-usergrp`
- `config user user-group`

user user-group

Use this command to configure user groups.

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

Before you can configure a user group, you must first configure any local user accounts or user queries that you want to include. For details, see `config user local-user`, `config user ldap-user`, `config server-policy custom-application application-policy`, or `config user ntlm-user`.

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

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For more information, see Permissions on page 74.

Syntax

```
config user user-group
   edit <user-group_name>
      set auth-type {basic | digest | NTLM}
      config members
         edit <entry_index>
            set type {ldap | local | ntlm | radius}
            set ldap-name <query_name>
            set local-name <query_name>
            set ntlm-name <query_name>
            set radius-name <query_name>
         next
      end
   next
end
```

Variable	Description	Default
<user-group_name>	Type the name of the user group. The maximum length is 35 characters. To display the list of existing groups, type: edit ?	No default.
auth-type {basic | digest | NTLM}	Select one of the following authentication types: • basic — 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 — Authentication encrypts the password and thus is more secure than the basic authentication. • NTLM — Authentication uses a proprietary protocol of Microsoft and is considered to be more secure than basic authentication.	basic
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
ldap-name <query_name>	Select the name of a LDAP user query. Available if the value of type is ldap. The maximum length is 35 characters.	No default.
local-name <query_name>	Select the name of a local user account. Available if the value of type is local. The maximum length is 35 characters.	No default.

Variable	Description	Default
ntlm-name <query_name>	Select the name of a NTLM user query. Available if the value of type is ntlm. The maximum length is 35 characters.	No default.
radius-name <query_name>	Select the name of a RADIUS user query. Available if the value of type is radius. The maximum length is 35 characters.	No default.
type {ldap | local | ntlm | radius}	Select which type of user or user query that you want to add to the group. **Note:** You can mix all user types in the group. However, if the authentication rule's authen-type does not support a given user type, all user accounts of that type will be ignored, effectively disabling them.	local

Example

For an example, see config waf http-authen http-authen-policy.

Related topics

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

wad file-filter

Use this command to specify the names of directories and files that you want to exclude from anti-defacement monitoring. Alternatively, you can specify the folders and files you want FortiWeb to monitor and it will exclude any others.

To use this command, your administrator account's access control profile must have either w or rw permission to the wadgrp area. For more information, see Permissions on page 74.

Syntax

```
config wad file-filter
   edit <wad-file-filter_name>
      set filter-type {black-file-list | white-file-list}
         edit <entry_index>
            set file-type {directory | regular-file}
            set file-name <file_str>
```

```
        next
    end
```

Variable	Description	Default
<wad-file-filter_name>	Type the name of the file filter you can reference in other parts of the configuration.	No default.
filter-type {black-file-list | white-file-list}	Specify the type of filter: • black-file-list — A list of files or folders that the anti-defacement feature does not monitor. • white-file-list — A list of files or folders that the anti-defacement feature monitors. The feature ignores all other files and folders. 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.	No default.
<entry_index>	Type the index number of the individual entry in the table.	No default.
file-type {directory | regular-file}	Specify the type of item to add to the list: • directory — A folder or directory path. • regular-file — A file.	No default.
file-name <file_str>	Type 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. If file-type is directory, include the / (forward slash). For example, if file-type is directory and you want to add a folder abc that is under the root folder of a web site, enter /abc. You can restrict the filter condition to a specific file by including file path information in file-name. For example, a web site contains many files with the name 123.txt. To specify the instance located in the abc folder only, enter /abc/123.txt.	No default.

Example

This example creates a filter video-folder that excludes the folder /abc from anti-defacement monitoring when it is applied to an anti-defacement monitoring configuration.

```
config wad file-filter
   edit video-folder
      set filter-type black-file-list
         edit 1
            set file-type directory
```

```
        set file-name /abc
    next
end
```

Related topics

- config wad website

wad website

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

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

Optionally, you can specify a filter that either defines which files and folders FortiWeb does not scan when it looks for changes (blacklist) or the specific files and folders you want it to monitor (whitelist). (See config wad file-filter.)

FortiWeb automatically backs up web site files and creates a revision in the following cases:

- When the FortiWeb appliance initiates monitoring for the first time, the FortiWeb appliance downloads a backup copy of the web site's files and stores it as the first revision.
- If the FortiWeb appliance could not successfully connect during a monitor interval, it creates a new revision the next time it re-establishes the connection.

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

Backup copies omit files exceeding the file size limit and/or matching the file extensions that you have configured the FortiWeb appliance to omit. See backup-max-fsize <limit_int> and backup-skip-ftype <extensions_str>.

To use this command, your administrator account's access control profile must have either w or rw permission to the wadgrp area. For more information, see Permissions on page 74.

Syntax

```
config wad website
  edit <entry_index>
    set alert-email <email-policy_name>
    set auto {disable | restore | acknowledge}
    set backup-max-fsize <limit_int>
    set backup-skip-ftype <extensions_str>
    set connect-type {ftp | smb | ssh}
    set description "<comment_str>"
    set hostname-ip {<host_ipv4> | <host_fqdn>}
```

```
        set interval-other <seconds_int>
        set interval-root <seconds_int>
        set monitor {enable | disable}
        set monitor-depth <folders_int>
        set name <name_str>
        set password <password_str>
        set port <port_int>
        set share-name <share_str>
        set user <user_str>
        set web-folder <path_str>
        set file-filter <wad-file-filter_name>
    next
end
```

Variable	Description	Default
`<entry_index>`	Type the index number of the individual entry in the table. The valid range is from 1 to 16.	No default.
`alert-email <email-policy_name>`	Type the name of the email policy that specifies the email address that FortiWeb sends an email to when it detects that the web site changed. (See `config log email-policy`.) The maximum length is 35 characters.	No default.
`auto {disable | restore | acknowledge}`	Type the action that FortiWeb takes when it detects that the web site has changed. • `disable` – FortiWeb takes no action. You can use the web UI to manually restore all or some of the changed files. • `restore` – Restore the web site to the previous revision number. • `acknowledge` – Accept changes to the web site. **Note**: When you intentionally modify the web site, type `acknowledge`. Otherwise, the FortiWeb appliance detects your changes as a defacement attempt and undoes them.	`disable`
`backup-max-fsize <limit_int>`	Type a file size limit in kilobytes (KB) to indicate which files will be included in the web site backup. Files exceeding this size will not be backed up. The valid range is from 1 to 1,048,576 kilobytes. **Note:** Backing up large files can impact performance.	`10240`
`backup-skip-ftype <extensions_str>`	Type zero or more file extensions, such as `iso,avi`, to exclude from the web site backup. Separate each file extension with a comma. The maximum length is 512 characters. **Note:** Backing up large files, such as video and audio, can impact performance.	No default.

Variable	Description	Default
`connect-type {ftp | smb | ssh}`	Select which protocol to use when connecting to the web site in order to monitor its contents and download web site backups. For Microsoft Windows-style shares, enter `smb`.	`ftp`
`description "<comment_str>"`	Type a description or other comment. If the comment is more than one word or contains special characters, surround the comment with double quotes (`"`). The maximum length is 255 characters.	No default.
`hostname-ip {<host_ipv4> | <host_fqdn>}`	Type the IP address or fully qualified domain name (FQDN) of the physical server on which the web site is hosted. This will be used when connecting by SSH or FTP to the web site to monitor its contents and download backup revisions, and therefore could be different from the real or virtual web host name that may appear in the `Host:` field of HTTP headers.	No default.
`interval-other <seconds_int>`	Type the number of seconds between each monitoring connection from the FortiWeb appliance to the web server. During this connection, the FortiWeb appliance examines the web site's subfolders to see if any files have been changed by comparing the files with the latest backup. The valid range is from 1 to 86,400 seconds. If any file change is detected, the FortiWeb appliance will download a new backup revision. If you have enabled auto {disable | restore | acknowledge}, the FortiWeb appliance will revert the files to their previous version.	`600`
`interval-root <seconds_int>`	Type the number of seconds between each monitoring connection from the FortiWeb appliance to the web server. During this connection, the FortiWeb appliance examines web-folder <path_str> (but **not** its subfolders) to see if any files have been changed by comparing the files with the latest backup. The valid range is from 1 to 86,400 seconds. If any file change is detected, the FortiWeb appliance will download a new backup revision. If you have enabled auto {disable | restore | acknowledge}, the FortiWeb appliance will revert the files to their previous version.	`60`
`monitor {enable | disable}`	Enable to monitor the web site's files for changes, and to download backup revisions that can be used to revert the web site to its previous revision if the FortiWeb appliance detects a change attempt.	`enable`

Variable	Description	Default
monitor-depth <folders_int>	Type how many folder levels deep to monitor for changes to the web site's files. Files in subfolders deeper than this level will not be backed up. The valid range is from 1 to 10 levels deep.	5
name <name_str>	Type a name for the web site. The maximum length is 63 characters. This name will not be used when monitoring the web site, nor will it be referenced in any other part of the configuration, and therefore can be any identifier that is useful to you. It does not need to be the web site's FQDN or virtual host name.	No default.
password <password_str>	Type the password for the user name you entered in user <user_str>. The maximum length is 63 characters.	No default.
port <port_int>	Type the port number on which the web site's physical server listens. The standard port number for FTP is 21; the standard port number for SSH is 22. This is applicable only if connect-type is ftp or ssh.	21
share-name <share_str>	Type the name of the shared folder on the web server. The maximum length is 63 characters. This variable appears only if connect-type is smb.	No default.
user <user_str>	Type the user name that the FortiWeb appliance will use to log in to the web site's physical server. The maximum length is 63 characters.	No default.
web-folder <path_str>	Type the path to the web site's folder, such as public_html, on the physical server. The path is relative to the initial location when logging in with the user name that you specify in user <user_str>. The maximum length is 1,023 characters. Available only if the value of connect-type is ftp or ssh.	No default.
file-filter <wad-file-filter_name>	Type the filter that specifies either the files and folders that FortiWeb excludes from anti-defacement monitoring or the specific files and folders to monitor.	No default.

Example

```
config wad website
   edit 1
      set alert-email email_policy_1
```

```
        set connect-type ssh
        set hostname-ip "192.168.1.10"
        set monitor enable
        set name "www.example.com"
        set password P@ssword1
        set port 22
        set user "fortiweb"
        set web-folder "public_html"
        set file-filter "video-folder"
    next
end
```

Related topics

- config wad file-filter
- config system interface
- config router static

waf allow-method-exceptions

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

While most URL and host name combinations controlled by a profile may require similar HTTP request methods, you may have some that require different methods. Instead of forming separate policies and profiles for those requests, you can configure allowed method exceptions. The exceptions define specific HTTP request methods that are allowed by specific URLs and hosts.

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

Before you configure an allowed method exception, if you want to apply it only to HTTP requests for a specific real or virtual host, you must first define the web host in a protected hosts group. For details, see config server-policy allow-hosts.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf allow-method-exceptions
   edit <method-exception_name>
      config allow-method-exception-list
         edit <entry_index>
            set allow-request {connect delete get head options others post put
                trace}
            set host <protected-hosts_name>
            set host-status {enable | disable}
            set request-file <url_str>
            set request-type {plain | regular}
         next
```

```
        end
    next
end
```

Variable	Description	Default
<method-exception_name>	Type the name of the allowed methods exception. The maximum length is 35 characters. To display a list of the existing exceptions, type: edit ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
allow-request {connect delete get head options others post put trace}	Select one or more of the allowed HTTP request methods that are an exception for that combination of URL and host. Methods that you do not select will be denied. The **OTHERS** option includes methods not specifically named in the other options. It often may be required by WebDAV (RFC 2518) applications such as Microsoft Exchange Server 2003 and Subversion, which may require HTTP methods not commonly used by web browsers, such as PROPFIND and BCOPY. **Note:** If a **WAF Auto Learning Profile** will be selected in the policy with an offline protection profile that uses this allowed method exception, you must enable the HTTP request methods that will be used by sessions that you want the FortiWeb appliance to learn about. If a method is disabled, the FortiWeb appliance will reset the connection, and therefore cannot learn about the session.	No default.
host <protected-hosts_name>	Type the name of a protected host that the Host: field of an HTTP request must be in order to match the exception. The maximum length is 255 characters. This setting is used only if host-status is enable.	No default.
host-status {enable | disable}	Enable to require that the Host: field of the HTTP request match a protected hosts entry in order to match the allowed method exception. Also configure host <protected-hosts_name>.	disable

Variable	Description	Default
request-file <url_str>	Depending on your selection in request-type {plain | regular}, either: • Type the literal URL, such as /index.php, that is an exception to the generally allowed HTTP request methods. The URL must begin with a slash (/). • Type a regular expression, such as ^/*.php, matching all and only the URLs which are exceptions to the generally allowed HTTP request methods. The pattern is **not** required to begin with a slash (/). However, it must at least match URLs that begin with a slash, such as /index.cfm. For example, if multiple URLs on a host have identical HTTP request method requirements, you would type a regular expression matching all of and only those URLs. Do not include the name of the web host, such as www.example.com, which is configured separately in host <protected-hosts_name>. The maximum length is 255 characters. **Note:** Regular expressions beginning with an exclamation point (!) are not supported. For information on language and regular expression matching, see the *FortiWeb Administration Guide*.	No default.
request-type {plain | regular}	Indicate whether request-file <url_str> is a literal URL (plain) or a regular expression (regular).	plain

Example

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

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

Related topics

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

waf allow-method-policy

Use this command to allow only specific HTTP request methods.

To define specific exceptions to this policy, use config waf allow-method-exceptions.

To use this command, your administrator account's access control profile must have either w or rw permission to the wafgrp area. For more information, see Permissions on page 74.

Syntax

```
config waf allow-method-policy
   edit waf allow-method-policy
      set allow-method {connect delete get head options others post put trace}
      set severity {High | Medium | Low}
      set triggered-action <trigger-policy_name>
      set [allow-method-exception <method-exception_name>]
   next
end
```

Variable	Description	Default
<allowed-methods_name>	Type the name of a new or existing allowed methods policy. This field cannot be modified if you are editing an existing allowed method exception. To modify the name, delete the entry, then recreate it using the new name. The maximum length is 35 characters. To display a list of the existing policies, type: edit ?	No default.

Variable	Description	Default
`allow-method {connect delete get head options others post put trace}`	Select one or more HTTP request methods that you want to allow for this specific policy. Methods that you do not select will be denied, unless specifically allowed for a host and/or URL in analyzer-policy <fortianalyzer-policy_name>. The `others` option includes methods not specifically named in the other options. It often may be required by WebDAV (RFC 2518) applications such as Microsoft Exchange Server 2003 and Subversion, which may require HTTP methods not commonly used by web browsers, such as `PROPFIND` and `BCOPY`. **Note:** If a **WAF Auto Learning Profile** is used in the server policy where the HTTP request method is applied (via the **Web Protection 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.	No default.
`severity {High | Medium | Low}`	Select the severity level to use in logs and reports generated when a violation of the policy occurs.	`High`
`triggered-action <trigger-policy_name>`	Type the name of the trigger policy you want FortiWeb to apply when a violation of the HTTP request method policy occurs. Trigger policies determine who will be notified by email when the policy violation occurs, and whether the log message associated with the violation are recorded. The maximum length is 35 characters. To display a list of the existing policies, type: `set triggered-action ?`	No default.
`[allow-method-exception <method-exception_name>]`	Type the name of an existing HTTP request method exception, if any, to apply to it. The maximum length is 35 characters. To display a list of the existing policy, type: `set allow-method-exception ?`	No default.

Example

This example allows the HTTP `GET` and `POST` methods and rejects others, except according to the exceptions defined in `MethodExceptions1`.

```
config waf allow-method-policy
   edit "allowpolicy1"
      set allow-method get post
```

```
        set triggered-action "TriggerActionPolicy1"
        set allow-method-exception "MethodExceptions1"
    next
end
```

Related topics

- config waf allow-method-exceptions

waf application-layer-dos-prevention

Use this command to create an HTTP-layer DoS protection policy. Once you create the policy, reference it in an inline protection profile that is used by a server policy.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf application-layer-dos-prevention
  edit <app-dos-policy_name>
    set enable-http-session-based-prevention {enable | disable}
    set http-connection-flood-check-rule <rule_name>
    set http-request-flood-prevention-rule <rule_name>
    set enable-layer4-dos-prevention {enable | disable}
    set layer4-access-limit-rule <rule_name>
    set layer4-connection-flood-check-rule <rule_name>
  next
end
```

Variable	Description	Default
<app-dos-policy_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: edit ?	No default.
enable-http-session-based-prevention {enable | disable}	Enable to use DoS protection based on session cookies. Also configure http-connection-flood-check-rule <rule_name> and http-request-flood-prevention-rule <rule_name>.	disable

Variable	Description	Default
`http-connection-flood-check-rule <rule_name>`	Type the name of an existing rule that sets the maximum number of HTTP requests per second to a specific URL. The maximum length is 35 characters. To display a list of the existing rules, type: `set http-connection-flood-check-rule ?` This setting applies only if `enable-http-session-based-prevention` is enabled.	No default.
`http-request-flood-prevention-rule <rule_name>`	Type the name of an existing rule that limits TCP connections from the same client. The maximum length is 35 characters. To display a list of the existing rules, type: `set http-request-flood-prevention-rule ?` This setting applies only if `enable-http-session-based-prevention` is enabled.	No default.
`enable-layer4-dos-prevention {enable | disable}`	Enable to use D oS protection that is **not** based on session cookies. Also configure layer4-access-limit-rule <rule_name> and layer4-connection-flood-check-rule <rule_name>.	`disable`
`layer4-access-limit-rule <rule_name>`	Type the name of a rule that limits the number of HTTP requests per second from any source IP address. The maximum length is 35 characters. To display a list of the existing rules, type: `set layer4-access-limit-rule ?` This setting applies only if `enable-layer4-dos-prevention` is enabled.	No default.
`layer4-connection-flood-check-rule <rule_name>`	Type the name of an existing rule that limits the number of TCP connections from the same source IP address. The maximum length is 35 characters. To display a list of the existing rules, type: `set layer4-connection-flood-check-rule ?` This setting applies only if `enable-layer4-dos-prevention` is enabled.	No default.

Example

This example shows the settings for a DoS protection policy that protects a web portal using existing DoS prevention rules.

```
config waf application-layer-dos-prevention
   edit "Web Portal DoS Policy"
        set enable-http-session-based-prevention enable
        set http-connection-flood-check-rule "Web Portal TCP Connect Limit"
        set http-request-flood-prevention-rule "Web Portal HTTP Request Limit"
        set enable-layer4-dos-prevention enable
        set layer4-access-limit-rule "Web Portal HTTP Request Limit"
        set layer4-connection-flood-check-rule "Web Portal Network Connect Limit"
   next
end
```

Related topics

- config waf http-connection-flood-check-rule
- config waf http-request-flood-prevention-rule
- config waf layer4-access-limit-rule
- config waf layer4-connection-flood-check-rule
- config system advanced
- config system global

waf base-signature-disable

Use this command to disable individual or whole categories of data leak and attack signatures in every signature group that currently exists.

For example, if you disable a certain signature ID with this command, the signature ID in every signature group you have defined will be disabled.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf base-signature-disable
   edit <signature-ID_name>
   next
end
```

Variable	Description	Default
<signature-ID_name>	Type the name of an individual signature or signature category ID. The maximum length is 35 characters. For example, to disable the first cross-site scripting attack signature everywhere it is currently selected, you would type: edit 010000001	No default.

Example

This example globally disables the XSS signature whose ID is 010000001.

```
config waf base-signature-disable
   edit "010000001"
   next
end
```

Related topics

- config waf signature

waf brute-force-login

Use this command to configure brute force login attack sensors.

Brute force attacks attempt to penetrate systems by the sheer number of clients, attempts, or computational power, rather than by intelligent insight. For example, in brute force attacks on authentication, multiple web clients may rapidly try one user name and password combination after another in an attempt to eventually guess a correct login and gain access to the system. In this way, behavior differs from web crawlers, which typically do not focus on a single URL.

Brute force login attack sensors track the rate at which each source IP address makes requests for specific URLs. If the source IP address exceeds the threshold, the FortiWeb appliance penalizes the source IP address by blocking additional requests for the time period that you indicate in the sensor.

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

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

To use this command, your administrator account's access control profile must have either w or rw permission to the wafgrp area. For more information, see Permissions on page 74.

Syntax

```
config waf brute-force-login
   edit <brute-force-login_name>
      set analyzer-policy <fortianalyzer-policy_name>
```

```
        set analyzer-policy <fortianalyzer-policy_name>
        config login-page-list
           edit <entry_index>
              set access-limit-standalone-ip <rate_int>
              set access-limit-share-ip <rate_int>
              set block-period <seconds_int>
              set host <allowed-hosts_name>
              set host-status {enable | disable}
              set request-file <url_str>
           next
        end
     next
  end
```

Variable	Description	Default
`<brute-force-login_name>`	Type the name of a new or existing brute force login attack sensor. The maximum length is 35 characters. To display a list of the existing sensor, type: `edit ?`	No default.
`severity {High | Medium | Low}`	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	`High`
`trigger <trigger-policy_name>`	Type the name of the trigger to apply when this policy is violated (see `config log trigger-policy`). The maximum length is 35 characters. To display the list of existing trigger policies, type: `set trigger ?`	No default.
`access-limit-standalone-ip <rate_int>`	Type the rate threshold for source IP addresses that are single clients. Request rates exceeding the threshold will cause the FortiWeb appliance to block additional requests for the length of the time in block-period <seconds_int>. The valid range is from 0 to 9,999,999,999,999,999,999. To disable the rate limit, type `0`.	`1`

Variable	Description	Default
access-limit-share-ip <rate_int>	Type the rate threshold for source IP addresses that are shared by multiple clients behind a network address translation (NAT) device such as a firewall or router. Request rates exceeding the threshold will cause the FortiWeb appliance to block additional requests for the length of the time in the block-period <seconds_int>. The valid range is from 0 to 9,999,999,999,999,999,999. To disable the rate limit, type 0. **Note:** Blocking a shared source IP address could block innocent clients that share the same source IP address with an offending client. In addition, the rate is a total rate for all clients that use the same source IP address. For these reasons, you should usually enter a greater value for this field than for access-limit-share-ip <rate_int>.	1
block-period <seconds_int>	Type the length of time for which the FortiWeb appliance will block additional requests after a source IP address exceeds a rate threshold. 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.	1
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
host <allowed-hosts_name>	Type the name of a protected host that the Host: field of an HTTP request must be in order to match the sensor. The maximum length is 255 characters. This setting is applied only if host-status is enable.	No default.
host-status {enable | disable}	Enable to require that the Host: field of the HTTP request match a protected hosts entry in order to be included in the brute force login attack sensor's rate calculations. Also configure host <allowed-hosts_name>.	disable
ip-port-enable {enable | disable}	Enable to apply the limit of login attempts specified by access-limit-standalone-ip or access-limit-share-ip per TCP/IP session. When the value is disable, the limit is applied per source IP. **Tip:** If you need to cover both possibilities, create two members.	disable

Variable	Description	Default
request-file <url_str>	Type the literal URL, such as /login.php, that the HTTP request must match to be included in the brute force login attack sensor's rate calculations. The URL must begin with a slash (/). Do not include the name of the web host, such as www.example.com, which is configured separately in host <allowed-hosts_name>. The maximum length is 255 characters.	No default.

Example

This example limits IP addresses of individual HTTP clients to 3 requests per second, and NAT IP addresses to 20 requests per second, when they request the file login.php on the host www.example.com on TCP port 8080.

```
config waf brute-force-login
   edit "brute_force_attack_sensor"
      set access-limit-share-ip 20
      set access-limit-standalone-ip 3
      set block-period 120
      config login-page-list
         edit 1
            set host "www.example.com:8080"
            set host-status enable
            set request-file "/login.php"
         next
      end
   next
end
```

Related topics

- config waf web-protection-profile inline-protection
- config system snmp community
- config waf application-layer-dos-prevention
- config log trigger-policy

waf cookie-security

Use this command to configure FortiWeb features that prevent cookie-based attacks.

To use this command, your administrator account's access control profile must have either w or rw permission to the sysgrp area. For more information, see Permissions on page 74.

Syntax

```
config waf cookie-security
   edit <cookie-security_name>
      set security-mode {no |encrypted | signed}
```

```
        set action {alert |alert_deny | remove_cookie}
        set block-period <block-period_int>
        set severity {High | Medium | Low}
        set trigger <trigger-policy_name>
        set cookie-replay-protection-type {no | IP}
        set max-age <max-age_int>
        set secure-cookie {enable | disable}
        set http-only {enable | disable}
        set allow-suspicious-cookies(Never | Always | Custom}
        set allow-time <time_str>
        config cookie-security-exception-list
           edit <entry_index>
              set cookie-name <cookie-name_str>
              set cookie-domain <cookie-domain_str>
              set cookie-path <cookie-path_str>
        end
     next
  end
```

Variable	Description	Default
<cookie-security_name>	Set cookie security policy name.	No default.
security-mode {no |encrypted | signed}	Set security mode for the cookie security policy • no — FortiWeb does not apply cookie tampering protection or encrypt cookie values. • encrypted — Encrypts cookie values the back-end web server sends to clients. Clients see encrypted cookies only. FortiWeb decrypts cookies submitted by clients before it sends them to the back-end server. • signed — Prevents tampering (cookie poisoning) by tracking the cookie value. This option requires you to enable Session Management in the protection policy (see the waf web-protection-profile inline-protection) and the client to support cookies. When FortiWeb receives the first HTTP or HTTPS request from a client, it uses a cookie to track the session. When you select this option, the session-tracking cookie includes a hash value that FortiWeb uses to detect tampering with the cookie from the back-end server response. If FortiWeb determines the cookie from the client has changed, it takes the specified action (action {alert |alert_deny | remove_cookie}).	no

Variable	Description	Default
`action {alert |alert_deny | remove_cookie}`	Select one of the following actions that the FortiWeb appliance will perform when it detects cookie poisoning: • `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 FortiWeb returns to the client with the HTTP status code. See the *FortiWeb Administration Guide* or config system replacemsg. • `block-period` — Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int>. **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 config waf x-forwarded-for). Failure to do so may cause FortiWeb to block **all** connections when it detects a violation of this type. • `remove_cookie` — 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. **Caution:** This setting will be ignored if monitor-mode {enable | disable} is enabled. **Note:** Logging and/or alert email will occur only if enabled and configured. See config log disk and config log alertemail. **Note:** If you select an auto-learning profile with this rule, you should select alert. If the action is alert_deny, for example, the FortiWeb appliance will block the request or reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see config waf web-protection-profile autolearning-profile.	`alert`
`block-period <block-period_int>`	Type the number of seconds to block a connection when `cookie-poison-action` is set to `block-period`. The valid range is from 1 to 3,600 seconds.	`60`
`severity {High |Medium | Low}`	Select the severity level to use in logs and reports generated when cookie poisoning is detected.	`High`

Variable	Description	Default
`trigger <trigger-policy_name>`	Type the name of the trigger to apply when cookie poisoning is detected (see config log triggerpolicy). The maximum length is 35 characters. To display the list of existing trigger policies, type: `set trigger ?`	No default.
`cookie-replay-protection-type {no | IP}`	Select whether FortiWeb uses the IP address of a request to determine the owner of the cookie. Because the public IP of a client is not static in many environments, Fortinet recommends that you do not enable Cookie Replay.	`no`
`max-age <max-age_int>`	Set the cookie security attributes. Enter the maximum age, in minutes, permitted for cookies that do not have an “Expires” or “Max-Age” attribute. To configure no expiry age for cookies, enter 0.	`0`
`secure-cookie {enable | disable}`	Set the cookie security attributes. Enable to add the secure flag to cookies, which forces browsers to return the cookie only when the request is for an HTTPS page.	`disable`
`http-only {enable | disable}`	Set the cookie security attributes. Enable to add the HttpOnly flag to cookies, which prevents client-side scripts from accessing the cookie.	`enable`

Variable	Description	Default
`allow-suspicious-cookies {Never |Always | Custom}`	Select whether FortiWeb allows requests that contain cookies that it does not recognize or that are missing cookies. • When `security-mode` is `encrypted`, suspicious cookies are cookies for which FortiWeb does not have a corresponding encrypted cookie value. • When `cookie-replay-protection-type` is `IP`, the suspicious cookie is a missing cookie that tracks the client IP address. In many cases, when you first introduce the cookie security features, cookies that client browsers have cached earlier generate false positives. To avoid this problem, either select `Never`, or select `Custom` and enter an appropriate date on which to start taking the specified action against suspicious cookies. • `Never` — FortiWeb does not take the action specified by `action` against suspicious cookies. • `Always` — FortiWeb always takes the specified action against suspicious cookies. • `Custom` — FortiWeb takes the specified action against suspicious cookies starting on the date specified by `allow-time`. This feature is not available if `security-mode` is `signed`.	`Custom`
`allow-time <time_str>`	Set the date on which FortiWeb starts to take the specified action against suspicious cookies if `allow-suspicious-cookies` is `Custom`.	No default.
`<entry_index>`	Type the index number of a new or existing entry in the exception list of the cookie security policy.	No default.
`cookie-name <cookie-name_str>`	Set the exception cookie entry name.	No default.
`cookie-domain <cookie-domain_str>`	Enter the partial or complete domain name or IP address as it appears in the cookie. For example: `www.example.com`, `.google.com` or `10.0.2.50`.	No default.
`cookie-path <cookie-path_str>`	Enter the path as it appears in the cookie, such as `/` or `/blog/folder`.	No default.

Related topics

- `config waf web-protection-profile inline-protection`

waf csrf-protection

Use this command to protect against cross-site request forgery (CSRF). CSRF is an attack that exploits the trust that a site has in a user's browser to transmit unauthorized commands.

The CRSF protection feature is not supported when the operation mode is offline protection or transparent inspection.

To protect back-end servers from CSRF attacks, you create two lists of items: a list of web pages to protect against CSRF attacks, and a corresponding list of the URLs found in the requests that the pages generate. For more information on configuring CSRF protection, including troubleshooting and adding parameter filters, see the *FortiWeb Administration Guide*.

To apply a CSRF protection rule, you select it in an inline protection profile. For details, see `config waf web-protection-profile inline-protection`.

Before you configure a CSRF protection rule, if you want to apply it only to HTTP requests for a specific real or virtual host, you must first define the web host in a protected hosts group. For details, see `config server-policy allow-hosts`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf csrf-protection
   edit <csrf-rule_name>
      set action {alert | alert_deny | block-period}
      set block-period <seconds_int>
      set severity {High | Medium | Low}
      set trigger <trigger-policy_name>
      config csrf-page-list
         edit <entry_index>
            set host <host_name>
            set request-url <url_str>
            set host-status {enable | disable}
            set request-type {plain | regular}
            set parameter-filter {enable | disable}
            set parameter-name <parameter-name_str>
            set parameter-value-type {plain | regular}
            set parameter-value <parameter-value_str>
         next
      end
      config csrf-url-list
         edit <entry_index>
            set host <host_name>
            set request-url <url_str>
            set host-status {enable | disable}
            set request-type {plain | regular}
            set parameter-filter {enable | disable}
            set parameter-name <parameter-name_str>
            set parameter-value-type {plain | regular}
            set parameter-value <parameter-value_str>
         next
      end
```

```
    next
  end
```

Variable	Description	Default
<csrf-rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: edit ?	No default.
action {alert | alert_deny | block-period}	Enter the action that FortiWeb takes when it detects a missing or incorrect anti-CSRF parameter: • alert — Accept the request and generate an alert email, a log message, or both. • alert_deny — Block the request (reset the connection) and generate an alert email, a log message, or both. You can customize the web page that FortiWeb returns to the client with the HTTP status code. See the *FortiWeb Administration Guide* or config system replacemsg. • block-period — Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int>. **Note:** Logging and alert email occur only if the corresponding settings are enabled and configured. See config log disk and config log alertemail.	alert
block-period <seconds_int>	Enter the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects a CSRF attack. The valid range is from 1 to 3,600 (1 hour). This setting applies only if action is block-period.	60
severity {High | Medium | Low}	Select the severity level to use in any logs and reports that FortiWeb generates when a violation of this rule occurs.	Low
trigger <trigger-policy_name>	Enter the name of the trigger to apply when this rule is violated (see config log trigger-policy). The maximum length is 35 characters. To display the list of existing trigger policies, type: set trigger ?	No default.
<entry_index>	Type the index number of the individual entry in the table.	No default.

Variable	Description	Default
`host <host_name>`	Enter a protected host name (either a web host name or IP address) that the `Host:` field of the HTTP request matches. This setting applies only if `host-status` is `enable`.	No default.
`request-url <url_str>`	Enter either a literal URL or regular expression, depending on the value of `request-type`.	No default.
`host-status {enable | disable}`	Enter `enable` to apply this rule only to HTTP requests for specific web hosts. Also configure `host`. Disable to match the rule based on the URL and any parameter filter only.	`disable`
`request-type {plain | regular}`	Select whether `request-url` contains a literal URL (`plain`), or a regular expression designed to match multiple URLs (`regular`).	`plain`
`parameter-filter {enable | disable}`	Enter `enable` to specify a parameter name and value to match. The parameter can be located in either the URL or the HTTP body of a request.	`disable`
`parameter-name <parameter-name_str>`	Enter the name of the parameter name to match.	No default.
`parameter-value-type {plain | regular}`	Select whether `parameter-value` contains a literal value (`plain`), or a regular expression designed to match multiple parameters (`regular`).	`plain`
`parameter-value <parameter-value_str>`	Enter either a literal parameter or regular expression, depending on the value of `parameter-value-type`. To match any parameter value, for `parameter-value-type`, enter `regular`, and for `parameter-value`, enter `*` (asterisk).	No default.

Example

The web page `csrf_login.html` contains the following HTML form:

```
<form name="do_some_action" id="form1" action="csrf_test2.php" method="GET">
   <input type="text" name="username" value=""/>
   <Input type="text" name="password" value=""/>
   <input type="submit" value="do Action"/>
</form>
```

This form generates the following request when the page is added to the list of pages protected by a CSRF protection policy:

```
http://target-site.com/csrf_
    test2.php?username=test&password=123&tknfv=3DF5BDCCIG3DCXNTE3RUNCTKRS3E36AD
```

The CSRF protection feature adds the parameter `tknfv` with a value that matches the session ID.

To create this example, you add `csrf_login.html` to the list of pages and `/csrf_check2.php` to the list of URLs.

```
config waf csrf-protection
   edit "csrf_rule1"
      set action alert_deny
      config csrf-page-list
         edit 1
            set request-url csrf_login.html
            set request-type regular
         next
      end
      config csrf-url-list
         edit 1
            set request-url /csrf_check2.php
            set request-type plain
         next
      end
   next
end
```

waf custom-access policy

Use this command to configure custom access policies.

Custom access policies group custom access rules.

To apply a custom access policy, select it within an inline protection profile or offline protection profile. For details, see `config waf web-protection-profile inline-protection` or `config waf web-protection-profile offline-protection`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf custom-access policy
   edit <custom-policy_name>
      config rule
         edit <entry_index>
            set rule-name "<custom-rule_name>"
         next
      end
   next
end
```

Variable	Description	Default
<custom-policy_name>	Type the name of a new or existing custom policy. The maximum length is 63 characters. To display a list of the existing policies, type: edit ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,223,372,036,854,775,807.	No default.
rule-name "<custom-rule_name>"	Type the name of the existing custom access rule to add to the policy. The maximum length is 63 characters.	No default.

Example

For an example, see config waf custom-access rule.

Related topics

- config waf web-protection-profile inline-protection
- config waf web-protection-profile offline-protection
- config waf custom-access rule

waf custom-access rule

Use this command to configure custom access rules.

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
- user name
- rate limit
- HTTP header such as X-Real-IP:
- URL line in the HTTP header

In the rule, add all criteria that you require allowed traffic to match.

Before you can apply a custom access rule, you must first group it with any others that you want to apply in a custom access policy. For details, see config waf custom-access policy.

To use this command, your administrator account's access control profile must have either w or rw permission to the wafgrp area. For more information, see Permissions on page 74.

Syntax

```
config waf custom-access rule
   edit <custom-access_name>
      set action {alert | alert_deny | block-period}
      set block-period <seconds_int>
      set severity {High | Medium | Low}
      set trigger <trigger-policy_name>
      set real-browser-enforcement {enable | disable}
      set validation-timeout <timeout_int>
      config access-limit-filter
         edit <entry_index>
            set access-rate-limit <rate_int>
      end
      config http-header-filter
         edit <entry_index>
            set header-name-type {custom | predefined}
            set predefined-header {host | connection | authorization | x-pad  |
                cookie | referer | user-agent  | X-Forwarded-For | Accept}
            set pre-header-type {plain | regular}
            set pre-header-rev-match {enable | disable}
            set custom-header-name <key_str>
            set cus-header-type {plain | regular}
            set cus-header-rev-match {enable | disable}
            set header-value <value_str>
      end
      config source-ip-filter
         edit <entry_index>
            set source-ip <ip_range>
      end
      config user-filter
         edit <entry_index>
            set reverse-match {no | yes}
            set user-name <user-name_str>
      end
      config url-filter
         edit <entry_index>
            set request-file <url_str>
            set reverse-match {no | yes}
      end
      config http-transaction
         edit <entry_index>
            set http-transation-timeout <timeout_int>
      end
      config response-code
         edit <entry_index>
            set response-code-min <response-code_int>
            set response-code-max <response-code_int>
      end
      config content-type
         edit <entry_index>
            set content-type-set {text/html text/plain text/xml application/xml
                application/soap+xml application/json}
      end
      config packet-interval
         edit <entry_index>
```

```
            set packet-interval-timeout <timeout_int>
          end
        config signature-class
          edit {010000000 | 020000000 | 030000000 | 040000000 | 050000000 |
              060000000 | 090000000}
            set status {enable | disable}
          end
        config custom-signature
          edit <entry_index>
            set custom-signature-enable {enable | disable}
            set custom-signature-type {custom-signature-group | custom-signature}
            set custom-signature-name <custom-signature-name_str>
          end
        config occurrence
          edit <entry_index>
            set occurrence-num <occurrence_int>
            set within <within_int>
            set percentage-flag {enable | disable}
            set percentage <percentage_int>
            set traced-by {Source-IP | User}
        end
    next
end
```

Variable	Description	Default
<custom-access_name>	Type the name of a new or existing custom access rule. The maximum length is 63 characters. To display a list of the existing rule, type: edit ?	No default.

Variable	Description	Default
`action {alert | alert_deny | block-period}`	Select the specific action to be taken when the request matches the signature. • `alert` — Accept the request and generate an alert email and/or log message. **Note:** If `type` is `data-leakage`, does **not** cloak, except for removing sensitive headers. (Sensitive information in the body remains unaltered.) • `alert_deny` — Block the request (or reset the connection) and generate an alert email and/or log message. This option is applicable only if `type` is `signature-creation`. You can customize the web page that FortiWeb returns to the client with the HTTP status code. See the *FortiWeb Administration Guide* or `config system replacemsg`. • `block-period` — Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int>. **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 `config waf x-forwarded-for`). Failure to do so may cause FortiWeb to block **all** connections when it detects a violation of this type.	`alert`
`block-period <seconds_int>`	Type the length of time for which the FortiWeb appliance will block additional requests after a source IP address violates this rule. The block period is shared by all clients whose traffic originates from the source IP address. The valid range is from 1 to 3,600 seconds.	`60`
`severity {High | Medium | Low}`	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	`Low`
`trigger <trigger-policy_name>`	Type the name of the trigger to apply when this policy is violated (see `config log trigger-policy`). The maximum length is 35 characters. To display the list of existing trigger policies, type: `set trigger ?`	No default.

Variable	Description	Default
real-browser-enforcement {enable | disable}	Enable to return a JavaScript to the client to test whether it is a web browser or automated tool when it violates the access rule. If the client either fails the test or does not return results before the timeout specified by validation-timeout, FortiWeb applies the specified action. If the client appears to be a web browser, FortiWeb allows the client to violate the rule. Disable this option to apply the access rule regardless of whether the client is a web browser (for example, Firefox) or an automated tool (for example, wget).	disable
validation-timeout <timeout_int>	Specifies the maximum amount of time that FortiWeb waits for results from the web browser test.	20
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
access-rate-limit <rate_int>	Type the rate threshold for source IP addresses. The valid range is from 1 to 65535. To disable the rate limit, type 0. **Note:** Blocking a shared source IP address could block innocent clients that share the same source IP address with an offending client.	1
header-name-type {custom | predefined}	Select whether to define the HTTP header filter by selecting a predefined HTTP header name, or by typing the name of a custom HTTP header. Also configure header-value <value_str> and, depending on which you indicate in this option, either: • predefined-header {host | connection | authorization | x-pad | cookie | referer | user-agent | X-Forwarded-For | Accept} , pre-header-type {plain | regular} , and pre-header-rev-match {enable | disable} • custom-header-name <key_str>, cus-header-type {plain | regular}, and cus-header-rev-match {enable | disable}	predefined

Variable	Description	Default
`predefined-header {host | connection | authorization | x-pad | cookie | referer | user-agent | X-Forwarded-For | Accept}`	Select the name (key) of the HTTP header such as `Accept:` that must be present in order for the request to be allowed. This field appears only if `header-name-type` is `predefined`.	`host`
`pre-header-type {plain | regular}`	Indicate whether header-value <value_str> is a literal header value (`plain`) or a regular expression that indicates multiple possible valid header values (`regular`).	`plain`
`pre-header-rev-match {enable | disable}`	Indicate how to use predefined-header {host | connection | authorization | x-pad | cookie | referer | user-agent | X-Forwarded-For | Accept} and header-value <value_str> when determining whether or not this condition has been met. • `no` — If the regular expression **does** match the request object, the condition is met. • `yes` — If the regular expression does **not** match the request object, the condition is met. The effect is equivalent to preceding a regular expression with an exclamation point (`!`). If all conditions are met, the FortiWeb appliance will allow access.	`disable`
`custom-header-name <key_str>`	Type the name (key) **without** the trailing colon (`:`), such as `X-Real-IP`, of the HTTP header that must be present in order for the request to be allowed. This field appears only if `header-name-type` is `custom`.	No default.
`cus-header-type {plain | regular}`	Indicate whether header-value <value_str> is a literal header value (`plain`) or a regular expression that indicates multiple possible valid header values (`regular`).	`plain`

Variable	Description	Default
`cus-header-rev-match {enable | disable}`	Indicate how to use custom-header-name <key_str> and header-value <value_str> when determining whether or not this condition has been met. • `no` — If the regular expression **does** match the request object, the condition is met. • `yes` — If the regular expression does **not** match the request object, the condition is met. The effect is equivalent to preceding a regular expression with an exclamation point (`!`). If all conditions are met, the FortiWeb appliance will allow access.	`disable`
`header-value <value_str>`	Depending on your selection in pre-header-type {plain | regular}, either: • Type the literal header value, such as `172.0.2.80`, your specified HTTP header must **contain** in order to match the filter. Value matching is **case sensitive**. (If you require a filter based upon more than one HTTP header, create multiple entries in the set, one for each HTTP header.). • Type a regular expression, such as `172\.0\.2\.*`, matching all and only the header values which accepted HTTP header values must match. For information on language and regular expression matching, see the *FortiWeb Administration Guide*. **Tip:** 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	No default.

Variable	Description	Default
source-ip <ip_range>	Enter the IP address or IP address range that specifies the clients that FortiWeb allows. For example: • 1.2.3.4 • 2001::1 • 1.2.3.4-1.2.3.40 • 2001::1-2001::100 Depending on your configuration of how FortiWeb will derive the client's IP (see config waf x-forwarded-for), this may be the IP address that is indicated in an HTTP header rather than the IP header.	No default.
reverse-match {no | yes}	Indicate how to use user-name when determining whether or not this rule's condition has been met. • no — If the regular expression **does** match the user name, the condition is met. • yes — If the regular expression does **not** match the user name, the condition is met. The effect is equivalent to preceding a regular expression with an exclamation point (!).	no
user-name <user-name_str>	Enter the user name to match.	No default.
request-file <url_str>	Type a regular expression that defines either all matching or all non-matching URLs. Then, also configure reverse-match {yes | no}. For example, for the URL access rule to match all URLs that begin with /wordpress, you could enter ^/wordpress, then, in reverse-match {yes | no}, select no. The pattern is **not** required to begin with a slash (/). The maximum length is 255 characters. **Note:** Regular expressions beginning with an exclamation point (!) are not supported. Instead, use reverse-match {yes | no}.	No default.

Variable	Description	Default
`reverse-match {no | yes}`	Indicate how to use request-file <url_str> when determining whether or not this rule's condition has been met. • `no` — If the regular expression **does** match the request URL, the condition is met. • `yes` — If the regular expression does **not** match the request URL, the condition is met. The effect is equivalent to preceding a regular expression with an exclamation point (`!`).	`no`
`http-transation-timeout <timeout_int>`	Specifies a timeout value of 1 to 3600 seconds. If the lifetime of a HTTP transaction exceeds this value, the transaction matches this condition.	`5`
`<response-code_int>`	Specifies the start and end code in a range of HTTP response codes. To specify a single code, enter the same value for the start and end codes (for example, `404-404` or `500-503`). If its HTTP response code is within this range, the HTTP transaction matches this condition.	No default.
`{text/html text/plain text/xml application/xml application/soap+xml application/json}`	Specifies a file content type to match. Use with `occurrence` to detect and control web scraping (content scraping) activity.	application/soap+xml application/xml(or) text/xml text/html text/plain application/json
`packet-interval-timeout <timeout_int>`	Specifies the maximum number of seconds allowed between packets arriving from either the client or server (request or response packets), in seconds. Enter a value from 1 to 60. If the interval exceeds this value, the HTTP transaction matches this condition.	`1`
`{010000000 | 020000000 | 030000000 | 040000000 | 050000000 | 060000000 | 090000000}`	Specifies the ID of a signature class. Ensure the signature is enabled in signature configuration before you use it in an advanced access control rule. See `config waf signature`.	No default.

Variable	Description	Default
`status {enable | disable}`	Specifies whether the HTTP transaction matches this condition if it matches the specified signature.	`disable`
`custom-signature-enable {enable | disable}`	Specifies whether the current custom signature filter is enabled.	`disable`
`{custom-signature-group | custom-signature}`	Specifies whether <custom-signature-name_str> specifies a custom signature group or an individual signature.	`custom-signature-group`
`<custom-signature-name_str>`	Specifies the custom signature group or individual signature to match. Ensure the signature is enabled in signature configuration before you use it in an advanced access control rule. See `config waf signature`.	No default.
`<occurrence_int>`	Specifies the maximum number of times a transaction can match other filter types in the current rule during the time period specified by `within`. Enter a value between 1 and 100,000. If the number of matches exceeds this threshold, the associated HTTP source client IP address or client matches this condition.	`1`
`<within_int>`	Specifies the time period during which FortiWeb counts the number of times transactions match other filter types in the current rule. Enter a value between 1 and 600.	`1`
`percentage-flag {enable | disable}`	Specifies whether the current filter matches when the rate of matches with other filter types in the current rule exceeds the `<percentage_int> value`.	`disable`
`<percentage_int>`	The maximum rate of matches with other filter types in the current rule, expressed as percent of hits. If percentage-flag {enable | disable} is enabled and the number of matches exceeds this threshold, the associated HTTP source client IP address or client matches this condition.	No default.

Variable	Description	Default
{Source-IP | User}	Specifies whether FortiWeb determines the rate at which a transaction matches other filter types in the current rule by counting matches by source client IP address or by client. To specify `user`, ensure that the value of `http-session-management` is `enabled` (see `config waf web-protection-profile inline-protection`).	source-ip

Example

This example allows access to URLs beginning with "/admin", but only if they originate from 172.16.1.5, and only if the client does not exceed 5 requests per second.

Clients that violate this rule will be blocked for 60 seconds (the default duration). The violation will be logged in the attack log using `severity_level=High`, and all servers configured in `notification-servers1` will be used to notify the network administrator.

```
config waf custom-access rule
   edit "combo-IP-rate-URL-rule1"
      set action block-period
      set severity High
      set trigger "notification-servers1"
      config access-limit-filter
         edit 1
            set access-rate-limit 5
         next
      end
      config source-ip-filter
         edit 1
            set source-ip 172.16.1.5
         next
      end
      config url-filter
         edit 1
            set request-file "/admin*"
         next
      end
   next
end
config waf custom-access policy
   edit "combo-IP-rate-URL-policy1"
      config rule
         edit 1
            set rule-name "combo-access-rate-rule1"
         next
      end
   next
end
```

Related topics

- config waf custom-access policy
- config log trigger-policy
- config waf signature

waf custom-protection-group

Use this command to configure custom protection groups, creating sets of custom protection rules that can be used with attack signatures (“server protection rule”).

Before you can configure this command, you must first define your custom data leak and attack signatures. For details, see config waf custom-protection-rule.

To use this command, your administrator account’s access control profile must have either w or rw permission to the wafgrp area. For more information, see Permissions on page 74.

Syntax

```
config waf custom-protection-group
   edit <custom-protection group_name>
      config type-list
         edit <entry_index>
            set custom-protection-rule <rule_name>
         next
      end
   next
end
```

Variable	Description	Default
<custom-protection group_name>	Type the name of a new or existing group. The maximum length is 35 characters. To display the list of existing group, type: edit ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
custom-protection-rule <rule_name>	Type the name of the custom protection rule to associate with the custom protection group. The maximum length is 35 characters. To display a list of the existing rules, type: set custom-protection-rule ?	No default.

Example

This example groups `custom protection rule 1` and `custom protection rule 3` together within `Custom Protection group 1`.

```
config waf custom-protection-group
   edit "Custom Protection group 1"
      config type-list
         edit 1
               set custom-protection-rule "custom protection rule 3"
            next
            edit 3
               set custom-protection-rule "custom protection rule 1"
            next
         end
   next
end
```

Related topics

- `config waf signature`
- `config waf custom-protection-rule`

waf custom-protection-rule

Use this command to configure custom data leak and attack signatures.

Before you enter custom signatures via the CLI, first enable cli-signature {enable | disable} in `config system global`.

To use your custom signatures, you must first group them so that they can be included in a rule. For details, see `config waf custom-protection-group`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf custom-protection-rule
   edit <custom-protection rule_name>
      set type {request | response}
      set action {alert | alert_deny | alert_erase | redirect | block-period |
          send_http_response}
      set block-period <seconds_int>
      set severity {High | Medium | Low}
      set trigger <trigger-policy_name>
      config meet-condition
         edit <entry_index>
            set operator {RE | GT | LT | NE | EQ}
```

```
            set request-target {REQUEST_FILENAME REQUEST_URI REQUEST_HEADERS_
                NAMES REQUEST_HEADERS REQUEST_COOKIES_NAMES REQUEST_COOKIES ARGS_
                NAMES ARGS_VALUE REQUEST_RAW_URI REQUEST_BODY CONTENT_LENGTH
                HEADER_LENGTH BODY_LENGTH COOKIE_NUMBER ARGS_NUMBER}
            set response-target {RESPONSE_BODY RESPONSE_HEADER CONTENT_LENGTH
                HEADER_LENGTH BODY_LENGTH RESPONSE_CODE}
            set threshold <threshold_int>
            set case-sensitive {enable | disable}
            set expression <regex_pattern>
          next
        end
      next
    end
```

Variable	Description	Default
`<custom-protection rule_name>`	Type the name of the new or existing custom signature. The maximum length is 35 characters. To display a list of the existing rules, type: `edit ?`	No default.
`type {request | response}`	Specify the type of regular expression: • `request` — The expression is an attack signature. • `data-leakage` — The expression is a server information disclosure signature.	`request`

Variable	Description	Default
`action {alert | alert_deny | alert_erase | redirect | block-period | send_http_response}`	Select the specific action to be taken when the request matches the this signature. • `alert` — Accept the request and generate an alert email and/or log message. **Note:** If `type` is `data-leakage`, does **not** cloak, except for removing sensitive headers. (Sensitive information in the body remains unaltered.) • `alert_deny` — Block the request (or reset the connection) and generate an alert email and/or log message. This option is applicable only if `type` is `signature-creation`. You can customize the web page that FortiWeb returns to the client with the HTTP status code. See the *FortiWeb Administration Guide* or `config system replacemsg`. • `alert_erase` — 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 `type` is `data-leakage`. If the sensitive information is a status code, you can customize the web page that FortiWeb returns to the client with the HTTP status code. See the *FortiWeb Administration Guide* or `config system replacemsg`. **Note:** This option is not fully supported in offline protection mode. Effects will be identical to `alert`; sensitive information will not be blocked or erased. • `block-period` — Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int>. **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 `config waf x-forwarded-for`). 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 and generate an alert email and/or log message. Also configure redirect-url <redirect_fqdn> and rdt-reason {enable | disable}. • `send_http_response` — Block and reply to the client with an HTTP error message, and generate an alert email, a log message, or both. You can customize the web page that FortiWeb returns to the client with the HTTP status code. See the *FortiWeb Administration Guide* or `config system replacemsg`.	`alert`

Variable	Description	Default
	Caution: This setting will be ignored if monitor-mode {enable | disable} is enabled. **Note:** Logging and/or alert email will occur only if enabled and configured. See `config log disk` and `config log alertemail`. **Note:** If an auto-learning profile will be selected in the policy with offline protection profiles that use this rule, you should select `alert`. If the `action` is `alert_deny`, the FortiWeb appliance will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see `config waf web-protection-profile autolearning-profile`.	
`block-period <seconds_int>`	If `action` is `block-period`, 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. For information on viewing the list of currently blocked clients, see the *FortiWeb Administration Guide*. The valid range is from 1 to 3,600 (1 hour).	`1`
`severity {High | Medium | Low}`	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.	`Medium`
`trigger <trigger-policy_name>`	Select which trigger policy, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a violation of the rule (see `config log trigger-policy`). The maximum length is 35 characters. To display the list of existing trigger policies, type: `set trigger ?`	No default.
`<entry_index>`	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.

Variable	Description	Default
`operator {RE | GT | LT | NE | EQ}`	• `RE` — The signature matches when the value of a selected target in the request or response matches the value of `expression`. • `GT` — The signature matches when specified target has a value greater than the value of `threshold`. • `LT` — The signature matches when specified target has a value less than the value of `threshold`. • `NE` — The signature matches when specified target has a different value than `threshold`. • `EQ` — The signature matches when specified target has the same value as `threshold`.	`RE`
`request-target {REQUEST_FILENAME REQUEST_URI REQUEST_HEADERS_NAMES REQUEST_HEADERS REQUEST_COOKIES_NAMES REQUEST_COOKIES ARGS_NAMES ARGS_VALUE REQUEST_RAW_URI REQUEST_BODY CONTENT_LENGTH HEADER_LENGTH BODY_LENGTH COOKIE_NUMBER ARGS_NUMBER}`	Type the name of one or more locations in the HTTP request to scan for a signature match. For example, `ARGS_NAMES` for the names of parameters or `REQUEST_COOKIES` for strings in the HTTP `Cookie:` header.	No default.
`response-target {RESPONSE_BODY RESPONSE_HEADER CONTENT_LENGTH HEADER_LENGTH BODY_LENGTH RESPONSE_CODE}`	Type the name of one or more locations in the HTTP response to scan for a signature match.	No default.
threshold <threshold_int>	Type the value that FortiWeb compares to the target value to determine if a request or response matches.	No default.
`case-sensitive {enable | disable}`	Enable to differentiate upper case and lower case letters when evaluating the web server's response for data leaks according to waf custom-protection-rule. For example, when enabled, an HTTP reply containing the phrase **C**`redit card` would **not** match an expression that looks for the phrase `credit card` (difference highlighted in bold).	`disable`

Variable	Description	Default

expression <regex_pattern>	When `operator` is `RE`, type a regular expression that matches either an attack from a client or a data leak from the server.
	
	If `action` is Alert & Erase, enclose the portion of the regular expression to erase in brackets.
	
	For example, the following command erases the expression "webattack" from the response packet:
	
	`config waf custom-protection-rule`
	`edit "test"`
	`set type response`
	`set action alert_erase`
	`config meet-condition`
	`edit 1`
	`set response-target RESPONSE_BODY`
	`set expression "(webattack)"`
	`next`
	`end`
	`next`
	`end`
	
	To prevent false positives, it should not match anything else. The maximum length is 2,071 characters.
		No default.

Example

This example configures a signature to detect and block an LFI attack that uses directory traversal through an unsanitized `controller` parameter in older versions of Joomla. Each time it detects an attack, the trigger policy named `notification-servers1` sends an alert email and attack log messages whose severity level is `High`.

```
config waf custom-protection-rule
   edit "Joomla_controller_LFI"
      set type request
      set action alert_deny
      set severity High
      set trigger notification-servers1
      config meet-condition
         edit 1
            set request-target REQUEST_RAW_URI
            set expression "^/index\.php\?option=com_ckforms\&controller=(\.\.\/)+?"
         next
      end
   next
end
```

Related topics

- config waf custom-protection-group
- config log trigger-policy

waf exclude-url

Use this command to configure URLs that are exempt from a file compression or file decompression rule.

To apply an exclusion, include it in a compression or decompression rule. See config waf file-compress-rule or config waf file-uncompress-rule.

To use this command, your administrator account's access control profile must have either w or rw permission to the wafgrp area. For more information, see Permissions on page 74.

Syntax

```
config waf exclude-url
   edit <rule_name>
      config exclude-rules
         edit <entry_index>
            set host <protected-host_name>
            set host-status {enable | disable}
            set request-file <url_str>
         next
      end
   next
end
```

Variable	Description	Default
<rule_name>	Type the name of a new or existing exception. The maximum length is 35 characters. To display a list of the existing exceptions, type: edit ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
host <protected-host_name>	Type the name of a protected host that the Host: field of an HTTP request must be in order to match the exception. The maximum length is 255 characters. This setting applies only if host-status is enable.	No default.

Variable	Description	Default
`host-status {enable | disable}`	Enable to apply this exception only to HTTP requests for specific web hosts. Also configure host <protected-host_name>. Disable to match the exception based upon the other criteria, such as the URL, but regardless of the `Host:` field.	`disable`
`request-file <url_str>`	Type the literal URL, such as `/archives`, to which the exception applies. The URL must begin with a slash (/). Do not include the name of the host, such as `www.example.com`, which is configured separately using `host`. The maximum length is 255 characters.	No default.

Example

This example configures two exclusion rules, one for compression and the other for decompression. Either rule can be referenced by name in a file compression or file decompression rule.

```
config waf exclude-url
   edit "Compression Exclusion"
      config exclude-rules
         edit 1
            set host "192.168.1.2"
            set host-status enable
            set request-file "/archives"
         next
      end
   next
   edit "Decompression Exclusion"
      config exclude-rules
         edit 1
            set host "www.example.com"
            set host-status enable
            set request-file "/products.cfm"
         next
      end
   next
end
```

Related topics

- config waf file-compress-rule
- config waf file-uncompress-rule

waf file-compress-rule

Use this command to compress specific file types in HTTP replies.

Compression can reduce bandwidth, which can reduce delivery time to end users. Modern browsers automatically decompress files before they display web pages.

You can configure most web servers to compress files when they respond to a request. However, if you do not want to configure each of your web servers separately, or if you want to offload compression for performance reasons, you can configure FortiWeb to do the compression.

By default, the maximum pre-compressed file size is 64 KB. FortiWeb transmits files larger than the maximum without compression. You can use the `config system advanced` command's `max-cache-size` setting to adjust the maximum files size (see `config system advanced`).

To exclude specific URLs from compression, see `config waf exclude-url`.

To apply a compression rule, select it in an inline protection profile. See `config waf web-protection-profile inline-protection`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf file-compress-rule
   edit <rule_name>
      config content-types
         edit <entry_index>
            set content-type <content-type_name>
         next
      end
      [set exclude-url <exclusion-rule_name>]
   next
end
```

Variable	Description	Default
`<rule_name>`	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: `edit ?`	No default.
`<entry_index>`	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.

Variable	Description	Default
content-type <content-type_name>	Type one of the following content types to compress it: • text/plain • text/html • application/xml(or)text/xml • application/soap+xml • application/x-javascript • text/css • application/javascript • text/javascript To compress multiple file types, add each file type in a separate table entry with its own <entry_index>. See Example.	No default.
exclude-url <exclusion-rule_name>	Type the name of an exclusion to use with the rule, if any. See config waf exclude-url. The maximum length is 35 characters.	No default.

Example

This example configures a file compression rule that compresses CSS and HTML files, unless they match one of the URLs in the exception named “Compression Exclusion 1”.

```
config waf file-compress-rule
   edit "Web Portal Compression Rule"
        config content-types
           edit 1
              set content-type text/css
           next
           edit 2
              set content-type text/html
           next
        end
      set exclude-url "Compression Exclusion 1"
   next
end
```

Related topics

- config waf file-uncompress-rule
- config waf exclude-url

waf file-uncompress-rule

Use this command to decompress a file that was already compressed by a protected web server.

Since the FortiWeb appliance cannot scan compressed files in order to perform features such as data leak prevention, you can configure the FortiWeb appliance to decompress files based on the file type.

By default, the maximum file size that FortiWeb can decompress is 64 KB. FortiWeb does not scan files larger than the maximum.

You can use the `config system advanced` command's `max-cache-size` setting to adjust the maximum files size (see `config system advanced`).

All decompressed files are recompressed after being scanned. As such, unlike `config waf file-compress-rule`, the effects of this command will not be visible to end-users.

To exclude specific URLs, see `config waf exclude-url`.

To apply a decompression rule, select it in an inline or offline protection profile. See `config waf web-protection-profile inline-protection` or `config waf web-protection-profile offline-protection`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf file-uncompress-rule
   edit <rule_name>
      config content-types
         edit <entry_index>
               set content-type <content-type_name>
         next
      end
      [set exclude-url <exclusion-rule_name>]
   next
end
```

Variable	Description	Default
`<rule_name>`	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: `edit ?`	No default.
`<entry_index>`	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.

Variable	Description	Default
`content-type <content-type_name>`	Specify one of the following content types: • `text/plain` • `text/html` • `application/xml(or)text/xml` • `application/soap+xml` • `application/x-javascript` • `text/css` • `application/javascript` • `text/javascript` To compress multiple file types, add each file type in a separate table entry with its own <entry_index>. See Example.	No default.
`exclude-url <exclusion-rule_name>`	Type the name of an exclusion to use with the rule, if any. See `config waf exclude-url`. The maximum length is 35 characters.	No default.

Example

The following example creates a decompression rule with two content types and one exclusion rule.

```
config waf file-uncompress-rule
   edit "Online Store Uncompress Rule"
         config content-types
            edit 1
               set content-type application/soap+xml
            next
            edit 2
               set content-type application/xml(or)text/xml
            next
         end
      set exclude-url "Uncompress Exclusion"
   next
end
```

Related topics

- `config waf file-compress-rule`
- `config waf exclude-url`

waf file-upload-restriction-policy

Use this command to set the file upload restriction policies that the FortiWeb appliance uses to limit the types of files that can be uploaded to your web servers.

The policies are composed of individual rules set using the `config server-policy custom-application application-policy` command. Each rule identifies the host and/or URL to which the restriction applies and the types of files allowed. To apply a file upload restriction policy, select it within an inline or offline protection profile.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf file-upload-restriction-policy
   edit <file-upload-restriction-policy_name>
      set action {alert | alert_deny | block-period}
      set block-period <seconds_int>
      set severity {High | Medium | Low}
      set trigger <trigger-policy_name>
      set trojan-detection {enable |disable}
      set av-scan {enable |disable}
      set fortisandbox-check {enable |disable}
      config rule
         edit <entry_index>
            set file-upload-restriction-rule <rule_name>
         next
      end
   next
end
```

Variable	Description	Default
`<file-upload-restriction-policy_name>`	Type the name of an existing or new file upload restriction policy. The maximum length is 35 characters. To display the list of existing policies, type: `edit ?`	No default.

Variable	Description	Default
action {alert | alert_deny | block-period}	Type the action you want FortiWeb to perform when the policy is violated: • alert — Accept the request and generate an alert 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 FortiWeb returns to the client with the HTTP status code. See the *FortiWeb Administration Guide* or config system replacemsg. • block-period — Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int>. **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 config waf x-forwarded-for). Failure to do so may cause FortiWeb to block **all** connections when it detects a violation of this type. **Caution:** This setting will be ignored if monitor-mode {enable | disable} is enabled. **Note:** Logging and/or alert email will occur only if enabled and configured. See config log disk and config log alertemail. **Note:** If an auto-learning profile will be selected in the policy with offline protection profiles that use this rule, you should select alert. If the action is alert_deny, the FortiWeb appliance will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see config waf web-protection-profile autolearning-profile.	alert
severity {High | Medium | Low}	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	Low
trigger <trigger-policy_name>	Type the name of the trigger to apply when this policy is violated (see config log trigger-policy). The maximum length is 35 characters. To display the list of existing triggers, type: set trigger ?	No default.

Variable	Description	Default
`trojan-detection {enable |disable}`	Enter `enable` to scan for Trojans. Attackers may attempt to upload Trojan horse code (written in scripting languages such as PHP and ASP) to the back-end web servers. The Trojan then infects clients who access an infected web page.	`disable`
`av-scan {enable |disable}`	Enter `enable` to scan for viruses, malware, and greyware.	`disable`
`fortisandbox-check {enable |disable}`	Specify `enable` to send matching files to FortiSandbox for evaluation. Also specify the FortiSandbox settings for your FortiWeb. See `config system fortisandbox`. FortiSandbox evaluates the file and returns the results to FortiWeb. If `av-scan` is `enable` and FortiWeb detects a virus, it does not send the file to FortiSandbox.	`disable`
`block-period <seconds_int>`	If `action` is `block-period`, type the number of seconds that violating requests will be blocked. The valid range is from 1 to 3,600 seconds.	1
`<entry_index>`	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
`file-upload-restriction-rule <rule_name>`	Type the name of an upload restriction rule to use with the policy, if any. See `config server-policy custom-application application-policy`. The maximum length is 35 characters. To display the list of existing rules, type: `set file-upload-restriction-rule ?`	No default.

Related topics

- `config server-policy custom-application application-policy`
- `config log trigger-policy`
- `config system fortisandbox`

waf file-upload-restriction-rule

Use this command to define the specific host and request URL for which file upload restrictions apply, and define the specific file types that can be uploaded to that host or URL.

To apply the rule, select it in a file upload restriction policy. See `config server-policy custom-application application-policy`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf file-upload-restriction-rule
   edit waf file-upload-restriction-rule
      set host-status {enable | disable}
      set host <protected-host_name>
      set request-file <url_pattern>
      set request-type {regular | plain}
      [set file-size-limit <size_int>]
      config file-types
         edit waf file-upload-restriction-rule
            set file-type-id <id_str>
            set file-type_name <file-type-extension_str>
         next
      end
   next
end
```

Variable	Description	Default
`<file-upload-restriction-rule_name>`	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: `edit ?`	No default.
`host-status {enable | disable}`	Enable to apply this exception only to HTTP requests for specific web hosts. Also configure analyzer-policy <fortianalyzer-policy_name>. Disable to match the exception based upon the other criteria, such as the URL, but regardless of the `Host:` field.	`disable`
`host <protected-host_name>`	Type the name of a protected host that the `Host:` field of an HTTP request must be in order to match the rule. The maximum length is 255 characters. This setting applies only if `host-status` is `enable`.	No default.

Variable	Description	Default
request-file <url_pattern>	Depending on your selection in waf file-upload-restriction-rule, type either: • the literal URL, such as /fileupload, that the HTTP request must contain in order to match the signature exception. The URL must begin with a slash (/). • a regular expression, such as ^/*.php, matching all and only the URLs to which the signature exception should apply. The pattern is **not** required to begin with a slash (/). However, it must at least match URLs that begin with a slash, such as /index.cfm. Do not include the name of the web host, such as www.example.com, which is configured separately in analyzer-policy <fortianalyzer-policy_name>. The maximum length is 255 characters. **Note:** Regular expressions beginning with an exclamation point (!) are not supported. For information on language and regular expression matching, see the *FortiWeb Administration Guide*.	No default.
request-type {regular | plain}	Select whether analyzer-policy <fortianalyzer-policy_name> will contain a literal URL (plain), or a regular expression designed to match multiple URLs (regular).	plain
file-size-limit <size_int>	Optionally, enter a number to represent the maximum size in kilobytes for any individual file. This places a size limit on allowed file types. The valid range is from 0 to 30720 KB (30 MB).	0
<entry_index>	Type the index number of the individual entry in the table. Each entry in the table can define one file type. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.

Variable	Description	Default
file-type-id <id_str>	Select the numeric type ID that corresponds to the file type. Recognized IDs are updated by FortiGuard services and may vary. For a list of available IDs, select all file types in the GUI, then use the CLI to view their corresponding IDs. Common IDs include: • 00001 (GIF) • 00002 (JPG) • 00003 (PDF) • 00004 (XML) • 00005 (MP3) • 00006 (MIDI) • 00007 (WAVE) • 00008 (FLV for a Macromedia Flash Video) • 00009 (RAR) • 00010 (ZIP) • 00011 (BMP) • 00012 (RM for RealMedia) • 00013 (MPEG for MPEG v) • 00014 (3GPP)	No default.
file-type_name <file-type-extension_str>	Type the extension, such as MP3, of the file type to allow to be uploaded. Recognized file types are updated by FortiGuard services and may vary. For a list of available names, use the GUI. **Note:** 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.	No default.

Example

This example allows both MPEG and FLV files uploaded to the URL `/file-uploads` on the host `www.example.com`.

```
config waf file-upload-restriction-rule
   edit file-upload-rule1
      set host-status enable
      set host www.example.com
      set request-file /file-uploads
      config file-types
         edit 1
            set file-type-id 00013
```

```
            set file-type-name MPEG
          next
          edit 2
            set file-type-id 00008
            set file-type-name FLV
          next
        end
    next
end
```

Related topics

- `config server-policy custom-application application-policy`

waf geo-block-list

Use this command to define large sets of client IP addresses to block based upon their associated geographical location.

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.

Optionally, you can also specify a list of IP addresses or IP address ranges that are exempt from this blacklist (see `config waf geo-ip-except`).

Alternatively, you can block clients individually (see `config server-policy custom-application application-policy`) or based upon their reputation (see `config waf ip-intelligence`).

To apply the rule, select it in a protection profile. See `config waf web-protection-profile inline-protection` or `config waf web-protection-profile offline-protection`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf geo-block-list
  edit <geography-to-ip_name>
    set severity {High | Medium | Low}
    set trigger <trigger-policy_name>
    set exception-rule <geo-ip-except_name>
    config country-list
      edit <entry_index>
        set country-name "<region_name>"
      next
    end
  next
end
```

Variable	Description	Default
<geography-to-ip_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: edit ?	No default.
severity {High | Medium | Low}	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	Low
trigger <trigger-policy_name>	Type the name of the trigger to apply when this rule is violated (see config log trigger-policy). The maximum length is 35 characters. To display the list of existing trigger policies, type: set trigger ?	No default.
exception-rule <geo-ip-except_name>	Type the name of a list of exceptions to this blacklist.	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
country-name "<region_name>"	Type the name of a region (Antarctica or Bouvet Island) or country (U.S.) as it is written in English. Surround names with multiple words or apostrophes in double quotes. The list of locations varies by the currently installed IP-to-geography mapping package. For a current list of locations, use the web UI.	No default.

Example

This example creates a set of North American IP addresses that a server policy can use to block clients with IP addresses belonging to Belize and Canada. FortiWeb does not block the IP addresses specified by the allow-north-america exception list.

```
config waf geo-block-list
   edit "north-america"
      set trigger "notification-servers1"
      set exception rule "allow-north-america"
      set severity Low
      config country-list
         edit 1
            set country-name "Belize"
         next
         edit 2
            set country-name "Canada"
         next
      end
```

```
    next
  end
```

Related topics

- config log trigger-policy
- config waf geo-ip-except
- config waf web-protection-profile inline-protection
- config waf web-protection-profile offline-protection
- config server-policy custom-application application-policy
- config waf ip-intelligence
- diagnose debug flow trace

waf geo-ip-except

Use this command to specify IP addresses or ranges of IP addresses that are exceptions to the list of client IP addresses that FortiWeb blocks based on their geographic location.

For information on creating the blacklist by country or region, see config waf geo-block-list.

To use this command, your administrator account's access control profile must have either w or rw permission to the wafgrp area. For more information, see Permissions on page 74.

Syntax

```
config waf geo-ip-except
   edit <geo-ip-except_name>
        edit <entry_index>
           set ip {address_ipv4 | ip_range_ipv4}
        next
     end
   next
end
```

Variable	Description	Default
<geo-ip-except_name>	Type the name of a new or existing list of exceptions. To display the list of existing rules, type: edit ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
ip {address_ipv4 | ip_range_ipv4}	Type the IP address or IP address range that is exempt from blocking based on its geographic location.	No default.

Example

This example adds the IP address range 192.0.2.0 to 192.0.2.5 to the geolocation blacklist exception list `allow-north-america`.

```
config waf geo-ip-except
   edit "allow-north-america"
      set ip 192.0.2.0-192.0.2.5
      end
   next
end
```

Related topics

- `config waf geo-block-list`
- `config server-policy custom-application application-policy`
- `config waf ip-intelligence`
- `diagnose debug flow trace`

waf hidden-fields-protection

Use this command to configure groups of hidden field rules.

To apply hidden field rule groups, select them within an inline protection profile. For details, see `config waf web-protection-profile inline-protection`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf hidden-fields-protection
   edit <hidden-field-group_name>
      config hidden_fields_list
         edit <entry_index>
            set hidden-field-rule <hidden-field-rule_name>
         next
      end
   next
end
```

Variable	Description	Default
`<hidden-field-group_name>`	Type the name of a new or existing hidden field rule group. The maximum length is 35 characters. To display the list of existing groups, type: `edit ?`	No default.

Variable	Description	Default
`<entry_index>`	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
`hidden-field-rule <hidden-field-rule_name>`	Type the name of an existing hidden field rule to add to the group. The maximum length is 35 characters. To display the list of existing rules, type: `set hidden-field-rule ?`	No default.

Related topics

- `config waf hidden-fields-rule`
- `config waf web-protection-profile inline-protection`

waf hidden-fields-rule

Use this command to configure hidden field rules.

Hidden form inputs, like other types of parameters and inputs, can be vulnerable to tampering and can be used as a vector for other attacks.

Unlike other inputs, they are often written into an HTML page by the web server when it serves that page to the client, and are not visible on the rendered web page. As such, they are difficult to for users to unintentionally modify, and are often incorrectly perceived as relatively safe by web site owners.

Like other inputs, however, they are accessible through the JavaScript document object model (DOM), and as inputs, can be used to inject invalid data into your databases or attempt to tamper with the session state.

Hidden field rules prevent such tampering. The FortiWeb appliance caches the values of a session's hidden inputs as they pass to the HTTP client, and verifies that they remain unchanged when the HTTP client submits a form.

You apply hidden field constraints by first grouping them into a hidden field group. For details, see `config waf hidden-fields-protection`.

Before you configure a hidden field rule, if you want to apply it only to HTTP requests for a specific real or virtual host, you must first define the web host in a protected hosts group. For details, see `config server-policy allow-hosts`.

Alternatively, you can use the web UI to fetch the request URL from the server and scan it for hidden inputs, using the results to configure the hidden input rule. For details, see the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf hidden-fields-rule
   edit <hidden-field-rule_name>
      set action {alert | alert_deny | redirect | block-period | send_403_
          forbidden}
      set block-period <seconds_int>
      set host <protected-hosts_name>
      set host-status {enable | disable}
      set request-file <url_str>
      set action-url0 <url_str>
      set action-url1 <url_str>
      set action-url2 <url_str>
      set action-url3 <url_str>
      set action-url4 <url_str>
      set action-url5 <url_str>
      set action-url6 <url_str>
      set action-url7 <url_str>
      set action-url8 <url_str>
      set action-url9 <url_str>
      set analyzer-policy <fortianalyzer-policy_name>
      set analyzer-policy <fortianalyzer-policy_name>
      config hidden-field-name
         edit <entry_index>
            set argument <hidden-field_str>
         next
      end
   next
end
```

Variable	Description	Default
<hidden-field-rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: `edit ?`	No default.

Variable	Description	Default
action {alert | alert_deny | redirect | block-period | send_403_forbidden}	Select one of the following actions that the FortiWeb appliance will perform when an HTTP request violates one of the hidden field rules in the entry: • 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 FortiWeb returns to the client with the HTTP status code. See the *FortiWeb Administration Guide* or config system replacemsg. • block-period — Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int>. **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 config waf x-forwarded-for). 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 and generate an alert email and/or log message. Also configure redirect-url <redirect_fqdn> and rdt-reason {enable | disable}. • send_403_forbidden — Reply to the client with an HTTP 403 Access Forbidden error message and generate an alert email and/or log message. **Caution:** This setting will be ignored if monitor-mode {enable | disable} is enabled. **Note:** Logging and/or alert email will occur only if enabled and configured. See config log disk and config log alertemail. **Note:** If you select an auto-learning profile with this rule, you should select alert. If the action is alert_deny, for example, the FortiWeb appliance will block the request or reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see config waf web-protection-profile autolearning-profile.	alert
block-period <seconds_int>	If action is block-period, type the number of seconds that the connection will be blocked. The valid range is from 1 to 3,600 seconds.	0

Variable	Description	Default
`host <protected-hosts_name>`	Type the name of a protected host that the `Host:` field of an HTTP request must be in order to match the rule. The maximum length is 255 characters. This setting applies only if `host-status` is `enable`.	No default.
`host-status {enable | disable}`	Enable to apply this hidden field rule only to HTTP requests for specific web hosts. Also configure host <protected-hosts_name>. Disable to match the input rule based upon the other criteria, such as the URL, but regardless of the `Host:` field.	`disable`
`request-file <url_str>`	Type the literal URL, such as `/login.jsp`, that contains the hidden form. The URL must begin with a slash (/). Do not include the name of the web host, such as `www.example.com`, which is configured separately in host <protected-hosts_name>. Regular expressions are not supported. The maximum length is 255 characters.	No default.
`action-url0 <url_str>`	Add up to 10 URLs that are valid to use with the HTTP `POST` method when the client submits the form containing the hidden fields in this rule.	No default.
`action-url1 <url_str>`		
`action-url2 <url_str>`		
`action-url3 <url_str>`		
`action-url4 <url_str>`		
`action-url5 <url_str>`		
`action-url6 <url_str>`		
`action-url7 <url_str>`		
`action-url8 <url_str>`		
`action-url9 <url_str>`		
`severity {High | Medium | Low}`	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	`High`

Variable	Description	Default
`trigger <trigger-policy_name>`	Type the name of the trigger to apply when this rule is violated (see `config log trigger-policy`). The maximum length is 35 characters. To display the list of existing trigger policies, type: `set trigger ?`	No default.
`<entry_index>`	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
`argument <hidden-field_str>`	Type the name of the hidden form input, such as `languagepref`. The maximum length is 35 characters.	No default.

Example

This example blocks and logs requests from search.jsp if its hidden form input, whose name is “languagepref”, is posted to any URL other than query.do.

```
config waf hidden-fields-rule
   edit "hidden_fields_rule1"
      set action alert_deny
      set request-file "/search.jsp"
      set action-url0 "/query.do"
      config hidden-field-name
         edit 1
            set argument "languagepref"
         next
      end
   next
end
```

Related topics

- `config server-policy allow-hosts`
- `config waf hidden-fields-protection`
- `config log trigger-policy`

waf http-authen http-authen-policy

Use this command to group HTTP authentication rules into HTTP authentication policies.

The FortiWeb appliance uses authentication policies with the HTTP authentication feature to authorize HTTP requests. For details, see the *FortiWeb Administration Guide*.

To apply HTTP authentication policies, select them in an inline protection profile. For details, see `config waf web-protection-profile inline-protection`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf http-authen http-authen-policy
   edit <auth-policy_name>
      set cache {enable | disable}
      set analyzer-policy <fortianalyzer-policy_name>
      set cache-timeout <timeout_int>
      set auth-timeout <timeout_int>
      config rule
         edit <entry_index>
            set http-authen-rule <http-auth-rule_name>
         next
      end
   next
end
```

Variable	Description	Default
`<auth-policy_name>`	Type the name of a new or existing HTTP authentication policy. The maximum length is 35 characters. To display the list of existing policies, type: `edit ?`	No default.
`cache {enable | disable}`	Enable to cache client user names and passwords from remote authentication such as LDAP queries. Also configure cache-timeout <timeout_int>. This can be used can improve performance by preventing frequent queries.	No default.
`alert-type {none | fail | success | all}`	Type the instances when alerts will be issued for HTTP authentication attempts: • `none` — No alerts are issued for HTTP authentication. • `fail` — Alerts are issued only for HTTP authentication failures. • `success` — Alerts are issued for successful HTTP authentication. • `all` — Alerts are issued for all failed and successful HTTP authentication.	`none`
`cache-timeout <timeout_int>`	Type the query cache timeout, in seconds. The valid range is from 0 to 3,600 seconds. This option is available only when `cache` is enabled.	`300`

Variable	Description	Default
`auth-timeout <timeout_int>`	Type the connection timeout for the query to the FortiWeb's query to the remote authentication server in milliseconds. The valid range is from 0 to 60,000 milliseconds. If the authentication server does not answer queries quickly enough, to prevent dropped connections, increase this value.	`2000`
`<entry_index>`	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
`http-authen-rule <http-auth-rule_name>`	Type the name of an existing HTTP authentication rule. The maximum length is 35 characters. To display the list of existing rules, type: `set http-authen-rule ?`	No default.

Example

This example first configures a user group that contains both a local user account and an LDAP query.

```
config user user-group
   edit "user-group1"
      config members
         edit 1
            set type local
            set local-name "user1"
         next
         edit 2
            set ldap-name "user2"
            set type ldap
         next
      end
   next
end
```

Second, it configures a rule that requires basic HTTP authentication when requesting the URL `/employees/holidays.html` on the host `www.example.com`. This URL will be identified as belonging to the realm named "Restricted Area". Users belonging to `user-group1` can authenticate.

```
config waf http-authen http-authen-rule
   edit "auth-rule1"
      set host-status enable
      set host "www.example.com"
      config rule
         edit 1
            set request-url "/employees/holidays.html"
            set authen-type basic
            set user-group "user-group1"
            set user-realm "Restricted Area"
         next
      end
   next
```

```
end
```

Third, it groups two HTTP authentication rules into an HTTP authentication policy that can be applied in an inline protection profile.

```
config waf http-authen http-authen-policy
   edit "http-auth-policy1"
      config rule
         edit 1
            set http-authen-rule "http-auth-rule1"
         next
         edit 2
            set http-authen-rule "http-auth-rule2"
         next
      end
   next
end
```

Related topics

- config waf http-authen http-authen-rule
- config waf web-protection-profile inline-protection

waf http-authen http-authen-rule

Use this command to configure HTTP authentication rules.

Authentication rules are used by the HTTP authentication feature to define sets of request URLs that will be authorized for each user group.

You apply authentication rules by adding them to an authentication policy, which is ultimately selected within an inline protection profile for use in web protection. For details, see config waf http-authen http-authen-policy.

To use this command, your administrator account's access control profile must have either w or rw permission to the wafgrp area. For more information, see Permissions on page 74.

Syntax

```
config waf http-authen http-authen-rule
   edit <auth-rule_name>
      set host <protected-hosts_name>
      set host-status {enable | disable}
      config rule
         edit <entry_index>
            set authen-type {basic | digest | ntlm}
            set request-url <path_str>
            set user-group <user-group_name>
            set user-realm <realm_str>
         next
      end
   next
end
```

Variable	Description	Default
`<auth-rule_name>`	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: `edit ?`	No default.
`host <protected-hosts_name>`	Type the name of a protected host that the `Host:` field of an HTTP request must be in order to match the HTTP authentication rule. The maximum length is 255 characters. This setting applies only if `host-status` is `enable`.	No default.
`host-status {enable | disable}`	Enable to apply this HTTP authentication rule only to HTTP requests for specific web hosts. Also configure host <protected-hosts_name>. Disable to match the HTTP authentication rule based upon the other criteria, such as the URL, but regardless of the `Host:` field.	`disable`
`<entry_index>`	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
`authen-type {basic | digest | ntlm}`	Select which type of HTTP authentication to use, either: • `basic` — Clear text, Base64-encoded user name and password. Supports local user accounts, and RADIUS and LDAP user queries. NTLM user queries are not supported. • `digest` — Hashed user name, realm, and password. RADIUS, LDAP and NTLM user queries are not supported. • `ntlm` — Encrypted user name and password. Local user accounts and RADIUS and LDAP user queries are not supported.	`basic`
`request-url <path_str>`	Type the literal URL, such as `/employees/holidays.html`, that a request must match in order to trigger HTTP authentication. The maximum length is 255 characters.	No default.
`user-group <user-group_name>`	Type the name of a user group that is authorized to use the URL in request-url <path_str>. The maximum length is 35 characters. To display the list of existing user groups, type: `set user-group ?`	No default.

Variable	Description	Default
user-realm <realm_str>	Type the realm, such as `Restricted Area`, to which the request-url <path_str> belongs. The maximum length is 35 characters. Browsers often use the realm multiple times. • It may appear in the browser's prompt for the user's credentials. Especially if a user has multiple logins, and only one login is valid for that specific realm, displaying the realm helps to indicate which user name and password should be supplied. • After authenticating once, the browser may cache the authentication credentials for the duration of the browser session. If the user requests another URL from the same realm, the browser often will automatically re-supply the cached user name and password, rather than asking the user to enter them again for each request. The realm may be the same for multiple authentication rules, if all of those URLs permit the same user group to authenticate. For example, the user group `All_Employees` could have access to the request-url <path_str> URLs `/wiki/Main` and `/wiki/ToDo`. These URLs both belong to the realm named `Intranet Wiki`. Because they use the same realm name, users authenticating to reach `/wiki/Main` usually will not have to authenticate again to reach `/wiki/ToDo`, as long as both requests are within the same browser session. This field does not appear if `authen-type` is `ntlm`, which does not support HTTP-style realms.	No default.

Example

For an example, see `config waf http-authen http-authen-policy`.

Related topics

- `config user user-group`
- `config waf http-authen http-authen-policy`

waf http-connection-flood-check-rule

Use this command to 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 `config waf layer4-connection-flood-check-rule`. 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.

To apply this rule, include it in an application-layer DoS-prevention policy. See `config waf application-layer-dos-prevention`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf http-connection-flood-check-rule
   edit <rule_name>
      set action {alert | alert_deny | block-period}
      set block-period <seconds_int>
      set http-connection-threshold <limit_int>
      set severity {High | Medium | Low}
      set trigger-policy <trigger-policy_name>
   next
end
```

Variable	Description	Default
`<rule_name>`	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: `edit ?`	No default.

Variable	Description	Default
action {alert | alert_deny | block-period}	Select one of the following actions that the FortiWeb appliance will perform when the count exceeds the rate limit: • alert — Accept the connection and generate an alert email and/or log message. • alert_deny — Block the connection and generate an alert email and/or log message. • block-period — Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int>. **Caution:** This setting will be ignored if monitor-mode {enable | disable} is enabled. **Note:** Logging and/or alert email will occur only if enabled and configured. See config log disk and config log alertemail. **Note:** If an auto-learning profile will be selected in the policy with offline protection profiles that use this rule, you should select alert. If the action is alert_deny, the FortiWeb appliance will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see config waf web-protection-profile autolearning-profile.	alert
block-period <seconds_int>	Type the length of time for which the FortiWeb appliance will block additional requests after a client exceeds the rate threshold. The valid range is from 1 to 3,600 seconds.	1
http-connection-threshold <limit_int>	Type the maximum number of TCP connections allowed from the same client. The valid range is from 1 to 1,024.	1
severity {High | Medium | Low}	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	Medium
trigger-policy <trigger-policy_name>	Type the name of the trigger to apply when this rule is violated (see config log trigger-policy). The maximum length is 35 characters. To display the list of existing trigger policies, type: set trigger ?	No default.

Related topics

- config log trigger-policy
- config waf application-layer-dos-prevention

waf http-constraints-exceptions

Use set statements under this command to configure exceptions to existing HTTP protocol parameter constraints for specific hosts.

Exceptions may be useful if you know that some HTTP protocol constraints, during normal use, will cause false positives by matching an attack signature. Exceptions define HTTP constraints that will **not** be subject to HTTP protocol constraint policy.

For example, if you enable `max-http-header-length` in a HTTP protocol constraint exception for a specific host, FortiWeb ignores the HTTP header length check when executing the web protection profile for that host.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf http-constraints-exceptions
   edit <http-exception_name>
      config http_constraints-exception-list
         edit <entry_index>
            set request-file <url_pattern>
            set request-type {plain | regular}
            set host-status {enable | disable}
            set block-malformed-request {enable | disable}
            set Illegal-content-length-check {enable | disable}
            set Illegal-content-type-check {enable | disable}
            set Illegal-header-name-check {enable | disable}
            set Illegal-header-value-check {enable | disable}
            set Illegal-host-name-check {enable | disable}
            set Illegal-http-request-method-check {enable | disable}
            set Illegal-responese-code-check {enable | disable}
            set max-cookie-in-request {enable | disable}
            set max-header-line-request {enable | disable}
            set max-http-body-length {enable | disable}
            set max-http-body-parameter-length {enable | disable}
            set max-http-content-length {enable | disable}
            set max-http-header-length {enable | disable}
            set max-http-header-line-length {enable | disable}
            set max-http-header-name-length {enable | disable}
            set max-http-header-value-length {enable | disable}
            set max-http-parameter-length {enable | disable}
            set max-http-request-filename-length {enable | disable}
            set max-http-request-length {enable | disable}
            set max-url-parameter {enable | disable}
            set max-url-parameter-length {enable | disable}
            set number-of-ranges-in-range-header {enable | disable}
            set parameter-name-check {enable | disable}
```

```
            set parameter-value-check {enable | disable}
        next
    end
  next
end
```

Variable	Description	Default
<http-exception_name>	Type the name of a new or existing HTTP protocol constraint exception. The maximum length is 35 characters. To display the list of existing exceptions, type: edit ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
request-file <url_pattern>	Type either: • the literal URL, such as /index.php, that the HTTP request must contain in order to match the input rule. The URL must begin with a slash (/). • a regular expression, such as ^/*.php, matching all and only the URLs to which the input rule should apply. The pattern is **not** required to begin with a slash (/). However, it must at least match URLs that begin with a slash, such as /index.cfm. Do not include the name of the web host, such as www.example.com, which is configured separately in host. The maximum length is 255 characters.	No default.
request-type {plain | regular}	Type either plain or regular (for a regular expression) to match the string entered in request-file.	No default.
host-status {enable | disable}	Enable to apply this exception only to HTTP requests for specific web hosts. Also configure analyzer-policy <fortianalyzer-policy_name>. Disable to match the exception based upon the other criteria, such as the URL, but regardless of the Host: field.	disable
block-malformed-request {enable | disable}	Enable to omit the constraint on syntax and FortiWeb parsing errors. **Caution:** Some web applications require abnormal or very large HTTP POST 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.	

Variable	Description	Default
`Illegal-content-length-check {enable | disable}`	Enable to omit the constraint on the maximum acceptable size in bytes of the request body.	`disable`
`Illegal-content-type-check {enable | disable}`	Enable to omit the constraint on whether the `Content Type:` value uses the format `<type>/<subtype>`.	`disable`
`Illegal-header-name-check {enable | disable}`	Enable to omit the constraint on whether the HTTP header name contains illegal characters.	`disable`
`Illegal-header-value-check {enable | disable}`	Enable to omit the constraint on whether the HTTP header value contains illegal characters.	`disable`
`Illegal-host-name-check {enable | disable}`	Enable to omit the constraint on host names with illegal characters.	`disable`
`Illegal-http-request-method-check {enable | disable}`	Enable to omit the constraint on illegal HTTP request methods.	`disable`
`Illegal-responese-code-check {enable | disable}`	Enable to omit the constraint on whether the HTTP response code is a 3-digit number.	`disable`
`max-cookie-in-request {enable | disable}`	Enable to omit the constraint on the maximum number of cookies per request.	`disable`
`max-header-line-request {enable | disable}`	Enable to omit the constraint on the maximum number of HTTP header lines.	`disable`
`max-http-body-length {enable | disable}`	Enable to omit the constraint on the maximum HTTP body length.	`disable`
`max-http-body-parameter-length {enable | disable}`	Enable to omit the constraint on the maximum acceptable size in bytes of all parameters in the HTTP body of HTTP POST requests.	`disable`
`max-http-content-length {enable | disable}`	Enable to omit the constraint on the maximum HTTP content length.	`disable`
`max-http-header-length {enable | disable}`	Enable to omit the constraint on the maximum HTTP header length.	`disable`
`max-http-header-line-length {enable | disable}`	Enable to omit the constraint on the maximum HTTP header line length.	`disable`
`max-http-header-name-length {enable | disable}`	Enable to omit the constraint on the maximum acceptable size in bytes of a single HTTP header name.	`disable`

Variable	Description	Default
`max-http-header-value-length {enable | disable}`	Enable to omit the constraint on the maximum acceptable size in bytes of a single HTTP header value.	`disable`
`max-http-request-filename-length {enable | disable}`	Enable to omit the constraint on the maximum HTTP request filename length.	`disable`
`max-http-parameter-length {enable | disable}`	Enable to omit the constraint on the maximum HTTP parameter length.	`disable`
`max-http-request-length {enable | disable}`	Enable to omit the constraint on the maximum HTTP request length.	`disable`
`max-url-parameter {enable | disable}`	Enable to omit the constraint on the maximum number of parameters in the URL.	`disable`
`max-url-parameter-length {enable | disable}`	Enable to omit the constraint on the maximum length of parameters in the URL.	`disable`
`number-of-ranges-in-range-header {enable | disable}`	Enable to omit the constraint on the maximum acceptable number of `Range:` fields of an HTTP header.	`disable`
`parameter-name-check {enable | disable}`	Enable to omit the constraint on null characters in parameter names.	`disable`
`parameter-value-check {enable | disable}`	Enable to omit the constraint on null characters in parameter values.	`disable`
`Post-request-ctype-check {enable | disable}`	Enable to omit the constraint on whether the `Content-Type:` header is available.	`disable`

Example

This example omits header length limits for HTTP requests to www.example.com and 10.0.0.1 for /login.asp.

```
config waf http-constraints-exceptions
   edit "exception1"
      config http_constraints-exception-list
         edit 1
            set host "www.example.com"
            set host-status enable
            set max-http-header-length enable
            set request-file "/login.asp"
            next
         edit 2
            set host "10.0.0.1"
            set host-status enable
            set max-http-body-length enable
            set request-file "/login.asp"
```

```
            next
          end
      next
    end
```

Related topics

- config waf web-protection-profile inline-protection
- config waf web-protection-profile offline-protection
- config log trigger-policy
- config waf http-protocol-parameter-restriction

waf http-protocol-parameter-restriction

Use this command to configure HTTP protocol constraints.

HTTP 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 content payload.

Use protocol constraints to prevent attacks such as buffer overflows in web servers that do not restrict elements of the HTTP protocol to acceptable lengths, or mishandle malformed requests. Such errors can lead to security vulnerabilities.

You can also use protocol constraints to block requests that are too large for the memory size you have configured for FortiWeb's scan buffers. If your web applications do not require large HTTP `POST` requests, configure block-malformed-request-check {enable | disable} on page 400 to harden your configuration. To configure the buffer size, see max-http-argbuf-length {8k-cache | 12k-cache | 32k-cache | 64k-cache} on page 222.

You can configure each protocol parameter independently with an action, severity and trigger that determines how an attack on that parameter is handled. For example, you can set the action for header constraints to alert, the severity to high, and a trigger set to deliver an email each time FortiWeb detects a violation of these protocol parameters.

To apply HTTP protocol constraints, select them in an inline or offline protection profile. For details, see config waf web-protection-profile inline-protection or config waf web-protection-profile offline-protection.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf http-protocol-parameter-restriction
   edit <http-constraint_name>
      set block-malformed-request-check {enable | disable}
      set Illegal-content-length-check {enable | disable}
      set Illegal-content-type-check {enable | disable}
      set Illegal-header-name-check {enable | disable}
      set Illegal-header-value-check {enable | disable}
```

```
        set Illegal-host-name-check {enable | disable}
        set Illegal-http-request-method-check {enable | disable}
        set Illegal-http-version-check {enable | disable}
        set Illegal-response-code-check {enable | disable}
        set max-cookie-in-request <limit_int>
        set max-header-line-request <limit_int>
        set max-http-body-length <limit_int>
        set max-http-content-length <limit_int>
        set max-http-header-length <limit_int>
        set max-http-header-name-length <limit_int>
        set max-http-header-value-length <limit_int>
        set max-http-parameter-length <limit_int>
        set max-http-request-filename-length <limit_int>
        set max-http-request-length <limit_int>
        set max-url-parameter <limit_int>
        set max-url-parameter-length <limit_int>
        set number-of-ranges-in-range-header <limit_int>
        set parameter-name-check {enable | disable}
        set parameter-value-check {enable | disable}
        set Post-request-ctype-check {enable | disable}
        set web-socket-protocol-check {enable | disable}
        set waf http-protocol-parameter-restriction
        set <parameter_name>-action {alert | alert_deny | block-period}
        set <parameter_name>-severity {High | Medium | Low}
        set <parameter_name>-trigger <trigger-policy_name>
        set <parameter_name>-block-period <seconds_int>
        [set exception_name <http-exception_name>]
    next
end
```

Variable	Description	Default
<http-constraint_name>	Type the name of a new or existing HTTP protocol constraint. The maximum length is 35 characters. To display the list of existing constraints, type: edit ?	No default.

Variable	Description	Default
`block-malformed-request-check {enable | disable}`	Enable to block the request if either: • it has syntax errors • parsing errors occur while FortiWeb is scanning the request (see `diagnose debug flow trace`) These can cause problems in web servers that do not handle them gracefully. Such problems can lead to security vulnerabilities. **Caution:** Fortinet strongly recommends to enable this option **unless** large requests or 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. **Unless you enable this option to block oversized items, FortiWeb will allow oversized those requests to pass through without scanning.** This could allow attackers to craft large attacks to bypass your FortiWeb policies, and reach your web servers. If feasible, instead of disabling this option: • enlarge the scan buffers (see max-http-argbuf-length {8k-cache | 12k-cache | 32k-cache | 64k-cache} on page 222) • omit this only for URLs that require oversized parameters (see `config server-policy custom-application application-policy`) **Note:** Do **not** enable this option if requests normally contain: • parameters larger than the scan buffer (Buffer size is configurable — see max-http-argbuf-length {8k-cache | 12k-cache | 32k-cache | 64k-cache} on page 222.) • large numbers of parameters • more than 32 cookies Requests like this will be flagged as potentially malformed by FortiWeb's parser, causing FortiWeb to block normal requests.	`enable`
`Illegal-content-length-check {enable | disable}`	Enable to check whether the `Content-Length:` header includes numeric characters only.	`disable`
`Illegal-content-type-check {enable | disable}`	Enable to check whether the `Content Type:` value has the format `<type>/<subtype>`.	`disable`
`Illegal-header-name-check {enable | disable}`	Enable to check whether the HTTP header name contains illegal characters.	`disable`

Variable	Description	Default
`Illegal-header-value-check {enable | disable}`	Enable to check whether the HTTP header value contains illegal characters.	`disable`
`Illegal-host-name-check {enable | disable}`	Enable to check the `Host:` line of the HTTP header for illegal characters, such as null or encoded characters like `0x0` or `%00*`.	`enable`
`Illegal-http-request-method-check {enable | disable}`	Enable to check for invalid HTTP request methods according to RFC 2616 or RFC 4918. FortiWeb considers any method that is not defined in these RFCs to be illegal. Thus, illegal methods including misspellings like GETT and other HTTP extension methods (for example, CalDAV) like MKCALENDAR.	`enable`
`Illegal-http-version-check {enable | disable}`	Enable to check for illegal HTTP version numbers. If the HTTP version is not “HTTP/1.0” or “HTTP/1.1”, it is considered illegal.	`enable`
`Illegal-response-code-check {enable | disable}`	Enable to check whether the HTTP response code is a 3-digit number.	`enable`
`max-cookie-in-request <limit_int>`	Type the maximum acceptable number of cookies in an HTTP request. The valid range is from 0 to 32.	`16`
`max-header-line-request <limit_int>`	Type the maximum acceptable number of lines in the HTTP header. The valid range is from 0 to 32.	32
`max-http-body-length <limit_int>`	Type the maximum acceptable length in kilobytes of the HTTP body. The valid range is from 0 to 65536. To disable the limit, type `0`.	`0`
`max-http-body-parameter-length <limit_int>`	Type the total maximum acceptable size in bytes of all the parameters in the HTTP body of HTTP `POST` requests. Question mark (?), ampersand (&), and equal (=) characters are not included.	`8192`
`max-http-content-length <limit_int>`	Type the maximum acceptable length in kilobytes of the request body. Length is determined by comparing this limit with the value of the `Content-Length:` field in the HTTP header. The valid range is from 0 to 65536. To disable the limit, type `0`.	`0`

Variable	Description	Default
`max-http-header-length <limit_int>`	Type the maximum acceptable length in bytes of the HTTP header. The valid range is from 0 to 12,288. To disable the limit, type `0`.	`4096`
`max-http-header-name-length <limit_int>`	Specifies the maximum acceptable size in bytes of a single HTTP header name (for example, `Host:`, `Content-Type:`, `User-Agent:`).	`50`
`max-http-header-value-length <limit_int>`	Specifies the maximum acceptable size of a single HTTP header value, in bytes.	`4096`
`max-http-parameter-length <limit_int>`	Type the total maximum total acceptable length in bytes of all parameters in the URL and/or, for HTTP `POST` requests, the HTTP body. Question mark (?), ampersand (&), and equal (=) characters are not included. The valid range is from 0 to 65,536. To disable the limit, type `0`.	`6144`
`max-http-request-filename-length <limit_int>`	Specifies the maximum acceptable length in bytes of the HTTP request filename. The valid range is from 0 to 65536. To disable the limit, type `0`.	`2048`
`max-http-request-length <limit_int>`	Type the maximum acceptable length in kilobytes of the HTTP request. The valid range is from 0 to 65536. To disable the limit, type `0`.	`67108864`
`max-url-parameter <limit_int>`	Type the maximum number of URL parameters. The valid range is from 1 to 64.	`16`
`max-url-parameter-length <limit_int>`	Type the total maximum acceptable length in bytes of all parameters, including their names and values, in the URL. Parameters usually appear after a `?`, such as: `/url?parameter=value` It does **not** include parameters in the HTTP body, which can occur with HTTP `POST` requests. The valid range is from 0 to 12,288.	`2048`

Variable	Description	Default
`number-of-ranges-in-range-header <limit_int>`	Type the maximum acceptable number of `Range:` fields of an HTTP header. **Tip:** 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 `Range:` headers. The default value is appropriate for unpatched versions of Apache 2.0 and 2.1. The valid range is from 0 to 64.	`5`
`parameter-name-check {enable | disable}`	Enable to check for null characters in parameter names.	`disable`
`parameter-value-check {enable | disable}`	Enable to check for null characters in parameter values.	`disable`
`Post-request-ctype-check {enable | disable}`	Enable to check whether the `Content-Type:` header is available.	`disable`
`web-socket-protocol-check {enable | disable}`	Enable to detect traffic that uses the WebSocket TCP-based protocol. Because FortiWeb acts as a pure socket proxy for WebSocket traffic, it cannot apply security features to it.	`disable`
`<parameter_name>-check {enable | alert_deny | block-period}`	Specifies whether FortiWeb includes the specified constraint when it applies this set of constraints.	

Variable	Description	Default
<parameter_name>-action {alert | alert_deny | block-period}	Select one of the following actions that the FortiWeb appliance will perform when an HTTP request violates one of the rules: • 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 FortiWeb returns to the client with the HTTP status code. See the *FortiWeb Administration Guide* or config system replacemsg. • block-period — Block subsequent requests from the client for a number of seconds. Also configure <parameter_name>-block-period <seconds_int>. **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 config waf x-forwarded-for). Failure to do so may cause FortiWeb to block **all** connections when it detects a violation of this type. **Caution:** This setting is ignored when the value of monitor-mode {enable | disable} is enabled. **Note:** Logging and/or alert email will occur only if enabled and configured. See config log disk and config log alertemail. **Note:** If you select an auto-learning profile with this rule, you should select alert. If the action is alert_deny, for example, the FortiWeb appliance will block the request or reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see config waf web-protection-profile autolearning-profile. **Note:** This is not a single setting. Configure the action setting for each violation type. The number of action settings equals the number of violation types. For example, for maximum HTTP header length violations, you might type the accompanying setting: `set max-http-header-length-action alert` **Note:** Available actions vary depending on operating mode and protocol parameter.	alert

Variable	Description	Default
`<parameter_name>-severity {High | Medium | Low}`	Select the severity level to use in logs and reports generated when a violation of the rule occurs. **Note:** This is not a single setting. Configure the severity setting for each violation type. The number of severity settings equals the number of violation types. For example, for maximum HTTP header length violations, you might type the accompanying setting: `set max-http-header-length-severity High`	`High`

`<parameter_name>-trigger <trigger-policy_name>`	Type the name of the trigger to apply when this rule is violated (see `config log trigger-policy`). The maximum length is 35 characters.
	To display the list of existing trigger policies, type:
	`set trigger ?`
	Note: This is not a single setting. Configure the trigger setting for each violation type. The number of trigger settings equals the number of violation types. For example, for maximum HTTP header length violations, you might type accompanying setting:
	`set max-http-header-length-trigger trigger-policy1`
		No default.

`<parameter_name>-block-period <seconds_int>`	If `action` is `block-period`, type the number of seconds that the connection will be blocked. The valid range is from 1 to 3,600 seconds.	`0`
`exception_name <http-exception_name>`	Type the name of an exceptions to existing HTTP protocol parameter constraints (see `config server-policy custom-application application-policy`).	No default.

Example

This example limits the total size of the HTTP header, including all lines, to 2,048 bytes. If the HTTP header length exceeds 2,048 bytes, the FortiWeb appliance takes an action to create a log message (`alert`), identifying the violation as `medium` severity, and sends an email to the administrators defined within the trigger policy `email-admin`.

```
config waf http-protocol-parameter-restriction
   edit "http-constraint1"
      set max-http-header-length 2048
      set max-http-header-length-action alert
      set max-http-header-length-severity Medium
      set max-http-header-length-trigger email-admin
   next
end
```

Related topics

- config waf web-protection-profile inline-protection
- config waf web-protection-profile offline-protection
- config log trigger-policy
- config server-policy custom-application application-policy
- diagnose debug application http
- diagnose debug flow trace

waf http-request-flood-prevention-rule

Use this command to limit the maximum number of HTTP requests per second coming from any client to a specific URL on one of your protected servers.

The FortiWeb appliance tracks the requests using a session cookie. If the count exceeds the request limit, FortiWeb performs the specified action.

To apply this rule, include it in an application-layer DoS-prevention policy. This feature is effective only when `http-session-management` is enabled in the inline protection profile that uses the parent DoS-prevention policy.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf http-request-flood-prevention-rule
   edit <rule_name>
      set access-limit-in-http-session <limit_int>
      set action {alert | alert_deny | block-period}
      set real-browser-enforcement {enable | disable}
      set block-period <seconds_int>
      set severity {High | Medium | Low}
      set trigger-policy <trigger-policy_name>
   next
end
```

Variable	Description	Default
`<rule_name>`	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: `edit ?`	No default.
`access-limit-in-http-session <limit_int>`	Type the maximum number of HTTP connections allowed per second from the same client. The valid range is from 0 to 4,096.	0

Variable	Description	Default
`action {alert | alert_deny | block-period}`	Select one of the following actions that the FortiWeb appliance will perform when the count exceeds the limit: • `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 FortiWeb returns to the client with the HTTP status code. See the *FortiWeb Administration Guide* or `config system replacemsg`. • `block-period` — Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int>. **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 `config waf x-forwarded-for`). Failure to do so may cause FortiWeb to block **all** connections when it detects a violation of this type. **Caution:** This setting will be ignored if monitor-mode {enable | disable} is enabled. **Note:** Logging and/or alert email will occur only if enabled and configured. See `config log disk` and `config log alertemail`. **Note:** If you select an auto-learning profile with this rule, you should select `alert`. If the `action` is `alert_deny`, for example, the FortiWeb appliance will block the request or reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see `config waf web-protection-profile autolearning-profile`.	`alert`
`real-browser-enforcement {enable | disable}`	Enable to return a JavaScript to the client to test whether it is a web browser or automated tool when it exceeds the rate limit. If the client either fails the test or does not return results before the timeout specified by `validation-timeout`, FortiWeb applies the specified action. If the client appears to be a web browser, FortiWeb allows the client to exceed the rate limit. Disable this option to apply the rate limit regardless of whether the client is a web browser (for example, Firefox) or an automated tool (for example, `wget`).	disable

Variable	Description	Default
`block-period <seconds_int>`	If `action` is `block-period`, type the number of seconds that the connection will be blocked. This setting applies only if `action` is `block-period`. The valid is from 0 to 10,000 seconds.	0
`severity {High | Medium | Low}`	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	Medium
`trigger-policy <trigger-policy_name>`	Type the name of the trigger to apply when this rule is violated (see `config log trigger-policy`). The maximum length is 35 characters. To display the list of existing trigger policies, type: `set trigger ?`	No default.
`validation-timeout <timeout_int>`	Specifies the maximum amount of time that FortiWeb waits for results from the client for Real Browser Enforcement.	

Example

This example illustrates a rule that imposes a two-minute blocking period on clients that exceed the set request limit.

```
config waf http-request-flood-prevention-rule
   edit "Web Portal HTTP Request Limit"
      set access-limit-in-http-session 10
      set action block-period
      set block-period 120
      set severity Medium
      set trigger-policy "Server_Policy_Trigger"
   next
end
```

Related topics

- `config log trigger-policy`
- `config waf application-layer-dos-prevention`

waf input-rule

Use this command to configure input rules.

Input rules define whether or not parameters are required, and sets their maximum allowed length, for HTTP requests matching the host and URL defined in the input rule.

Each input rule contains one or more individual rules. This enables you to define, within one input rule, all parameter restrictions that apply to HTTP requests matching that URL and host name.

For example, one web page might have multiple inputs: a user name, password, and a preference for whether or not to remember the login. Within the input rule for that web page, you could define separate rules for each parameter in the HTTP request: one rule for the user name parameter, one rule for the password parameter, and one rule for the preference parameter.

To apply input rules, select them within a parameter validation rule. For details, see `config waf parameter-validation-rule`.

Before you configure an input rule, if you want to apply it only to HTTP requests for a specific real or virtual host, you must first define the web host in a protected hosts group. For details, see `config server-policy allow-hosts`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf input-rule
   edit <input-rule_name>
      set action {alert | alert_deny | redirect | send_403_forbidden | block-
          period}
      set block-period <seconds_int>
      set host <protected-host_name>
      set host-status {enable | disable}
      set request-file <url_str>
      set request-type {plain | regular}
      set analyzer-policy <fortianalyzer-policy_name>
      set analyzer-policy <fortianalyzer-policy_name>
      config rule-list
         edit <entry_index>
            set type-checked (enable | disable}
            set argument-type <custom-data-type | data-type | regular-
                expression}
            set argument-name-type {plain | regular}
            set argument-name <input_name>
            set argument-expression <regex_pattern>
            set custom-data-type <custom-data-type_name>
            set data-type <predefined_name>
            set is-essential {yes | no}
            set max-length <limit_int>
         next
      end
   next
end
```

Variable	Description	Default
`<input-rule_name>`	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: `edit ?`	No default.

Variable	Description	Default
action {alert | alert_deny | redirect | send_403_forbidden | block-period}	Select one of the following actions that the FortiWeb appliance will perform when an HTTP request violates one of the input rules in the entry: • 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 FortiWeb returns to the client with the HTTP status code. See the *FortiWeb Administration Guide* or config system replacemsg. • block-period — Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int>. • 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 <redirect_fqdn> and rdt-reason {enable | disable}. • send_403_forbidden — Reply to the client with an HTTP 403 Access Forbidden error message and generate an alert email and/or log message. **Caution:** This setting will be ignored if monitor-mode {enable | disable} is enabled. **Note:** Logging and/or alert email will occur only if enabled and configured. See config log disk and config log alertemail. **Note:** If you select an auto-learning profile with this rule, you should select alert. If the action is alert_deny, for example, the FortiWeb appliance will block the request or reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see config waf web-protection-profile autolearning-profile.	alert
block-period <seconds_int>	Type the number of seconds to block the source IP. The valid range is from 0 to 3,600 seconds. This setting applies only if action is block-period.	60
host <protected-host_name>	Type the name of a protected host that the Host: field of an HTTP request must be in order to match the rule. The maximum length is 255 characters. This setting applies only if host-status is enable.	No default.

Variable	Description	Default
`host-status {enable | disable}`	Enable to apply this input rule only to HTTP requests for specific web hosts. Also configure host <protected-host_name>. Disable to match the input rule based upon the other criteria, such as the URL, but regardless of the `Host:` field.	`disable`
`request-file <url_str>`	Depending on your selection in request-type {plain | regular}, type either: • the literal URL, such as `/index.php`, that the HTTP request must contain in order to match the input rule. The URL must begin with a slash (/). • a regular expression, such as `^/*.php`, matching all and only the URLs to which the input rule should apply. The pattern is **not** required to begin with a slash (/). However, it must at least match URLs that begin with a slash, such as `/index.cfm`. Do not include the name of the web host, such as `www.example.com`, which is configured separately in host <protected-host_name>. The maximum length is 255 characters. **Note:** Regular expressions beginning with an exclamation point (`!`) are not supported. For information on language and regular expression matching, see the *FortiWeb Administration Guide*.	No default.
`request-type {plain | regular}`	Select whether request-file <url_str> will contain a literal URL (`plain`), or a regular expression designed to match multiple URLs (`regular`).	`plain`
`severity {High | Medium | Low}`	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	`Low`
`trigger <trigger-policy_name>`	Type the name of the trigger to apply when this rule is violated (see `config log trigger-policy`). The maximum length is 35 characters. To display the list of existing trigger policies, type: `set trigger ?`	No default.
`<entry_index>`	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.

Variable	Description	Default
`is-essential {yes | no}`	Select `yes` if the parameter is required for HTTP requests to this combination of `Host:` field and URL. Otherwise, select `no`.	`no`
`max-length <limit_int>`	Type the maximum allowed length of the parameter value. The valid range is from 0 to 1,024 characters. To disable the length limit, type `0`.	`0`
`type-checked {enable | disable}`	Enable to use predefined or configured data types when validating parameters. Also configure `data-type`, `custom-data-type`, or `argument-expression`. Disable to ignore `data-type` and `custom-data-type` settings.	`enable`
`argument-type <custom-data-type | data-type | regular-expression}`	Specify the type of argument.	No default.
`argument-name-type {plain | regular}`	Specify one of the following options: • `plain` — `argument-name` is the name attribute of the parameter's input tag exactly as it appears in the form on the web page. • `regular` — `argument-name` is a regular expression designed to match the name attribute of the parameter's input tag.	
`argument-name <input_name>`	If `argument-name-type` is `plain`, specify the name of the input as it appears in the HTTP content, such as `username`. The maximum length is 35 characters. If `argument-name-type` is `regular`, specify a regular expression designed to match the name attribute of the parameter's input tag.	No default.
`argument-expression <regex_pattern>`	Type a regular expression that matches all valid values, and no invalid values, for this input. The maximum length is 2,071 characters. **Note:** Regular expressions beginning with an exclamation point (`!`) are not supported.	

Variable	Description	Default
custom-data-type <custom-data-type_name>	Type the name of a custom data type, if any. The maximum length is 35 characters. To display the list of custom data types, type: `set custom-data-type ?` This setting applies only if `type-checked` is `enable`.	No default.
data-type <predefined_name>	Select one of the predefined data types, if the input matches one of them (available options vary by FortiGuard updates). To display available options, type: `set data type ?` For match descriptions of each option, see `config server-policy pattern data-type-group`). Alternatively, configure argument-type <custom-data-type | data-type | regular-expression}. This option is ignored if you configure argument-type <custom-data-type | data-type | regular-expression}, which also defines parameters to which the input rule applies, but supersedes this option.	No default.

Example

This example blocks and logs requests for the file named login.php that do not include a user name and password, both of which are required, or whose user name and password exceed the 64-character limit.

```
config waf input-rule
   edit "input_rule1"
      set action alert_deny
      set request-file "/login.php?*"
      request-type regular
      config rule-list
         edit 1
            set argument-name "username"
            set argument-type data-type
            set data-type Email
            set is-essential yes
            set max-length 64
         next
         edit 2
            set argument-name "password"
            set data-type String
            set is-essential yes
            set max-length 64
         next
      end
   next
end
```

Related topics

- config server-policy allow-hosts
- config waf parameter-validation-rule

waf ip-intelligence

Use this command to configure reputation-based source IP blacklisting.

Clients with suspicious behaviors or poor reputations include spammers, phishers, botnets, and anonymizing proxy users. If you have purchased a subscription for the FortiGuard IP Reputation service, your FortiWeb can periodically download an updated blacklist to keep your appliance current with changes in dynamic IPs, spreading virus infections, and spammers changing service providers.

IP intelligence settings apply globally, to all policies that use this feature.

Before or after using this command, use config waf ip-intelligence-exception to configure any exemptions that you want to apply. To apply IP reputation-based blocking, configuring these category settings first, then enable ip-intelligence {enable | disable} in the server policy's protection profile.

Alternatively, you can block sets of many clients based upon their geographical origin (see config waf geo-block-list) or manually by specific IPs (see config server-policy custom-application application-policy).

To use this command, your administrator account's access control profile must have either w or rw permission to the wafgrp area. For more information, see Permissions on page 74.

Syntax

```
config waf ip-intelligence
   edit <entry_index>
      set action {alert | alert_deny | redirect | send_403_forbidden | block-
          period}
      set block-period <seconds_int>
      set category <category_name>
      set severity {Low | Medium | High}
      set status {enable | disable}
      set trigger <trigger-policy_name>
   next
end
```

Variable	Description	Default
<entry_index>	Type the index number of the individual entry in the table entry in the table.	No default.

Variable	Description	Default
action {alert | alert_deny | redirect | send_403_forbidden | block-period}	Select one of the following actions that the FortiWeb appliance performs when a client's source IP matches the blacklist category: • 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 FortiWeb returns to the client with the HTTP status code. See the *FortiWeb Administration Guide* or config system replacemsg. • block-period — Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int>. • 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 <redirect_fqdn> and rdt-reason {enable | disable}. • send_403_forbidden — Reply to the client with an HTTP 403 Access Forbidden error message and generate an alert email and/or log message. **Caution:** FortiWeb ignores this setting when monitor-mode {enable | disable} is enabled. **Note:** Logging and/or alert email will occur only if enabled and configured. See config log disk and config log alertemail. **Note:** If you select an auto-learning profile with this rule, you should select alert. If the action is alert_deny, for example, the FortiWeb appliance will block the request or reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see config waf web-protection-profile autolearning-profile.	alert
block-period <seconds_int>	Type the number of seconds to block the source IP. The valid range is from 0 to 3,600 seconds. This setting applies only if action is block-period.	60

Variable	Description	Default
`category <category_name>`	Type the name of an existing IP intelligence category, such as `"Anonymous Proxy"` or `Botnet`. If the category name contains a space, you must surround the name in double quotes. The maximum length is 35 characters. Category names vary by the version number of your FortiGuard IRIS package.	
`status {enable | disable}`	Enable to block clients whose source IP belongs to this category according to the FortiGuard IRIS service.	`enable`
`severity {Low | Medium | High}`	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 uses when a blacklisted IP address attempts to connect to your web servers: • `Low` • `Medium` • `High`	`Low`
`trigger <trigger-policy_name>`	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 `config log trigger-policy`). The maximum length is 35 characters. To display the list of existing trigger policies, type: `set trigger ?`	No default.

Example

The following command blacklists clients whose source IPs are currently known by Fortinet to be members of a botnet. In the FortiGuard IRIS package for this example, "Botnet" is the first item in the list of categories.

When a botnet member makes a request, FortiWeb blocks the connection and continues to block it without re-evaluating it for the next 6 minutes (360 seconds). FortiWeb logs the event with a high severity level and sends notifications to the Syslog and email servers specified in `notification-servers1`.

```
config waf ip-intelligence
   edit 1
      set status enable
      set action period_block
      set block-period 360
      set severity High
      set trigger-policy notification-servers1
   next
end
```

Related topics

- config waf ip-intelligence-exception
- config log trigger-policy
- config waf web-protection-profile inline-protection
- config waf web-protection-profile offline-protection
- config waf geo-block-list
- config server-policy custom-application application-policy
- diagnose debug flow trace

waf ip-intelligence-exception

Use this command to exempt IP addresses from reputation-based blocking. The settings apply globally, to all policies that use this feature.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf ip-intelligence-exception
   edit <entry_index>
      set status {enable | disable}
      set ip <client_ipv4>
   next
end
```

Variable	Description	Default
<entry_index>	Type the index number of the individual entry in the table entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
status {enable | disable}	Enable to exempt clients from IP reputation-based blocking.	disable
ip <client_ipv4>	Type the client's source IP address.	No default.

Example

See config waf ip-intelligence.

Related topics

- config waf ip-intelligence

waf ip-list

Use this command to 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. To determine skipped scans, see `diagnose debug flow trace`.
- **Neither** — If a source IP address **is neither** explicitly blacklisted or trusted by an IP list policy, the client can access your web servers, **unless** it is blocked by any of your other configured, subsequent web protection scan techniques (see `diagnose debug flow trace`).
- **Blacklisted IPs** — Blocked and prevented from accessing your protected web servers. Requests from blacklisted IP addresses receive a warning message in response. The warning message page includes **ID: 70007**, which is the ID of all attack log messages about requests from blacklisted IPs.

Because FortiWeb evaluates trusted and blacklisted IP policies before many other techniques, defining these IP addresses can improve performance.

Alternatively, you can block sets of many clients based upon their reputation (see `config waf ip-intelligence`) or geographical origin (see `config waf geo-block-list`).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf ip-list
   edit <ip-list_name>
      config members
         edit <entry_index>
            set ip <client_ip>
            set type {trust-ip | black-ip}
            set severity {Low | Medium | High}
            set trigger-policy <trigger-policy_name>
         next
      end
   next
end
```

Variable	Description	Default
`<ip-list_name>`	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: `edit ?`	No default.

Variable	Description	Default
`<entry_index>`	Type the index number of the individual entry in the table entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
`ip <client_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 (for example, `172.22.14.1-172.22.14.255` or `10:200::10:1-10:200:10:100`).	No default.
`type {trust-ip | black-ip}`	Select either: • `trust-ip` — The source IP address is trusted and allowed to access your web servers, **unless** it fails a previous scan (see `diagnose debug flow trace`). • `black-ip` — The source IP address that is **dis**trusted, and is permanently blocked (blacklisted) from accessing your web servers, even if it would normally pass all other scans. **Note:** 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.	`trust-ip`
`severity {Low | Medium | High}`	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 a blacklisted IP address attempts to connect to your web servers: • `Low` • `Medium` • `High`	No default.
`trigger-policy <trigger-policy_name>`	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 `config log trigger-policy`). The maximum length is 35 characters. To display the list of existing trigger policies, type: `set trigger ?`	No default.

Example

The following shows the configuration for a trusted host of 192.0.2.0 followed by a blacklisted client of 192.0.2.1.

```
config waf ip-list
   edit "IP-List-Policy1"
      config members
         edit 1
            set ip 192.0.2.0
            next
         edit 2
            set type black-ip
            set ip 192.0.2.1
            set severity Medium
            set trigger-policy "TriggerActionPolicy1"
         next
      end
   next
end
```

Related topics

- config log trigger-policy
- config waf web-protection-profile inline-protection
- config waf web-protection-profile offline-protection
- config waf geo-block-list
- config waf ip-intelligence
- diagnose debug flow trace

waf layer4-access-limit-rule

Use this command to limit the number of HTTP requests per second from any IP address to your web server. The FortiWeb appliance tracks the number of requests. If the count of HTTP `GET` or `POST` requests exceeds the request limit, FortiWeb performs the action you specified.

To apply this rule, include it in an application-layer DoS-prevention policy (see `config waf application-layer-dos-prevention`) and include that policy in an inline protection profile.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf layer4-access-limit-rule
   edit <rule_name>
      set access-limit-standalone-ip <limit_int>
      set access-limit-share-ip <limit_int>
      set action {alert | alert_deny | block-period}
      set real-browser-enforcement {enable | disable}
      set block-period <seconds_int>
      set severity {High | Medium | Low}
```

```
        set trigger-policy <trigger-policy_name>
        set validation-timeout <timeout_int>

    next
end
```

Variable	Description	Default
<rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: edit ?	No default.
access-limit-standalone-ip <limit_int>	Type the maximum number of HTTP requests allowed per second from any source IP address representing a single client. The valid range is from 0 to 65,536.	0
access-limit-share-ip <limit_int>	Type the maximum number of HTTP requests allowed per second from any source IP address shared by multiple clients behind a network address translation (NAT) device, such as a firewall or router. The valid range is from 0 to 65,536.	0

Variable	Description	Default
action {alert | alert_deny | block-period}	Select one of the following actions that the FortiWeb appliance will perform when the count exceeds either threshold limit: • 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 FortiWeb returns to the client with the HTTP status code. See the *FortiWeb Administration Guide* or config system replacemsg. • block-period — Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int>. **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 config waf x-forwarded-for). Failure to do so may cause FortiWeb to block **all** connections when it detects a violation of this type. **Caution:** This setting will be ignored if monitor-mode {enable | disable} is enabled. **Note:** Logging and/or alert email will occur only if enabled and configured. See config log disk and config log alertemail. **Note:** If you select an auto-learning profile with this rule, you should select alert. If the action is alert_deny, for example, the FortiWeb appliance will block the request or reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see config waf web-protection-profile autolearning-profile.	alert

Variable	Description	Default
`real-browser-enforcement {enable | disable}`	Enable to return a JavaScript to the client to test whether it is a web browser or automated tool when it exceeds the rate limit. If the client either fails the test or does not return results before the timeout specified by `validation-timeout`, FortiWeb applies the specified action. If the client appears to be a web browser, FortiWeb allows the client to exceed the rate limit. Disable this option to apply the rate limit regardless of whether the client is a web browser (for example, Firefox) or an automated tool (for example, `wget`).	disable
`block-period <seconds_int>`	Type the number of seconds to block access to the client. This applies only when the `action` setting is `block-period`. The valid range is from 0 to 10,000.	0
`severity {High | Medium | Low}`	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	`Medium`
`trigger-policy <trigger-policy_name>`	Type the name of the trigger to apply when this rule is violated (see `config log trigger-policy`). The maximum length is 35 characters. To display the list of existing trigger policies, type: `set trigger ?`	No default.
`validation-timeout <timeout_int>`	Specifies the maximum amount of time that FortiWeb waits for results from the client for Real Browser Enforcement.	

Example

This examples includes two rules. One blocks connections for two minutes while the other creates an alert and denies the connection.

```
config waf layer4-access-limit-rule
   edit "Web Portal HTTP Request Limit"
      set access-limit-share-ip 10
      set access-limit-standalone-ip 10
      set action block-period
      set block-period 120
      set severity Medium
      set trigger-policy "Web_Protection_Trigger"
   next
   edit "Online Store HTTP Request Limit"
      set access-limit-share-ip 5
      set access-limit-standalone-ip 5
      set action alert_deny
      set severity High
      set trigger-policy "Web_Protection_Trigger"
```

```
    next
end
```

Related topics

- config log trigger-policy
- config waf application-layer-dos-prevention
- config waf layer4-connection-flood-check-rule

waf layer4-connection-flood-check-rule

Use this command to 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 forms 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 opens 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 `config waf http-connection-flood-check-rule`. However, this feature counts TCP connections per IP, while the other command counts TCP connections per session cookie.

It is also similar to `syncookie` in `config server-policy policy`. However, this feature counts fully-formed TCP connections, while the anti-SYN flood feature counts partially-formed TCP connections.

To apply this rule, include it in an application-layer DoS-prevention policy (see `config waf application-layer-dos-prevention`) and include that policy in an inline protection profile.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf layer4-connection-flood-check-rule
   edit <rule_name>
      set layer4-connection-threshold <limit_int>
      set action {alert | alert_deny | block-period}
      set block-period <seconds_int>
      set severity {High | Medium | Low}
      set trigger-policy <trigger-policy_name>
   next
end
```

Variable	Description	Default
`<rule_name>`	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: `edit ?`	No default.
`layer4-connection-threshold <limit_int>`	Type enter the maximum number of TCP connections allowed from the same IP address. The valid range is from 0 to 65,536.	0
`action {alert | alert_deny | block-period}`	Select one of the following actions that the FortiWeb appliance will perform when the count exceeds the rate limit: • `alert` — Accept the connection and generate an alert email and/or log message. • `alert_deny` — Block the connection and generate an alert email and/or log message. • `block-period` — Block subsequent requests from the client for a number of seconds. Also configure `block-period <seconds_int>`. **Caution:** This setting will be ignored if monitor-mode {enable | disable} is enabled. **Note:** Logging and/or alert email will occur only if enabled and configured. See `config log disk` and `config log alertemail`. **Note:** If an auto-learning profile will be selected in the policy with offline protection profiles that use this rule, you should select `alert`. If the `action` is `alert_deny`, the FortiWeb appliance will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see `config waf web-protection-profile autolearning-profile`.	`alert`
`block-period <seconds_int>`	Type the length of time for which the FortiWeb appliance will block additional requests after a source IP address exceeds the rate threshold. The block period is shared by all clients whose traffic originates from the source IP address. The valid range is from 1 to 3,600 seconds (1 hour).	`1`
`severity {High | Medium | Low}`	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	Medium

Variable	Description	Default
`trigger-policy <trigger-policy_name>`	Type the name of the trigger to apply when this rule is violated (see `config log trigger-policy`). The maximum length is 35 characters. To display the list of existing trigger policies, type: `set trigger ?`	No default.

Example

This example illustrates a basic TCP flood check rule.

```
config waf layer4-connection-flood-check-rule
   edit "Web Portal Network Connect Limit"
      set action alert_deny
      set layer4-connection-threshold 10
      set severity Medium
      set trigger-policy "Server_Policy_Trigger"
   next
end
```

Related topics

- `config log trigger-policy`
- `config waf application-layer-dos-prevention`
- `config waf layer4-access-limit-rule`

waf padding-oracle

Use this command to create a policy that protects vulnerable block cipher implementations for web applications that selectively encrypt inputs without using HTTPS.

To apply this policy, include it in an inline web or offline protection profile. For details, see `config waf web-protection-profile inline-protection` or `config waf web-protection-profile offline-protection`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf padding-oracle
   edit <padding-oracle_rule_name>
      set action {alert | alert_deny | block-period}
      set block-period <block-period_int>
      set severity {High | Medium | Low}
      set trigger <trigger-policy_name>
      config protected-url-list
         edit <entry_index>
```

```
            set host-status {enable | disable}
            set host <host_str>
            set url-type {plain | regular}
            set protected-url <protected-url_str>
            set target {cookie parameter url}
        end
    next
end
```

Variable	Description	Default
<padding-oracle_rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing policies, type: edit ?	No default.

Variable	Description	Default
	Specify the action that FortiWeb takes when a request violates the rule: • `alert` — Accept the request 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. • `block-period` — Block subsequent requests from the client for a number of seconds. Also configure `block-period`. **Note:** If FortiWeb is deployed behind a NAT load balancer, when using this option, define an X-header that indicates the original client's IP (see `config waf x-forwarded-for`). Failure to do so may cause FortiWeb to block all connections when it detects a violation of this type.	
`{alert | alert_deny | block-period}`	Attack log messages contain `Padding Oracle Attack` 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. **Caution:** This setting is ignored if the value of `monitor-mode` is `enabled`. See `config server-policy policy`. **Note:** Logging and/or alert email occur only when the these features are enabled and configured. See `config log attack-log` and `config log alertemail`. **Note:** To use this rule set with auto-learning, 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 session information for auto-learning will be incomplete.	`alert`
`<block-period_int>`	Type the number of seconds that FortiWeb blocks subsequent requests from the client after it detects that the client has violated the rule. This setting is available only if `action` is `block-period`. The valid range is from 1 to 4,294,967,295.	1

Variable	Description	Default
{High | Medium | Low}	When rule violations are recorded in the attack log, each log message contains a Severity Level (severity_level) field. Specify the severity level FortiWeb uses when it logs a violation of this rule.	Medium
<trigger-policy_name>	Type the name of the trigger policy, if any, that the FortiWeb appliance uses when it logs and/or sends an alert email about a violation of the rule. See config log trigger-policy. To display the list of existing triggers, type: set trigger ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
host-status {enable | disable}	Specify enable to apply this rule only to HTTP requests for specific web hosts. Also specify host. Specify disable to match the rule based on the other criteria, such as the URL, but regardless of the Host: field.	disable
<host_str>	Specify 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 rule. This option is available only if the value of host-status is enabled. Maximum length is 255 characters.	No default.
{plain | regular}	Specify how the value of protected-url is specified: • plain — A literal URL. • regular — A regular expression designed to match multiple URLs.	plain

Variable	Description	Default

<protected-url_str>	If the value of `url-type` is `plain`, specify the literal URL that HTTP requests that match the rule contain.
	For example:
	`/profile.jsp`
	The URL must begin with a backslash (/).
	If the value of `url-type` is `regular`, specify a regular expression matching all and only the URLs to which the rule should apply.
	For example:
	`^/*\.jsp\?uid\=(.*)`
	The pattern does not require a slash (/).; however, it must at least match URLs that begin with a slash, such as `/profile.cfm`.
	Do not include the domain name, such as `www.example.com`, which is specified by `host`.
	Regular expressions beginning with an exclamation point (`!`) are not supported. For information on language and regular expression matching, see the *FortiWeb Administration Guide*.
		No default.

{cookie parameter url}	Specify which parts of the client's requests FortiWeb examines for padding attack attempts: • `url` — A URL (for example, the parameter `/user/0000012FE03BC2` is embedded in the URL). • `parameter` — A parameter (for example, the parameter **/index.php?user=0000012FE03BC2** appended to a traditional GET or POST body). • `cookie` — A cookie.	`parameter`

Example

This example illustrates a padding oracle rule that blocks requests to the host `www.example.com` when a parameter appended in a traditional GET URL parameter or POST body matches the specified regular expression. When a request matches the expression, FortiWeb logs or sends a high-severity message as specified in the `notification-servers1` trigger policy.

```
config waf padding-oracle
  edit padding-oracle1
    set action block-period
    set block-period 3600
    set severity High
    set trigger notification-servers1
    config protected-url-list
```

```
edit 1
   set host-status enable
   set host www.example.com
   set url-type regular
   set protected-url \/profile\.jsp\?uid\=(.*)
   set target parameter
   end
```

Related topics

- config waf web-protection-profile inline-protection
- config waf web-protection-profile offline-protection

waf page-access-rule

Use this command to configure page access rules.

Page access rules define URLs that can be accessed only in a **specific order**, such as to enforce the business logic of a web application. Requests for other, non-ordered URLs may interleave ordered URLs during the client's session. Page access rules may be specific to a web host.

For example, an e-commerce application might be designed to work properly in this order:

1. A client begins a session by adding an item to a shopping cart. (`/addToCart.do?*`)
2. The client either views and adds additional items to the shopping cart, or proceeds directly to the checkout.
3. The client confirms the items that he or she wants to purchase. (`/checkout.do`)
4. The client provides shipping information. (`/shipment.do`)
5. The client pays for the items and shipment, completing the transaction. (`/payment.do`)

Sessions that begin at the shipping or payment stage should therefore be invalid. If the web application does not enforce this rule itself, it could be open to cross-site request forgery (CSRF) attacks on the payment feature. To prevent such abuse, the FortiWeb appliance could enforce the rule itself using a page access rule set with the following order:

1. `/addToCart.do?item=*`
2. `/checkout.do?login=*`
3. `/shipment.do`
4. `/payment.do`

Attempts to request `/payment.do` before those other URLs during a session would be denied, and generate an alert and attack log message (see config log disk).

To apply page access rules, select them within an inline protection profile. For details, see config waf web-protection-profile inline-protection.

Before you configure a page access rule, if you want to apply it only to HTTP requests for a specific real or virtual host, you must first define the web host in a protected hosts group. For details, see config server-policy allow-hosts.

You can use SNMP traps to notify you when a page access rule is enforced. For details, see `config system snmp community`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

In order for page access rules to be enforced, you must also enable http-session-management {enable | disable} in the inline protection profile.

Syntax

```
config waf page-access-rule
   edit <page-access-rule_name>
      config page-access-list
         edit <entry_index>
            set host <protected-hosts_name>
            set host-status {enable | disable}
            set request-file <url_str>
            set request-type {plain | regular}
         next
      end
   next
end
```

Variable	Description	Default
<page-access-rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: `edit ?`	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999. Page access rules should be added to the set in the order which clients will be permitted to access them. For example, if a client must access `/login.asp` before `/account.asp`, add the rule for `/login.asp` first.	No default.
host <protected-hosts_name>	Type the name of a protected host that the `Host:` field of an HTTP request must be in order to match the page access rule. The maximum length is 255 characters. This setting applies only if `host-status` is `enable`.	No default.

Variable	Description	Default
`host-status {enable | disable}`	Enable to apply this page access rule only to HTTP requests for specific web hosts. Also configure host <protected-hosts_name>. Disable to match the page access rule based upon the other criteria, such as the URL, but regardless of the `Host:` field.	`disable`
`request-file <url_str>`	Depending on your selection in request-type {plain | regular}, type either: • the literal URL, such as `/cart.php`, that the HTTP request must contain in order to match the page access rule. The URL must begin with a slash (/). • a regular expression, such as `^/*.php`, matching all and only the URLs to which the page access rule should apply. The pattern is **not** required to begin with a slash (/). However, it must at least match URLs that begin with a slash, such as `/cart.cfm`. Do not include the name of the web host, such as `www.example.com`, which is configured separately in host <protected-hosts_name>. The maximum length is 255 characters. **Note:** Regular expressions beginning with an exclamation point (`!`) are not supported. For information on language and regular expression matching, see the *FortiWeb Administration Guide*.	No default.
`request-type {plain | regular}`	Select whether request-file <url_str> will contain a literal URL (`plain`), or a regular expression designed to match multiple URLs (`regular`).	`plain`

Example

This example allows any request to www.example.com, as long as it follows the expected sequence within a session for the four key shopping cart URLs (`/addToCart.do`, `/checkout.do`, `/shipment.do`, then `/payment.do`).

```
config waf page-access-rule
   edit "page-access-rule1"
      config page-access-list
         edit 1
            set host "www.example.com"
            set host-status enable
            set request-file "/addToCart.do?item=*"
            set request-type regular
         next
         edit 2
            set host "www.example.com"
```

```
            set host-status enable
            set request-file "/checkout.do?login=*"
            set request-type regular
         next
         edit 3
            set host "www.example.com"
            set host-status enable
            set request-file "/shipment.do"
            set request-type plain
         next
         edit 4
            set host "www.example.com"
            set host-status enable
            set request-file "/payment.do"
            set request-type plain
         next
      end
   next
end
```

Related topics

- config server-policy allow-hosts
- config system snmp community
- config waf web-protection-profile inline-protection

waf parameter-validation-rule

Use this command to configure parameter validation rules, each of which is a group of input rule entries.

To apply parameter validation rules, select them within an inline or offline protection profile. For details, see config waf web-protection-profile inline-protection or config waf web-protection-profile offline-protection.

Before you can configure parameter validation rules, you must first configure one or more input rules. For details, see config waf input-rule.

You can use SNMP traps to notify you when a parameter validation rule is enforced. For details, see config system snmp community.

To use this command, your administrator account's access control profile must have either w or rw permission to the wafgrp area. For more information, see Permissions on page 74.

Syntax

```
config waf parameter-validation-rule
   edit <rule_name>
      config input-rule-list
         edit <entry_index>
            set input-rule <input-rule_name>
         next
      end
   next
```

```
    end
```

Variable	Description	Default
<rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: `edit ?`	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
input-rule <input-rule_name>	Type the name of an input rule to use in the parameter validation rule. The maximum length is 35 characters. To display the list of existing input rules, type: `set input-rule ?`	No default.

Example

This example configures a parameter validation rule that applies two input rules.

```
config waf parameter-validation-rule
   edit "parameter_validator1"
      config input-rule-list
         edit 1
            set input-rule "input_rule1"
      next
         edit 2
            set input-rule "input_rule2"
         next
      end
   next
end
```

Related topics

- config waf input-rule
- config waf web-protection-profile inline-protection
- config waf web-protection-profile offline-protection

waf signature

Use this command to configure server protection rules.

There are several security features specifically designed to protect web servers from known attacks. You can configure defenses against:

- cross-site scripting (XSS)
- SQL injection and many other code injection styles
- generic attacks
- known exploits
- trojans/viruses
- information disclosure
- bad robots
- credit card data leaks
- FortiWeb scans:
- HTTP headers
- 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 xml-protocol-detection {enable | disable} is enabled)
- cookies

In addition to scanning standard requests, signatures can also scan action message format 3.0 (AMF3) binary inputs used by Adobe Flash clients to communicate with server-side software and XML. For more information, see amf3-protocol-detection {enable | disable} and malformed-xml-check {enable | disable} (for inline protection profiles) or amf3-protocol-detection {enable | disable} (for offline protection profiles).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Updating signatures

Known attack signatures can be updated. For information on uploading a new set of attack definitions, see the *FortiWeb Administration Guide*. You can also create your own. See `config waf custom-protection-rule`.

Configuring signatures

Before configuring a server protection rule, if you want to configure your own attack or data leak signatures, you must also configure custom server protection rules. For details, see `config waf custom-protection-group`.

Each server protection rule can be configured with the severity and notification settings ("trigger") that, in combination with the action, determines how FortiWeb handles each violation.

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.

Alternatively, you can automatically configure a server protection rule that detects all attack types by generating a default auto-learning profile. For details, see the *FortiWeb Administration Guide*.

Threat scoring

The threat scoring feature allows you to configure your signature policy to take action based on multiple signature violations by a client, instead of a single signature violation. When a client violates a signature in a threat scoring category, it contributes to a combined threat score. When the combined threat score exceeds a maximum value you specify, FortiWeb takes action.

For an overview of the threat scoring mechanism, see the *FortiWeb Administration Guide*.

Overriding signature category configuration

To override category-wide actions for a specific signature, configure:

- config signature_disable_list — Disable a specific signature ID (e.g. 040000007), even if the category in general (e.g. **SQL Injection (Extended)**) is enabled.
- config sub_class_disable_list — Disable a subcategory of signatures (e.g. **Session Fixation**), even if the category in general (e.g. **General Attacks**) is enabled.
- config alert_only_list — Only log/alert when detecting the attack, even if the category in general is configured to block.
- config filter_list — Exempt specific host name and/or URL combinations from scanning with this signature.

Applying signature policies

To apply server protection rules, select them within an inline or offline protection profile. For details, see `config waf web-protection-profile inline-protection` or `config waf web-protection-profile offline-protection`.

You can use SNMP traps to notify you when an attack or data leak has been detected. For details, see `config system snmp community`.

Syntax

```
config waf signature
   edit <signature-set_name>
      set threat-scoring_mode {enable | disable}
      set scoring-threshold {Information-Security | Low-Security | Medium-
          Security | High-Security | Critical-Security}
      set scoring-scope {HTTP-Transaction | TCP-Session | HTTP-Session}
      set scoring-action {alert | alert_deny | redirect | block-period | send_
          http_response}
      set scoring-block-period <seconds_int>
      set scoring-severity {High | Medium | Low}
      set scoring-trigger
      set credit-card-detection-threshold <instances_int>
      [set custom-protection-group <group_name>]
      config main_class_list
         edit {010000000 | 020000000 | 030000000 | 040000000 | 050000000 |
             060000000 | 070000000 | 080000000 | 090000000 | 100000000}
            set fpm-status {enable | disable}
            set scoring-status {enable | disable}
            set action {alert |alert_deny | block-period |only_erase | send_http_
                response | alert_erase | redirect}
            set block-period <seconds_int>
            set severity {Low | Medium | High}
            set trigger <trigger-policy_name>
```

```
        next
      end
      config signature_disable_list
        edit <signature-id_str>
        next
      end
      config sub_class_disable_list
        edit {010000000 | 020000000 | 030000000 | 040000000 | 050000000 |
            060000000 | 070000000 | 080000000 | 090000000 | 100000000}
        next
      end
      config alert_only_list
        edit <alert-only-list_signature-id_str>
        next
      end
      config fpm_disable_list
        edit <fpm-disable-list_signature-id_str>
        next
      end
      config scoring_override_disable_list
        edit <scoring-override-disable-list_signature-id_str>
        next
      end
      config score_grade_list
        edit <score-grade-list_signature-id_str>
          set scoring-grade {Information | Low | Medium | High | Critical}
        next
      end
      config filter_list
        edit <entry_index>
          set signature_id <signature-id_str>
          set match-target {HTTP_METHOD | CLIENT_IP | HOST | URI| FULL_URL |
              PARAMETER| COOKIE}
          set operator {STRING_MATCH | REGEXP_MATCH | EQ | NE| INCLUDE |
              EXCLUDE}
          set http-method {get post head options trace connect delete put
              others}
          set ip {<ipv4> | <ipv6>}
          set name {name_str | name_pattern]
          set value-check {enable | disable}
          set value {value_str | value_pattern
          set concatenate-type {AND | OR}
        next
      set comment "<comment_str>"
      end
  next
end
```

Variable	Description	Default
`<signature-set_name>`	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: `edit ?`	No default.
`threat-scoring_mode {enable | disable}`	Specifies whether threat scoring is enabled. The threat scoring feature allows you to configure your signature policy to trigger an action based on attack or leak detection by multiple signatures, instead of a single signature.	`disable`
`scoring-threshold {Information-Security | Low-Security | Medium-Security | High-Security | Critical-Security}`	Specifies the maximum combined threat score to exceed before FortiWeb takes the specified action. • `Information-Security` – 10 • `Low-Security` – 7 • `Medium-Security` – 5 • `High-Security` – 4 • `Critical-Security` – 2 Available only when `threat-scoring_mode` is `enable`.	`Medium-Security`
`scoring-scope {HTTP-Transaction | TCP-Session | HTTP-Session}`	Specifies how FortiWeb calculates the combined threat score before it compares it to the `scoring-threshold` value. • `HTTP-Transaction` – FortiWeb compares the score for each transaction to the `scoring-threshold` value. • `TCP-Session` – FortiWeb compares the score for each session to the `scoring-threshold` value. The score can include multiple transactions. • `HTTP-Session` – FortiWeb compares the score for sessions associated with a specific client to the `scoring-threshold` value. This option requires `http-session-management` in the appropriate protection profile to be `enable` . Available only when `threat-scoring_mode` is `enable`.	`TCP-Session`

Variable	Description	Default
`scoring-action {alert | alert_deny | redirect | block-period | send_ http_response}`	Select which action the FortiWeb appliance takes when the combined threat score exceeds the specified threshold. • `alert` — Accept the request and generate an alert email, a log message, or both. **Note:** Does **not** cloak, except for removing sensitive headers. (Sensitive information in the body remains unaltered.) • `alert_deny` — Block the request (or reset the connection) and generate an alert email, a log message, or both. You can customize the web page that FortiWeb returns to the client with the HTTP status code. See the *FortiWeb Administration Guide* or `config system replacemsg`. • `redirect` — Redirect the request to the URL that you specify in the protection profile and generate an alert email, a log message, or both. Also configure redirect-url <redirect_fqdn> and rdt-reason {enable | disable}. • `block-period` — Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int>. **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 `config waf x-forwarded-for`). Failure to do so may cause FortiWeb to block **all** connections when it detects a violation of this type. • `send_http_response` — Block and reply to the client with an HTTP error message, and generate an alert email, a log message, or both. You can customize the web page that FortiWeb returns to the client with the HTTP status code. See the *FortiWeb Administration Guide* or `config system replacemsg`. **Caution:** FortiWeb ignores this setting if monitor-mode {enable | disable} is enabled. Available only when `threat-scoring_mode` is `enable`.	`alert`

Variable	Description	Default
`scoring-block-period <seconds_int>`	Specifies the number of seconds that FortiWeb blocks subsequent requests from the client after it detects that the client has exceeded the threat score threshold. The valid range is from 1 to 3,600. The setting is applicable only if `scoring-action` is `period-block`.	`60`
`scoring-severity {High | Medium | Low}`	Specifies the severity level value to use when FortiWeb records threat scoring violations in the attack log, each log message contains a **Severity Level** (`severity_level`) field. • `Low` • `Medium` • `High` Available only when `threat-scoring_mode` is `enable`.	`Medium`
`scoring-trigger`	Specifies the trigger, if any, that FortiWeb applies when a threat scoring threshold is exceeded (see `config log trigger-policy`). The maximum length is 35 characters. To display the list of existing triggers, type: `set scoring-trigger ?` Available only when `threat-scoring_mode` is `enable`.	No default.
`credit-card-detection-threshold <instances_int>`	Type the number of credit cards that triggers the credit card number detection feature. For example, to ignore web pages with only one credit card number, but to detect when a web page containing two or more credit cards, enter `2`. The valid range is from 1 to 128 instances.	`1`
`custom-protection-group <group_name>`	Type the name of the custom signature group to be used, if any. The maximum length is 35 characters. To display the list of existing custom signature groups, type: `set custom-protection-group ?`	No default.

Variable	Description	Default
{010000000 | 020000000 | 030000000 | 040000000 | 050000000 | 060000000 | 070000000 | 080000000 | 090000000 | 100000000}	Type the ID of a signature class (or, for subclass overrides, the subclass ID). To display the list of signature classes, type: `edit ?`	No default.
fpm-status {enable | disable}	For signatures that identify SQL injection attacks, specifies whether FortiWeb performs additional SQL syntax validation. When this option is enabled and the validation is successful, FortiWeb takes the specified action. If it fails, FortiWeb takes no action.	enable
scoring-status {enable | disable}	Specifies whether violations of signatures in this category contribute to the combined threat score for the signature policy instead of triggering the specified action. Available only when `threat-scoring_mode` is `enable`.	disable

Variable	Description	Default
`action {alert |alert_ deny | block-period |only_ erase | send_http_ response | alert_ erase | redirect}`	Select which action the FortiWeb appliance will take when it detects a signature match. **Note:** This is not a single setting. Available actions may vary slightly, depending on what is possible for each specific type of attack/information disclosure. • `alert` — Accept the request and generate an alert email and/or log message. **Note:** Does **not** cloak, except for removing sensitive headers. (Sensitive information in the body remains unaltered.) • `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 FortiWeb returns to the client with the HTTP status code. See the *FortiWeb Administration Guide* or `config system replacemsg`. • `block-period` — Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int>. **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 `config waf x-forwarded-for`). Failure to do so may cause FortiWeb to block **all** connections when it detects a violation of this type. • `only_erase` — Hide sensitive information in replies from the web server (sometimes called "cloaking"). Block the request or remove the sensitive information, but do not generate an alert email and/or log message. **Caution:** This option is not supported in offline protection mode. • `send_http_response` — Block and reply to the client with an HTTP error message, and generate an alert email, a log message, or both • `alert_erase` — 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. **Note:** This option is not fully supported in offline protection mode. Effects will be identical to `alert`; sensitive information will not be blocked or erased.	`alert`

Variable	Description	Default
	• `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 <redirect_fqdn> and rdt-reason {enable | disable}. **Caution:** FortiWeb ignores this setting if monitor-mode {enable | disable} is enabled. **Note:** Actions that generate log messages alert email actions require the features to be enabled and configured. See `config log disk` and `config log alertemail`. **Note:** If you select an auto-learning profile in the policy with offline protection profiles that use this rule, select `alert`. If the `action` is `alert_deny`, the FortiWeb appliance resets the connection when it detects an attack and the session information for the auto-learning feature will be incomplete. For more information on auto-learning requirements, see `config waf web-protection-profile autolearning-profile`.	
`block-period <seconds_int>`	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. The valid range is from 1 to 3,600. The setting is applicable only if `action` is `period-block`. **Note:** This is not a single setting. You can configure the block period separately for each signature category.	`60`
`severity {Low | Medium | High}`	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` **Note:** This is not a single setting. You can configure the severity separately for each signature category.	`Medium`

Variable	Description	Default
`trigger <trigger-policy_name>`	Type the name of the trigger, if any, to apply when a protection rule is violated (see `config log trigger-policy`). The maximum length is 35 characters. To display the list of existing triggers, type: `set trigger ?` **Note:** This is not a single setting. You can configure a different trigger for each signature category.	No default.
`<signature-id_str>`	Type the ID of a specific signature that you want to disable. Some signatures often cause false positives and are disabled by default. To display a list, type: `edit ?`	No default.
`<alert-only-list_signature-id_str>`	Type the ID of a specific signature that generates logs or alert email only and does not block matching requests.	No default.
`<fpm-disable-list_signature-id_str>`	Type the ID of a specific signature for which false positive mitigation is disabled. The false positive mitigation feature performs additional lexical and syntax analysis after a SQL injection signature matches a request.	No default.
`<scoring-override-disable-list_signature-id_str>`	Type the ID of a specific signature that is not affected by the threat score settings. When traffic violates this signature, FortiWeb takes the action specified for that signature immediately. Available only when `threat-scoring_mode` is `enable`.	No default.
`<score-grade-list_signature-id_str>`	Type the ID of a specific signature that has a custom threat score. Also specify `scoring-grade`. Available only when `threat-scoring_mode` is `enable`.	No default.

Variable	Description	Default
scoring-grade {Information | Low | Medium | High | Critical}	Specifies the threat score that the signature adds to the combined threat score for the signature policy. • Information – 1 • Low – 2 • Medium – 3 • High – 4 • Critical – 5 Available only when threat-scoring_mode is enable.	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 32.	No default.
signature_id <signature-id_str>	Type the ID of a specific signature that you want to disable when the request matches the specified object.	No default.
match-target {HTTP_METHOD | CLIENT_IP | HOST | URI| FULL_URL | PARAMETER| COOKIE}	Type the type of object that FortiWeb examines for matching values: • HTTP_METHOD — One or more HTTP methods specified by http-method. • CLIENT_IP — The IP address specified by ip. • HOST — The Host: field value specified by value. • URI — The URL value specified by value. The value does not include parameters. • FULL_URL — The URL value specified by value. The value includes parameters to match. • PARAMETER — A parameter specified by name. To match a specific parameter value, enable value-check, and then specify value. • COOKIE — A cookie specified by name. To match a specific cookie value, enable value-check, and then specify value.	

Variable	Description	Default
operator {STRING_MATCH | REGEXP_MATCH | EQ | NE| INCLUDE | EXCLUDE}	Type the type of values to match. The match-target value determines which types are available. • STRING_MATCH — value is a literal value (for example, a literal host name). • REGEXP_MATCH — value is a regular expression that matches the object the exception applies to. • EQ — When match-target is CLIENT_IP, FortiWeb only performs a signature scan for requests with a client IP address that matches the value of ip. • NE — When match-target is CLIENT_IP, FortiWeb does not perform a signature scan for requests with a client IP address that matches the value of ip. • INCLUDE — When match-target is HTTP_METHOD, FortiWeb does not perform a signature scan for requests that include the HTTP methods specified by http-method. • EXCLUDE — When match-target is HTTP_METHOD, FortiWeb only performs a signature scan for requests that include the HTTP methods specified by http-method.	
http-method {get post head options trace connect delete put others}	When match-target is HTTP_METHOD, specifies one or more HTTP methods to match.	No default.
ip {<ipv4> | <ipv6>}	When match-target is CLIENT_IP, specifies the IP address to match.	No default.
name {name_str | name_pattern]	Type the name of a parameter or cookie to match. Whether the value is a literal value or a regular expression is determined by the value of operator. Available when match-target is PARAMETER or COOKIE.	No default.
value-check {enable | disable}	Specifies whether matching requests match a specified parameter or cookie value as well as the specified parameter or cookie name.	disable
value {value_str | value_pattern	Type the value to match (for example, a Host: field value). Whether the value is a literal value or a regular expression is determined by the value of operator.	No default.

Variable	Description	Default
concatenate-type {AND | OR}	• AND — A matching request matches this entry in addition to other entries in the list. • OR —A matching request matches this entry or other entries in the list.	AND
comment "<comment_str>"	Type a description or other comment.	No default.

Example

This example enables both the Trojans (070000000) and XSS (010000000) classes of signatures, setting them to result in attack logs with a severity_level field of High, and using the email and SNMP settings defined in notification-servers1. It also enables use of custom attack and data leak signatures in the set named custom-signature-group1.

This example disables by ID a signature that is known to cause false positives (080200001). It also makes an exception (config filter_list) by ID for a specific signature (070000001) for a URL (/virus-sample-upload) on a host (www.example.com) that is used by security researchers to receive virus samples.

```
config waf signature
   edit "attack-signatures1"
      set custom-protection-group "custom-signature-group1"
      config main_class_list
         edit "010000000"
            set severity High
            set trigger "notification-servers1"
         next
         edit "070000000"
            set severity High
            set trigger "notification-servers1"
         next
      end
      config signature_disable_list
         edit "080200001"
         next
      end
      config filter_list
         edit 1
            set signature_id "070000001"
            set match-target HOST
            set value "www.example.com"
         next
         edit 2
            set signature_id "070000001"
            set match-target URI
            set value "/virus-sample-upload"
         next
      end
   next
end
```

Related topics

- config waf web-protection-profile inline-protection
- config waf web-protection-profile offline-protection
- config system snmp community
- config waf custom-protection-group
- config log trigger-policy

waf site-publish-helper authentication-server-pool

Use this command to create a pool of authentication server connections for use with a site publishing rule.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf site-publish-helper authentication-server-pool
   edit <authentication-server-pool_name>
        edit <entry_index>
           set server-type {ldap | radius}
           set ldap-server <ldap-query_name>
           set radius-server <radius-query_name>
           set rsa-securid {enable | disable}
      end
   next
end
```

Variable	Description	Default
<authentication-server-pool_name>	Type the name of a new or existing authentication server pool. The maximum length is 35 characters. To display the list of existing pools, type: edit ?	No default.
<entry_index>	Type the index number of a new or existing server entry in the authentication server pool.	No default.
server-type {ldap | radius}	Set the server type to the server entry <entry_index>. Type ldap for a LDAP server or radius for a RADIUS server.	ldap
ldap-server <ldap-query_name>	Set the name of the LDAP query to the server entry <entry_index> if you set the server entry as LDAP. See the user ldap-user.	No default.

Variable	Description	Default
`radius-server <radius-query_name>`	Set the name of the RADIUS query to the server entry `<entry_index>` if you set the server entry as RADIUS. See the user radius-user.	No default.
`rsa-securid {enable | disable}`	Specify whether FortiWeb authenticates clients using a username and a RSA SecurID authentication code only. Users are not required to enter a password. When this option is enabled, the authentication delegation options in the site publish rule are not available. Available only if server-type {ldap | radius} is `radius` and client-auth-method {html-form-auth | http-auth | client-cert-auth} is `html-form-auth`.	`disable`

Example

For an example, see `config waf site-publish-helper rule`.

Related topics

- `config waf site-publish-helper rule`

waf site-publish-helper keytab_file

Use this command to group together web applications that you want to publish.

waf site-publish-helper policy

Use this command to group together web applications that you want to publish.

Before you configure site publishing policies, you must first define the individual sites that will be a part of the group. For details, see `config waf site-publish-helper rule`.

To apply this policy, include it in an inline web protection profile. See `config waf web-protection-profile inline-protection`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf site-publish-helper policy
   edit <site-publish-policy_name>
      set account-lockout {enable | disable}
```

```
        set lockout-threshold <lockout-threshold_int>
        set account-block-period <account-block-period_int>
        set reset-time <reset-time_int>
        config rule
          edit <entry_index>
            set rule-name <site-publish-rule_name>
          next
        end
      next
    end
```

Variable	Description	Default
<site-publish-policy_name>	Type the name of a new or existing policy. The maximum length is 35 characters. To display the list of existing policies, type: edit ?	No default.
account-lockout {enable | disable}	Enable or disable Account Lockout to prevent account cracking by locking an account out after several failures logging into FortiWeb.	disable
lockout-threshold <lockout-threshold_int>	Set the threshold of login failure. FortiWeb will trigger lockout to the account if number of login failure exceeds the threshold during the specified time period (reset-time <reset-time_int>).	5
account-block-period <account-block-period_int>	Set the time period (in minutes) that FortiWeb locks out an account for. No more login is accepted for the locked account during the period.	60
reset-time <reset-time_int>	Set the time period (in minutes) for FortiWeb counting the login failures and judging lockout to accounts. Count of login failure of an account will be reset when the time period is up.	3
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
rule-name <site-publish-rule_name>	Type the name of an existing rule.	No default.

Example

For an example, see config waf site-publish-helper rule.

Related topics

- config waf site-publish-helper rule
- config waf web-protection-profile inline-protection

waf site-publish-helper rule

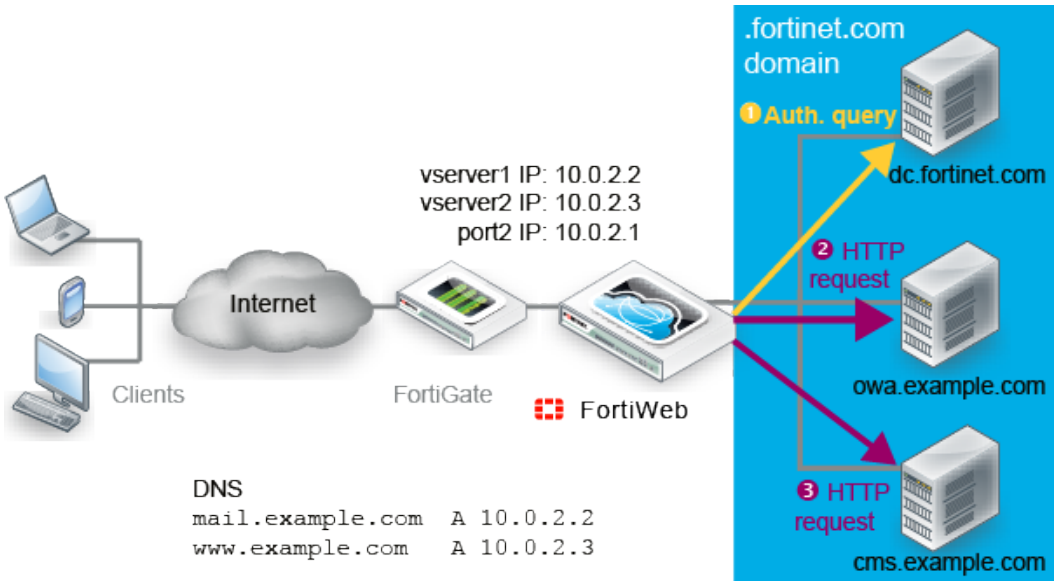
Use this command to configure access control, authentication, and, optionally, SSO for your web applications.

If:

- your users access 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: 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 sends the client’s credentials in a query to the authentication server. Once the client is successfully authenticated, if the web application supports HTTP authentication and you have configured delegation, 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..



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, and/or IIS. Your users will only need to authenticate once while using those resources.

Before you configure site publishing, you must first define the queries to your authentication server. For details, see `config user ldap-user` or `config server-policy custom-application application-policy`.

FortiWeb supports the following additional site publishing options:

- RADIUS authentication that requires users to provide a secondary password, PIN, or token code in addition to a username and password (two-factor authentication)
- RADIUS authentication that allows users to authenticate using their username and RSA SecurID token code only (no password)
- Regular Kerberos authentication delegation and Kerberos constrained delegation

For more information on these options, see the descriptions of the individual site publishing rule settings and the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf site-publish-helper rule
   edit <site-publish-rule_name>
      set status {enable | disable}
      set req-type {plain | regular}
      set published-site <host_fqdn>
      set path <url_str>
      set client-auth-method {html-form-auth | http-auth | client-cert-auth}
      [set logoff-path-type {plain | regular}]
      [set Published-Server-Logoff-Path <url_str>]
      set cookie-timeout <timeout_int>
      set auth-server-pool <authentication-server-pool_name>
```

```
        set auth-delegation {http-basic | kerberos  | kerberos-constrained-
            delegation | no-delegation}
        set field-name {subject | SAN}
        set attribution-name {email | UPN}
        set delegated-spn <delegated-spn_str>
        set keytab-file <keytab_file>
        set delegator-spn <delegator-spn_str>
        set prefix-support {enable | disable}
        set prefix-domain <prefix-domain_str>
        set alert-type {all | fail | none | success}
        set sso-support {enable | disable}
        set sso-domain <domain_str>
    next
end
```

Variable	Description	Default
`<site-publish-rule_name>`	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: `edit ?`	No default.
`status {enable | disable}`	Enable to activate this rule. This can be used to temporarily deactivate access to a single web application without removing it from a site publishing policy.	`enable`
`req-type {plain | regular}`	Select whether published-site <host_fqdn> contains a literal FQDN (`plain`), or a regular expression designed to match multiple host names or fully qualified domain names (`regular`).	`plain`
`published-site <host_fqdn>`	Depending on your selection in req-type {plain | regular}, type either: • the literal `Host:` name, such as `sharepoint.example.com`, that the HTTP request must contain in order to match the rule. • a regular expression, such as `^*\.example\.edu`, matching all and only the host names to which the rule should apply. The maximum length is 255 characters. **Note:** Regular expressions beginning with an exclamation point (`!`) are not supported. For information on language and regular expression matching, see the *FortiWeb Administration Guide*.	No default.

Variable	Description	Default
`path <url_str>`	Type the URL of the request for the web application, such as `/owa`. It must begin with a forward slash (/).	No default.
`client-auth-method {html-form-auth | http-auth | client-cert-auth}`	Specify one of the following options: • `html-form-auth` — FortiWeb authenticates clients by presenting an HTML web page with an authentication form • `http-auth` — FortiWeb authenticates clients by providing an HTTP `AUTH` code so that the browser displays its own dialog.return an HTTP `AUTH` code so that the browser displays its own dialog. • `client-cert-auth` — FortiWeb validates the HTTP client's personal certificate using the certificate verifier specified in the associated server policy or server pool configuration. Used when auth-delegation {http-basic | kerberos | kerberos-constrained-delegation | no-delegation} is `kerberos` or `no-delegation`. **Note:** This option requires you to select a value for ssl-client-verify <verifier_name> in the server policy or certificate-verify <verifier_name> in the server pool configuration.	`html-form-auth`
`logoff-path-type {plain | regular}`	Specify whether `Published-Server-Logoff-Path` contains a literal URL (`plain`), or a regular expression designed to match multiple URLs (`regular`).	

Variable	Description	Default
Published-Server-Logoff-Path <url_str>	This setting appears only if client-auth-method {html-form-auth | http-auth | client-cert-auth} is html-form-auth. Depending on the value of logoff-path-type, enter one of the following values: • the literal URL of the request that a client sends to log out of the application (for example, /owa/auth/logoff.aspx . • a regular expression that matches the request that a client sends to log out of the application. Ensure that the value is a sub-path of the path value. For example, if path is /owa , /owa/auth/logoff.aspx is a valid value. When a client logs out of the web application, FortiWeb redirects the client to its authentication dialog. **Note:**Regular expressions beginning with an exclamation point (!) are not supported. For information on language and regular expression matching, see the *FortiWeb Administration Guide*.	No default.
cookie-timeout <timeout_int>	Specify the length of time that passes before the cookie that the site publish rule adds expires and the client must re-authenticate. Valid values are from 0 to 3600 hours. To configure the cookie with no expiration, specify 0 (the default). The browser only deletes the cookie when the user closes all browser windows.	0
auth-server-pool <authentication-server-pool_name>	Enter the name of the pool of servers that FortiWeb uses to authenticate clients. See the waf site-publish-helper authentication-server-pool.	No default.

Variable	Description	Default
`auth-delegation {http-basic | kerberos | kerberos-constrained-delegation | no-delegation}`	Specify one of the following options: • `http-basic` — Use HTTP `Authorization:` 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 **protocol**-based authentication. Available only if client-auth-method {html-form-auth | http-auth | client-cert-auth} is `html-form-auth` or `http-auth`. • `kerberos` — After it authenticates the client via the HTTP form or HTTP basic method, FortiWeb obtains a Kerberos service ticket for the specified web application on behalf of the client. It adds the ticket to the HTTP `Authorization:` header of the client request with Base64 encoding. Available only if client-auth-method {html-form-auth | http-auth | client-cert-auth} is `html-form-auth` or `http-auth`. • `kerberos-constrained-delegation` — After it authenticates the client's certificate, FortiWeb obtains a Kerberos service ticket for the specified web application on behalf of the client. It adds the ticket to the HTTP `Authorization:` header of the client request with Base64 encoding. Available only if client-auth-method {html-form-auth | http-auth | client-cert-auth} is `client-cert-auth`. • `no-delegation` — FortiWeb does not send the client's credentials to the web application. Select this option when the web application has no authentication of its own or uses HTML form-based authentication. **Note:** If the web application uses HTML form-based authentication, the client is required to authenticate twice: once with FortiWeb and once with the web application's form. Not available when waf site-publish-helper rule is `enable`.	`no-delegation`

Variable	Description	Default
field-name {subject | SAN}	Use one of the following options to specify the certificate information that FortiWeb uses to determines the client username: • subject — The email address value in the certificate's Subject information. For attribution-name {email | UPN}, select email. • SAN — The certificate's subjectAltName (Subject Alternative Name or SAN) and either the User Principal Name (UPN) or the email address value in the certificate's Subject information. For attribution-name {email | UPN}, select UPN or email. In certificates issued in a Windows environment, the certificate's SAN and UPN contain the username. For example: username@domain Available only when auth-delegation {http-basic | kerberos | kerberos-constrained-delegation | no-delegation} is kerberos-constrained-delegation.	SAN
attribution-name {email | UPN}	Use one of the following options to specify the certificate information that FortiWeb uses to determines the client username: • email — The email address value in the certificate's Subject information. For field-name {subject | SAN}, specify subject or SAN. • UPN — The User Principal Name (UPN) value. For field-name {subject | SAN}, specify SAN. **Note:** Because the email value can be an alias rather than the real DC (domain controller) domain, the most reliable method for determining the username is SAN and UPN. Available only when auth-delegation {http-basic | kerberos | kerberos-constrained-delegation | no-delegation} is kerberos-constrained-delegation.	UPN

Variable	Description	Default
`delegated-spn <delegated-spn_str>`	Specify the Service Principal Name (SPN) for the web application that clients access using this site publish rule. A service principal name uses the following format: `<service_type >/<instance_name>:<port_number>/<service_name>` For example, for an Exchange server that belongs to the domain `dc1.com` and has the hostname `USER-U3LOJFPLH1`, the SPN is `http/USER-U3LOJFPLH1.dc1.com@DC1.COM`. Available only when auth-delegation {http-basic | kerberos | kerberos-constrained-delegation | no-delegation} is `kerberos` or `kerberos-constrained-delegation`.	No default.
`keytab-file <keytab_file>`	Specify the keytab file configuration for the AD user that FortiWeb uses to obtain Kerberos service tickets for clients. See `config waf site-publish-helper keytab_file`. Available only when auth-delegation {http-basic | kerberos | kerberos-constrained-delegation | no-delegation} is `kerberos-constrained-delegation`.	No default.
`delegator-spn <delegator-spn_str>`	Specify the Service Principal Name (SPN) that you used to generate the keytab specified by `keytab-file <keytab_file>`. This is the SPN of the AD user that FortiWeb uses to obtain a Kerberos service tickets for clients. Available only when auth-delegation {http-basic | kerberos | kerberos-constrained-delegation | no-delegation} is `kerberos-constrained-delegation`.	No default.

Variable	Description	Default
`prefix-support {enable | disable}`	Enable to allow users in environments that require users to log in using both a domain and username to log in with just a username. Also specify `prefix-domain <prefix-domain_str>`. In some environments, the domain controller requires users to log in with the username format `domain\username`. For example, if the domain is `example.com` and the username is `user1`, the user enters `EXAMPLE\user1`. Alternatively, enable this option and enter `EXAMPLE` for prefix-domain <prefix-domain_str>. The user enters `user1` for the username value and FortiWeb automatically adds `EXAMPLE\` to the HTTP `Authorization:` header before it forwards it to the web application. Available only when auth-delegation {http-basic | kerberos | kerberos-constrained-delegation | no-delegation} is `http-basic` or `kerberos`.	enable
`prefix-domain <prefix-domain_str>`	Enter a domain name that FortiWeb adds to the HTTP `Authorization:` header before it forwards it to the web application. Available only when prefix-support {enable | disable} is enabled. If `auth-delegation` is `kerberos`, ensure that the string is the full domain name (for example, `example.com`).	No default.
`sso-domain <domain_str>`	Type the domain suffix of `Host:` names that will be allowed to share this rule's authentication sessions, such as `.example.com`. Include the period (`.`) that precedes the host's name.	No default.

Variable	Description	Default
`sso-support {enable | disable}`	Enable for single sign-on support. For example, if this web site is `www1.example.com` and the SSO domain is `.example.com`, once a client has authenticated with that site, it can access `www2.example.com` without authenticating a second time. 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.	`disable`
`alert-type {all | fail | none | success}`	Select which site publishing-related authentication events the FortiWeb appliance will log and/or send an alert email about. • `all` • `fail` • `success` • `none` Event log messages contain the user name, authentication type, success or failure, and source address (for example, `User jdoe [Site Publish] login successful from 172.0.2.5`) when an end-user successfully authenticates. A similar message is recorded if the authentication fails (for example, `User hackers [Site Publish] login failed from 172.0.2.5`). **Note:** Logging and/or alert email occurs only if it is enabled and configured. See `config log disk` and `config log alertemail`.	`none`

Example

This example configures a site publisher with SSO for both Outlook and Sharepoint on the example.com domain.

```
config waf site-publish-helper authentication-server-pool
   edit "LDAP server pool"
      edit 1
         set server-type ldap
         set ldap-server "LDAP query 1"
      end
   next
end
config waf site-publish-helper authentication-server-pool
```

```
      edit "RADIUS server pool"
         edit 1
            set server-type radius
            set ldap-server "RADIUS query 1"
         end
      next
   end
   config waf site-publish-helper rule
      edit "Outlook"
         set published-site ^*\.example\.edu
         set auth-server-pool "LDAP server pool"
         set auth-delegation http-basic
         set sso-support enable
         set sso-domain .example.edu
         set path /owa
         set alert-type fail
         set Published-Server-Logoff-Path /owa/auth/logoff.aspx?Cmd=logoff
      next
      edit "Sharepoint"
         set published-site ^*\\.example\\.edu
         set req-type regular
         set auth-server-pool "RADIUS server pool"
         set auth-delegation http-basic
         set sso-support enable
         set sso-domain .example.edu
         set path /sharepoint
         set alert-type fail
      next
   end
   config waf site-publish-helper policy
      edit "example_com_apps"
         config rule
            edit 1
               set rule-name Outlook
            next
            edit 2
               set rule-name Sharepoint
            next
         end
      next
   end
```

Related topics

- config waf site-publish-helper policy
- config waf site-publish-helper authentication-server-pool
- config log trigger-policy
- config server-policy allow-hosts
- config waf web-protection-profile inline-protection

waf start-pages

Use this command to configure start page rules.

When a start page group is selected in the inline protection profile, HTTP clients must begin from a valid start page in order to initiate a valid session.

For example, you may wish to specify that HTTP clients of an e-commerce web site must begin their session from either an item view or the first stage of the shopping cart checkout, and cannot begin a valid session from the third stage of the shopping cart checkout.

To apply start pages, select them within an inline protection profile. For details, see `config waf web-protection-profile inline-protection`.

Before you configure a start page rule, if you want to apply it only to HTTP requests for a specific real or virtual host, you must first define the web host in a protected hosts group. For details, see `config server-policy allow-hosts`.

You can use SNMP traps to notify you when a start page rule is enforced. For details, see `config system snmp community`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf start-pages
   edit <start-page-rule_name>
      set action {alert | alert_deny | block-period | redirect | send_403_
          forbidden}
      set block-period <seconds_int>
      set severity {Low | Medium | High}
      set trigger <trigger-policy_name>
      config start-page-list
         edit <entry_index>
            set host <protected-hosts_name>
            set host-status {enable | disable}
            set request-file <url_str>
            set request-type {plain | regular}
            set default {yes | no}
         next
      end
   next
end
```

Variable	Description	Default
`<start-page-rule_name>`	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: `edit ?`	No default.

Variable	Description	Default
action {alert | alert_deny | block-period | redirect | send_403_forbidden}	Select one of the following actions that the FortiWeb appliance will perform when an HTTP request that initiates a session does not begin with one of the allowed start pages. • 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 FortiWeb returns to the client with the HTTP status code. See the *FortiWeb Administration Guide* or config system replacemsg. • block-period — Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int>. **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 config waf x-forwarded-for). 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 and generate an alert email and/or log message. Also configure redirect-url <redirect_fqdn> and rdt-reason {enable | disable}. • send_403_forbidden — Reply to the client with an HTTP 403 Access Forbidden error message and generate an alert email and/or log message. **Caution:** This setting will be ignored if monitor-mode {enable | disable} is enabled. **Note:** Logging and/or alert email will occur only if enabled and configured. See config log disk and config log alertemail. **Note:** If you select an auto-learning profile with this rule, you should select alert. If the action is alert_deny, for example, the FortiWeb appliance will block the request or reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see config waf web-protection-profile autolearning-profile.	No default.
block-period <seconds_int>	If action is block-period, type, specify the number of seconds that the connection will be blocked. The valid range is from 1 to 3,600 seconds.	1

Variable	Description	Default
`severity {Low | Medium | High}`	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	`Low`
`trigger <trigger-policy_name>`	Type the name of the trigger to apply when this rule is violated (see `config log trigger-policy`). The maximum length is 35 characters. To display the list of existing trigger policies, type: `set trigger ?`	No default.
`<entry_index>`	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
`host <protected-hosts_name>`	Type the name of a protected host that the `Host:` field of an HTTP request must be in order to match the start page rule. The maximum length is 255 characters. This setting applies only if `host-status` is `enable`.	No default.
`host-status {enable | disable}`	Enable to apply this start page rule only to HTTP requests for specific web hosts. Also configure host <protected-hosts_name>. Disable to match the start page rule based upon the other criteria, such as the URL, but regardless of the `Host:` field.	`disable`
`request-file <url_str>`	Depending on your selection in request-type {plain | regular}, type either: • the literal URL, such as `/index.php`, that the HTTP request must contain in order to match the start page rule. The URL must begin with a slash (/). • a regular expression, such as `^/*.php`, matching all and only the URLs to which the start page rule should apply. The pattern is **not** required to begin with a slash (/). However, it must at least match URLs that begin with a slash, such as `/index.cfm`. Do not include the name of the web host, such as `www.example.com`, which is configured separately in host <protected-hosts_name>. The maximum length is 255 characters. **Note:** Regular expressions beginning with an exclamation point (`!`) are not supported. For information on language and regular expression matching, see the *FortiWeb Administration Guide*.	No default.

Variable	Description	Default
`request-type {plain | regular}`	Select whether request-file <url_str> will contain a literal URL (`plain`), or a regular expression designed to match multiple URLs (`regular`).	`plain`
`default {yes | no}`	Type `yes` to use the page as the default for HTTP requests that either: • do not specify a URL • do not specify the URL of a valid start page (only if you have selected `redirect` from `action`) Otherwise, type `no`.	`no`

Example

This example redirects clients to the default start page, /index.html, if clients request a page that is not one of the valid start pages (`/index.html` or `/cart/login.jsp`). Redirection will occur only if the request is destined for one of the virtual or real hosts defined in the protected hosts group named `example_com_hosts`.

```
config waf start-pages
   edit "start-page-rule1"
      edit 1
         set host "example_com"
         set host-status enable
         set request-file "/index.html"
         set default yes
      next
      edit 2
         set host "example_com_hosts"
         set host-status enable
         set request-file "/cart/login.jsp"
         set default no
      next
   next
end
```

Related topics

- config log trigger-policy
- config server-policy allow-hosts
- config waf web-protection-profile inline-protection
- config system snmp community

waf url-access url-access-policy

Use this command to configure a set of URL access rules that define HTTP requests that are allowed or denied.

Before using this command, you must first define your URL access rules (see `config waf url-access url-access-rule`).

To apply URL access policies, select them within an inline or offline protection profile. For details see `config waf web-protection-profile inline-protection` or `config waf web-protection-profile offline-protection`.

You can use SNMP traps to notify you when a URL access rule is enforced. For details, see `config system snmp community`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf url-access url-access-policy
   edit <url-access-policy_name>
      config rule
         edit <entry_index>
            set url-access-rule-name <url-access-rule_name>
         next
      end
   next
end
```

Variable	Description	Default
`<url-access-policy_name>`	Type the name of the new or existing URL access policy. The maximum length is 35 characters. To display the list of existing policies, type: `edit ?`	No default.
`<entry_index>`	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
`url-access-rule-name <url-access-rule_name>`	Type the name of the existing URL access rule to add to the policy. The maximum length is 35 characters.	No default.

Example

This example adds two rules to the policy, with the first one set to priority level 0, and the second one set to priority level 1. The rule with priority 0 would be applied first.

```
config waf url-access url-access-policy
   edit "URL-access-set2"
      config rule
         edit 1
            set url-access-rule-name "URL Access Rule 1"
         next
         edit 2
            set url-access-rule-name "Blocked URL"
         next
      next
```

```
    end
```

Related topics

- config waf url-access url-access-rule
- config waf web-protection-profile inline-protection
- config waf web-protection-profile offline-protection

waf url-access url-access-rule

Use this command to configure URL access rules that define the HTTP requests that are allowed or denied based on their host name and URL.

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.

To apply URL access rules, first group them within a URL access policy. For details see, config waf url-access url-access-policy.

You can use SNMP traps to notify you when a URL access rule is enforced. For details, see config system snmp community.

To use this command, your administrator account's access control profile must have either w or rw permission to the wafgrp area. For more information, see Permissions on page 74.

Syntax

```
config waf url-access url-access-rule
   edit <url-access-rule_name>
      set action {alert_deny | continue | pass}
      set host <protected-hosts_name>
      set host-status {enable | disable}
      set severity {Low | Medium | High}
      set trigger <trigger-policy_name>
      config match-condition
         edit <entry_index>
            set sip-address-check {enable | disable}
            set sip-address-type {sip | sdomain | source-domain}
            set sip-address-value <client_ip>
            set sdomain-type {ipv4 | ipv6}
            set sip-address-domain <fqdn_str>
            set source-domain-type {simple-string | regex-expression}
            set source-domain <source-domain_str>
            set type {regex-expression | simple-string}
            set reg-exp <object_pattern>
            set reverse-match {yes | no}
         next
      end
   next
end
```

Variable	Description	Default
<url-access-rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: edit ?	No default.
action {alert_deny | continue | pass}	Select which action the FortiWeb appliance will take when a request matches the URL access rule. • 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 FortiWeb returns to the client with the HTTP status code. See the *FortiWeb Administration Guide* or config system replacemsg. • continue — Generate an alert and/or log message, then continue by evaluating any subsequent rules defined in the web protection profile (see diagnose debug flow trace). If no other rules are violated, allow the request. If multiple rules are violated, a single request will generate multiple attack log messages. • pass — Allow the request. Do **not** generate an alert and/or log message. **Caution:** This setting will be ignored if monitor-mode {enable | disable} is enabled. **Note:** Logging and/or alert email will occur only if enabled and configured. See config log disk and config log alertemail. **Note:** If an auto-learning profile will be selected in the policy with offline protection profiles that use this rule, you should select pass. If the action is alert_deny, the FortiWeb appliance will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For more information on auto-learning requirements, see config waf web-protection-profile autolearning-profile.	alert
host <protected-hosts_name>	Type the name of a protected host that the Host: field of an HTTP request must be in order to match the rule. The maximum length is 255 characters. This setting is used only if host-status is enable.	No default.

Variable	Description	Default
`host-status {enable | disable}`	Enable to require that the `Host:` field of the HTTP request match a protected hosts entry in order to match the rule. Also configure `host <protected-hosts_name>`.	`disable`
`severity {Low | Medium | High}`	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 a blacklisted IP address attempts to connect to your web servers: • `Low` • `Medium` • `High`	No default.
`trigger <trigger-policy_name>`	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 `config log trigger-policy`). The maximum length is 35 characters. To display the list of existing trigger policies, type: `set trigger ?`	No default.
`<entry_index>`	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
`sip-address-check {enable | disable}`	Enable to add the client's source IP address as a criteria for matching the URL access rule. Also configure sip-address-type {sip | sdomain | source-domain} and the specific settings for each source address type.	`disable`
`sip-address-type {sip | sdomain | source-domain}`	• `sip` — Configure sip-address-value <client_ip>. • `sdomain` — Configure sdomain-type {ipv4 | ipv6} and sip-address-domain <fqdn_str>. • `source-domain` — Configure source-domain-type {simple-string | regex-expression} and source-domain <source-domain_str>.	`sip`

Variable	Description	Default
sip-address-value <client_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 (for example, 172.22.14.1-172.22.14.255 or 10:200::10:1-10:200:10:100). Available only if sip-address-type {sip | sdomain | source-domain} is sip.	0.0.0.0
sdomain-type {ipv4 | ipv6}	Specifies the type of IP address FortiWeb retrieves from the DNS lookup of the domain specified by sip-address-domain <fqdn_str>. Available only if sip-address-type {sip | sdomain | source-domain} is sdomain.	No default.
sip-address-domain <fqdn_str>	Specifies the domain to match the client source IP after DNS lookup. Available only if sip-address-type {sip | sdomain | source-domain} is sdomain.	No default.
source-domain-type {simple-string | regex-expression}	• simple-string — source-domain specifies a literal domain. • regex-expression — source-domain specifies a regular expression that is designed to match multiple URLs. Available only if sip-address-type {sip | sdomain | source-domain} is source-domain.	simple-string
source-domain <source-domain_str>	Enter a literal domain or a regular expression that is designed to match multiple URLs. Available only if sip-address-type {sip | sdomain | source-domain} is sdomain.	No default.
type {regex-expression | simple-string}	Select how to use the text in reg-exp <object_pattern> to determine whether or not a request URL meets the conditions for this rule. • simple-string — The text is a string that request URLs must match exactly. • regular-expression — The text is a regular expression that defines a set of matching URLs.	No default.

Variable	Description	Default
reg-exp <object_pattern>	Depending on your selection in type {regex-expression | simple-string} and reverse-match {yes | no}, type a regular expression that defines either all matching or all non-matching URLs. Then, also configure reverse-match {yes | no}. For example, for the URL access rule to match all URLs that begin with /wordpress, you could enter ^/wordpress, then, in reverse-match {yes | no}, select no. The pattern is **not** required to begin with a slash (/). The maximum length is 255 characters. **Note:** Regular expressions beginning with an exclamation point (!) are not supported. Instead, use reverse-match {yes | no}.	No default.
reverse-match {yes | no}	Indicate how to use reg-exp <object_pattern> when determining whether or not this rule's condition has been met. • no — If the simple string or regular expression **does** match the request URL, the condition is met. • yes — If the simple string or regular expression does **not** match the request URL, the condition is met. The effect is equivalent to preceding a regular expression with an exclamation point (!).	no

Example

This example defines two sets of URL access rules.

The first set, Blocked URL, defines two URL match conditions: one uses a simple string to match an administrative page, and the other uses a regular expression to match a set of dynamic URLs for statistics pages.

The second set, Allowed URL, defines a single match condition that uses a regular expression to match all dynamic forms of the index page.

Actual blocking or allowing of the URLs, however, would not occur until a policy applies these URL access rules, and sets an action that the FortiWeb appliance will perform when an HTTP request matches either rule set.

```
config waf url-access url-access-rule
   edit "Blocked URL"
      config match-condition
         edit 1
            set type simple-string
            set reg-exp "/admin.php"
         next
         edit 2
            set type regular-expression
            set reverse-match no
```

```
            set reg-exp "statistics.php*"
          next
        end
      next
      edit "Allowed URL"
        config match-condition
          edit 1
            set type regular-expression
            set reverse-match no
            set reg-exp "index.php*"
          next
        end
      next
    end
```

Related topics

- config waf web-protection-profile inline-protection
- config waf web-protection-profile offline-protection
- config waf url-access url-access-policy

waf url-rewrite url-rewrite-policy

Use this command to group URL rewrite rules.

Before you can configure a URL rewrite group, you must first configure any URL rewriting rules that you want to include. For details, see config waf url-rewrite url-rewrite-rule.

To apply a URL rewriting group, select it in an inline protection profile. For details, see config waf web-protection-profile inline-protection.

To use this command, your administrator account's access control profile must have either w or rw permission to the wafgrp area. For more information, see Permissions on page 74.

Syntax

```
config waf url-rewrite url-rewrite-policy
  edit <url-rewrite-group_name>
    config rule
      edit <entry_index>
        set url-rewrite-rule-name <url-rewrite-rule_name>
        next
    end
  next
end
```

Variable	Description	Default
<url-rewrite-group_name>	Type the name of the URL rewriting rule group. The maximum length is 35 characters. To display the list of existing group, type: edit ?	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
url-rewrite-rule-name <url-rewrite-rule_name>	Type the name of an existing URL rewriting rule that you want to include in the group. The maximum length is 35 characters.	No default.

Related topics

- config waf url-rewrite url-rewrite-rule
- config waf web-protection-profile inline-protection

waf url-rewrite url-rewrite-rule

Use this command to configure URL rewrite rules or to redirect requests.

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 the *FortiWeb Administration Guide*.

To use a URL rewriting rule, add it to a policy. For details, see `config waf url-rewrite url-rewrite-policy`.

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf url-rewrite url-rewrite-rule
   edit <url-rewrite-rule_name>
      set action {403-forbidden | redirect | redirect-301 |
          http-body-rewrite | http-header-rewrite | location-rewrite}
      set host {<server_fqdn> | <server_ipv4> | <host_pattern>}
      set host-status {enable | disable}
      set host-use-pserver {enable | disable}
      set url <replacement-url_str>
      set url-status {enable | disable}
      set location <location_str>
      set location_replace <location_str>
      set referer-status {enable | disable}
      set referer <referer-url_str>
      set referer-use-pserver {enable | disable}
      set analyzer-policy <fortianalyzer-policy_name>
      config match-condition
         edit <entry_index>
            set content-filter {enable | disable}
            set content-type-set {text/html text/plain text/javascript
                application/xml(or)text/xml application/javascript
                application/soap+xml application/x-javascript}
            set HTTP-protocol {http | https}
            set is-essential {yes | no}
            set object {http-host | http-reference | http-url}
            set protocol-filter {enable | disable}
            set reg-exp <object_pattern>
            set reverse-match {yes | no}
```

```
            next
          end
        next
      end
```

Variable	Description	Default
<url-rewrite-rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing rules, type: edit ?	No default.
action {403-forbidden | redirect | redirect-301 | http-body-rewrite | http-header-rewrite | location-rewrite}	Specify one of the following values: • 403-forbidden — Send a 403 (Forbidden) response to the client. • redirect — Send a 302 (Moved Temporarily) response to the client, with a new Location: field in the HTTP header. • redirect-301 — Send a 301 (Moved Permanently) response to the client, with a new Location: field in the HTTP header. • http-body-rewrite — Replace the specific HTTP content in the body of responses. • http-header-rewrite — Rewrite the host, referer and request URL fields in HTTP header. • location-rewrite — Rewrite the location string in a 302 redirect.	http-header-rewrite

Variable	Description	Default

`host {<server_fqdn> | <server_ipv4> | <host_pattern>}`	Type the FQDN of the host, such as `store.example.com`, to which the request will be redirected. The maximum length is 255 characters.
	
	This option is available only when `host-status` is enabled and `action` is `http-header-rewrite`.
	
	This field supports back references such as `$0` to the parts of the original request that matched any capture groups that you entered in reg-exp <object_pattern> for each object in the condition table. (A capture group is a regular expression, or part of one, surrounded in parentheses.)
	
	Use `$`**n** (0 <= **n** <= 9) to invoke a substring, where **n** is the order of appearance of the regular expression, from left to right, from outside to inside, then from top to bottom.
	
	For example, regular expressions in the condition table in this order:
	
	`(a)(b)(c(d))(e)`
	
	`(f)`
	
	would result in invokable variables with the following values:
	
	• `$0` — a
	• `$1` — b
	• `$2` — cd
	• `$3` — d
	• `$4` — e
	• `$5` — f
		No default.

`host-status {enable | disable}`	Enable to rewrite the `Host:` field or host name part of the `Referer:` field. When disabled, the FortiWeb appliance preserves the value from the client's request when rewriting it. This option is available only when `action` is `http-header-rewrite`.	`disable`

Variable	Description	Default
`host-use-pserver {enable | disable}`	Enable this when you have a server farm for server balance or content routing. In this case you do not know which server in the server farm the FortiWeb appliance will use. When FortiWeb processes the request, it sets the value for the actual host. This option is available only when `host-status` is enabled and `action` is `http-header-rewrite`. Any setting you make for `host` is ignored.	`disable`
`url <replacement-url_str>`	Type the string, such as `/catalog/item1`, that will replace the request URL. The maximum length is 255 characters. This option is available only when `url-status` is enabled and `action` is `http-header-rewrite`. Do not include the name of the web host, such as `www.example.com`, nor the protocol, which are configured separately in host {<server_fqdn> | <server_ipv4> | <host_pattern>}. Like `host`, this field supports back references such as `$0` to the parts reg-exp <object_pattern> for each object in the condition table. For an example, see the *FortiWeb Administration Guide*.	No default.
`url-status {enable | disable}`	Enable to rewrite the URL part of the request URL. If you disable this option, the FortiWeb appliance preserves the value from the client's request when it rewrites it. This option is available only when `action` is `http-header-rewrite`.	`disable`
`location <location_str>`	Enter the replacement value for the `Location:` field in the HTTP header for the 302 response. The maximum length is 255 characters. This option is available only when `action` is `redirect`.	No default.
`location_replace <location_str>`	Type the URL string that provides a location for use in a 302 HTTP redirect response from a web server connected to FortiWeb. The maximum length is 255 characters. This option is available only when `action` is `location-rewrite`.	No default.

Variable	Description	Default
`referer-status {enable | disable}`	Enable to rewrite the `Referer:` field in the HTML header. Also configure referer <referer-url_str> and referer-use-pserver {enable | disable}.	`disable`
`referer <referer-url_str>`	Type the replacement value for the `Referer:` field in the HTML header. The maximum length is 255 characters. This option is available only when `referer-status` is enabled.	No default.
`referer-use-pserver {enable | disable}`	Enable this when you have a server farm for server balance or content routing. In this case you do not know which server in the server farm the FortiWeb appliance will use. When FortiWeb processes the request, it sets the value for the actual referrer. This option is available only when `referer-status` is enabled and `action` is `http-header-rewrite`. Any setting you make for `referer` is ignored.	`disable`
`body_replace <replacement_str>`	Type the value that will replace matching HTTP content in the body of responses. The maximum is 255 characters. For an example, see the *FortiWeb Administration Guide*. This option is available only when `action` is `http-body-rewrite`.	No default.
`<entry_index>`	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
`content-filter {enable | disable}`	Enable if you want to match this condition only for specific HTTP content types (also called Internet or MIME file types) such as `text/html`, as indicated in the `Content-Type:` HTTP header. Also configure content-type-set {text/html text/plain text/javascript application/xml(or)text/xml application/javascript application/soap+xml application/x-javascript}.	`disable`
`content-type-set {text/html text/plain text/javascript application/xml(or) text/xml application/javascript application/soap+xml application/x-javascript}`	Type the HTTP content types that you want to match in a space-delimited list, such as: `set content-type-set text/html text/plain`	No default.

Variable	Description	Default
`HTTP-protocol {http | https}`	Select which protocol will match this condition, either HTTP or HTTPS. This option is applicable only if `protocol-filter` is set to `enable`.	`http`
`is-essential {yes | no}`	Select what to do if there is no `Referer:` field, either: • `no` — Meet this condition. • `yes` — Do not meet this condition. Requests can lack a `Referer:` field for several reasons, such as if the user manually types the URL, and the request does not result from a hyperlink from another web site, or if the URL resulted from an HTTPS connection. (See the RFC 2616 section on the `Referer:` field.) In those cases, the field cannot be tested for a matching value. This option appears only if `object` is `http-reference`.	`yes`
`object {http-host | http-reference | http-url}`	Select which part of the HTTP request to test for a match: • `http-host` • `http-url` • `http-reference` (the `Referer:` field) If the request must match multiple conditions (for example, it must contain both a matching `Host:` field and a matching URL), add each object match condition to the condition table separately.	`http-host`
`protocol-filter {enable | disable}`	Enable if you want to match this condition only for either HTTP or HTTPS. Also configure HTTP-protocol {http | https}. 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. 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.	`disable`

Variable	Description	Default
`reg-exp <object_pattern>`	Depending on your selection in object {http-host | http-reference | http-url} and `reverse-match {yes | no}`, type a regular expression that defines either all matching or all non-matching `Host:` fields, URLs, or `Referer:` fields. Then, also configure `reverse-match {yes | no}`. For example, for the URL rewriting rule to match all URLs that begin with `/wordpress`, you could enter `^/wordpress`, then, in `reverse-match {yes | no}`, select `no`. The pattern is **not** required to begin with a slash (/). The maximum length is 255 characters. **Note:** Regular expressions beginning with an exclamation point (`!`) are not supported. Instead, use `reverse-match {yes | no}`.	No default.
`reverse-match {yes | no}`	Indicate how to use reg-exp <object_pattern> when determining whether or not this URL rewriting condition has been met. • `no` — If the regular expression **does** match the request object, the condition is met. • `yes` — If the regular expression does **not** match the request object, the condition is met. The effect is equivalent to preceding a regular expression with an exclamation point (`!`). If all conditions are met, the FortiWeb appliance will do your selected `action`.	`no`

Related topics

- `config waf url-rewrite url-rewrite-policy`

waf user-tracking policy

Use this command to group user tracking rules, which track sessions by user and capture a username to reference in traffic and attack log messages.

Before you configure a user-tracking policy, define the rules to add (see `config waf user-tracking rule`).

To apply a user tracking policy, you select it in an inline or offline protection profile. For details, see `config waf web-protection-profile inline-protection` or `config waf web-protection-profile offline-protection`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf user-tracking policy
   edit <user-tracking-policy_name>
      config input-rule-list
         edit <entry_index>
            set input-rule <input-rule_name>
         next
      end
   next
end
```

Variable	Description	Default
`<user-tracking-policy_name>`	Type the name of a new or existing policy. The maximum length is 35 characters. To display the list of existing policies, type: `edit ?`	No default.
`<entry_index>`	Type the index number of the individual entry in the table.	No default.
`input-rule <input-rule_name>`	Type the name of an existing rule.	No default.

waf user-tracking rule

Use this command to configure FortiWeb to track sessions by user and capture a username to reference in traffic and attack log messages.

When FortiWeb detects users that match the criteria that you specify in a user tracking policy, it stores the session ID and username.

To apply a user tracking rule, add it to a user tracking policy that you can select in an inline or offline protection profile. See `config waf user-tracking policy`.

You can apply a user tracking policy using either an inline or offline protection profile. However, in offline protection mode, `session-fixation-protection`, `session-timeout-enforcement`, and the deny, redirect and period block actions are not supported.

You can also use the user tracking feature to create a filter in a custom rule that matches specific users. This type of custom rule requires you to create a user tracking policy and apply it to the protection profile that uses the custom rule. See `config waf custom-access rule`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf user-tracking rule
   edit <rule_name>
      set hostname-ip <hostname-ip_str>
      set host-status { enable | disable}
      set authentication-url <url_str>
      set username-parameter <username_str>
      set password-parameter <password_str>
      set session-id-name <session-id_str>
      set logoff-path <logoff_str>
      set session-fixation-protection { enable | disable}
      set session-timeout-enforcement { enable | disable}
      set session-timeout <timeout_int>
      set session-frozen-time <frozen-time_int>
      set session-frozen-action { alert | alert_deny | redirect | block-period}
      set session-frozen-block-period <block-period_int>
      set session-frozen-severity { High | Medium | Low}
      set session-frozen-trigger <trigger-policy_name>
      set default-action { failed | success}
         config match-condition
            edit <entry_index>
               set authentication-result-type { failed | success}
               set HTTP-match-target { return-code | response-body | redirect-url}
               set value-type { plain | regular}
               set value <value-str>
            next
         end
   next
end
```

Variable	Description	Default
<rule_name>	Enter a name that identifies the rule.	No default.
hostname-ip <hostname-ip_str>		No default.
host-status { enable | disable}		No default.
authentication-url <url_str>	Enter the URL to match in authorization requests. Ensure that the value begins with a forward slash (/).	No default.
username-parameter <username_str>	Enter the username field value to match in authorization requests.	No default.
password-parameter <password_str>	Enter the password field value to match in authorization requests.	No default.

Variable	Description	Default
`session-id-name <session-id_str>`	Type the name of the session ID that is used to identify each session. Examples of session ID names are `sid`, `PHPSESSID`, and `JSESSIONID`	No default.
`logoff-path <logoff_str>`	Optionally, enter the URL of the request that a client sends to log out of the application. When the client sends this URL, FortiWeb stops tracking the user session. Ensure that the value begins with a forward slash (/).	No default.
`session-fixation-protection { enable | disable}`	Enter `enable` to configure FortiWeb to erase session IDs from the cookie and argument fields of a matching login request. FortiWeb erases the IDs for non-authenticated sessions only. For web applications that do not renew the session cookie when a user logs in, it is possible for an attacker to trick a user into authenticating with a session ID that the attacker acquired earlier. This feature prevents the attacker from accessing the web app in an authenticated session. When this feature removes session IDs, FortiWeb does not generate a log message because it is very common for a legitimate user to access a web application using an existing cookie. For example, a client who leaves his or her web browser open between sessions presents the cookie from an earlier session. **Caution:** This option is not supported in offline protection mode.	`disable`
`session-timeout-enforcement { enable | disable}`	Enter `enable` to configure FortiWeb to remove the session ID for user sessions that are idle for longer than the length of time specified by `session-timeout`. When a session is reset, the client has to log in again to access the back-end server. If a session exceeds the timeout threshold, instead of tracking subsequent matching sessions by user, FortiWeb takes the specified action, for a length of time specified by `session-frozen-time`.	`disable`

Variable	Description	Default
`session-timeout <timeout_int>`	Enter the length of time in minutes that FortiWeb waits before it stops tracking an inactive user session. Valid values are from 1 to 14400.	`30`
`session-frozen-time <frozen-time_int>`	Enter the length of time after a session exceeds the timeout threshold that FortiWeb takes the specified action against requests with the ID of the timed-out session. After the freeze time has elapsed, FortiWeb removes the session ID for idle sessions but no longer takes the specified action. Available only when `session-timeout-enforcement` is `enable`.	`30`

Variable	Description	Default
`session-frozen-action { alert | alert_deny | redirect | block-period}`	Enter the action that FortiWeb takes against requests with the ID of a timed-out session during the specified time period: • `alert` — Accept the request and generate an alert email and/or log message. • `alert_deny` — Block the request and generate an alert email and/or log message. You can customize the web page that FortiWeb returns to the client with the HTTP status code. See the *FortiWeb Administration Guide* or `config system replacemsg`. **Note:** In offline protection mode, because the deny action is not supported, this option has the same effect as `alert`. • `redirect` — Redirect the request to the URL that you specify in the protection profile and generate an alert and/or log message. Also configure `redirect-url <redirect_fqdn>` and `rdt-reason {enable | disable}`. **Caution:** This option is not supported in offline protection mode • `block-period` — Block subsequent requests from the client for a specified number of seconds. You can customize the web page that FortiWeb returns to the client with the HTTP status code. See the *FortiWeb Administration Guide* or `config system replacemsg`. **Caution:** This option is not supported in offline protection mode When the action generates a log message, the message field value is `Session Timeout Enforcement: triggered by user <username>`. Available only when `session-timeout-enforcement` is `enable`.	`alert`
`session-frozen-block-period <block-period_int>`	Type the number of seconds to block requests with the ID of a timed-out session. This setting is available only if `action` is `block-period`. The valid range is from 1 to 3,600 (1 hour).	`60`

Variable	Description	Default
`session-frozen-severity { High | Medium | Low}`	When the session timeout settings generate an attack log, each log message contains a **Severity Level** (`severity_level`) field. Select which severity level FortiWeb uses when it takes the specified action: • `Low` • `Medium` • `High` Available only when `session-timeout-enforcement` is `enable`.	`Low`
`session-frozen-trigger <trigger-policy_name>`	Type the name of the trigger, if any, to apply when FortiWeb detects requests with the ID of a timed-out session (see `config log trigger-policy`). The maximum length is 35 characters. To display the list of existing triggers, type: `set trigger ?`	No default.
`default-action { failed | success}`	Enter the authentication result that FortiWeb associates with requests that match the criteria but do not match an entry in the Authentication Result Condition Table. When the login result is successful, FortiWeb tracks the session using the session ID and username values.	`failed`
`<entry_index>`	Type the index number of the individual entry in the table.	No default.
`authentication-result-type { failed | success}`	Specify the status FortiWeb assigns to user logins that match this table item: `failed` or `successful`. FortiWeb tracks sessions by user only when the status is `successful`. If the request does not match any rules in this table, FortiWeb uses the value specified by `default-action`.	`success`
`HTTP-match-target { return-code | response-body | redirect-url}`	Select the location of the value to match with the string or regular expression specified in this table item: `return-code`, `response-body`, `redirect-url`.	`return-code`
`value-type { plain | regular}`	Indicate whether `value` is a simple string (`plain`) or a regular expression (`regular`).	`plain`
`value <value-str>`	Enter the value to match.	No default.

Example

This example matches requests from clients using the URL "/login2" with the parameters "user" and "pass" and a session ID specified by "jsessionid." FortiWeb tracks matching sessions by user and stops tracking if the client logs out using the URL "/logout2".

FortiWeb tracks only requests with the return code 200, which it classifies as successful. It does not track requests with a response body that matches the regular expression "deny". In addition, because the rule uses the default value for the default authentication result, it does not track requests that do not match an item in the list of match conditions.

The rule enables both session fixation protection and session timeout enforcement for tracked sessions. If a session is idle longer than the default session timeout, FortiWeb blocks requests from clients that use the session ID that has timed out for the default period block time. It performs this action for 30 minutes after the session times out (the default session freeze time).

```
config waf user-tracking
   edit "rule1"
      set authentication-url /login2
      set username-parameter user
      set password-parameter pass
      set session-id-name jsessionid
      set logoff-path /logout2
      set session-fixation-protection enable
      set timeout-enforcement enable
      set session-frozen-action period-block
      set session-frozen-severity High
      set session-frozen-trigger "trigger1"
      config match-condition
         edit 1
            set authentication-result-type success
            set HTTP-match-target return-code
            set value-type plain
            set value 200
         next
         edit 2
            set authentication-result-type failed
            set HTTP-match-target return
            set value-type regular
            set value deny
         next
      end
   next
end
```

Related topics

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

waf web-cache-exception

Use this command to configure FortiWeb to cache responses from your servers.

Use `web-cache-exception` to cache all URLs except for a few. To cache only a few URLs, see `config waf web-cache-policy`.

To apply this policy, include it in an inline protection profile. For details, see `config waf web-protection-profile inline-protection`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf web-cache-exception
   edit <web-cache-exception_rule_name>
      config exception-list
         edit <entry_index>
            set host-status {enable | disable}
            set host <host_str>
            set url-type {plain | regular}
            set url-pattern <url-pattern_str>
            set cookie-name <cookie-name_str>
      end
   next
end
```

Variable	Description	Default
<web-cache-exception_rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing policies, type: `edit ?`	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
host-status {enable | disable}	Specify `enable` to require that the `Host:` field of the HTTP request match a protected host names entry in order to match the exception. Also specify a value for `host`.	`disable`
<host_str>	Specify 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 exception. Maximum length is 255 characters. This option is available only if the value of `host-status` is `enabled`.	No default.

Variable	Description	Default
{plain | regular}	Specify the type of value that is used for url-pattern: • plain — A literal URL. • regular — A regular expression designed to match multiple URLs.	plain
<url-pattern_str>	If the value of url-type is plain, specify the literal URL, such as /index.php, that the HTTP request must contain in order to match the rule. The URL must begin with a slash (/). If the value of url-type is regular, specify a regular expression, such as ^/*.php, that matches all and only the URLs that the rule applies to. The pattern does not require a slash (/); however, it must match URLs that begin with a slash, such as /index.cfm. Do not include the domain name, such as www.example.com, which is specified by host. Maximum length is 255 characters. **Tip:** Generally, URLs that require autolearning adapters do not work well with caching either. Do not cache dynamic URLs that contain variables such as user names (e.g. older versions of Microsoft OWA) or volatile data such as parameters. Because FortiWeb is unlikely to receive identical subsequent requests for them, dynamic URLs can rapidly consume cache without improving performance.	No default.
<cookie-name_str>	Specify the name of the cookie, such as sessionid, as it appears in the Cookie: HTTP header. Maximum length is 127 characters. **Tip:** 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.	No default.

Related topics

- config waf web-cache-policy
- config waf web-protection-profile inline-protection

waf web-cache-policy

Use this command to configure FortiWeb to cache responses from your servers.

Use `web-cache-policy` to cache only a few URLs. To cache all URLs except for a few, see `config waf web-cache-exception`.

To apply this policy, include it in an inline protection profile. For details, see `config waf web-protection-profile inline-protection`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf web-cache-policy
   edit <web-cache-policy_rule_name>
      set cache-buffer-size <cache-size_int>
      set max-cached-page-size <page-size_int>
      set default-cache-timeout <cache-timeout_int>
      set exception <web-cache-exception_name>
      config url-match-list
         edit <entry_index>
            set host-status {enable | disable}
            set host <host_str>
            set url-type {plain | regular}
            set url-pattern <url-pattern_str>
      end
   next
end
```

Variable	Description	Default
<web-cache-policy_rule_name>	Type the name of a new or existing rule. The maximum length is 35 characters. To display the list of existing policies, type: `edit ?`	No default.

Variable	Description	Default
<cache-size_int>	Specify the maximum amount of RAM to allocate to caching content, in MB (megabytes). You cannot store cached content on FortiWeb's hard disk. The FortiWeb model determines the valid range of values: • FortiWeb 400C, FortiWeb-VM (2-4 GB RAM) — 1-100 MB • FortiWeb 1000C, FortiWeb-VM (4-8 GB RAM) — 1-200 MB • FortiWeb 3000C, FortiWeb 3000C/CFsx, FortiWeb-VM (8-16 GB RAM)— 1-400 MB • FortiWeb 4000C — 1-600 MB • FortiWeb 1000D — 1-800 MB • FortiWeb-VM (16+ GB RAM) — 1-1024 MB • FortiWeb 3000D/DFsx — 1-1200 MB • FortiWeb 4000D — 1-2048 MB If administrative domains (ADOMs) are enabled, the maximums apply to the total RAM allotted to all ADOMs. For example, a FortiWeb 1000D has two ADOMs. If the `cache-buffer-size` value for the first ADOM is `600`, the valid range for `cache-buffer-size` for the second ADOM is 1-200. **Tip:** 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.	`100`
<page-size_int>	Specify the maximum size of each URL that FortiWeb caches, in kilobytes (KB). FortiWeb does not cache objects such as high-resolution images, movies, or music that are larger than this value. Valid range is 1 to 10,240. **Tip:** For improved performance, adjust this setting until FortiWeb can fit most graphics and server processing-intensive pages into its cache.	`2048`

Variable	Description	Default
<cache-timeout_int>	Specify the time to live for each entry in the cache. FortiWeb removes expired entries. Valid range is 0 to 7200. When it receives a subsequent request for the URL, FortiWeb forwards the request to the server and refreshes the cached response. Any additional requests receive the new cached response until the URL's cache timeout expires.	1440
<web-cache-exception_name>	Specify the name of a list of exceptions. See config waf web-cache-exception.	No default.
<entry_index>	Type the index number of the individual entry in the table. The valid range is from 1 to 9,999,999,999,999,999,999.	No default.
host-status {enable | disable}	Specify enable to require that the Host: field of the HTTP request match a protected host names entry in order to match the policy. Also specify a value for host.	disable
<host_str>	Specify 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 policy. This option is available only if the value of host-status is enabled.	No default.
{plain | regular}	Specify the type of value that is used for url-pattern: plain — A literal URL. regular — A regular expression designed to match multiple URLs.	plain
<url-pattern_str>	If the value of url-type is plain, specify the literal URL, such as /index.php, that the HTTP request must contain in order to match the rule. The URL must begin with a slash (/). If the value of url-type is regular, specify a regular expression, such as ^/*.php, that matches all and only the URLs that the rule applies to. The pattern does not require a slash (/); however, it must match URLs that begin with a slash, such as /index.cfm. Do not include the domain name, such as www.example.com, which is specified by host.	No default.

Related topics

- config waf web-cache-exception
- config waf web-protection-profile inline-protection

waf web-protection-profile autolearning-profile

Use this command to configure auto-learning profiles.

Auto-learning profiles are useful when you want to collect information about the HTTP sessions on your unique network in order to design inline or offline protection profiles suited for them. This reduces much of the research and guesswork about what HTTP request methods, data types, and other types of content that your web sites and web applications use when designing an appropriate defense.

Auto-learning profiles track your web servers' response to each request, such as `401 Unauthorized` or `500 Internal Server Error`, to learn about whether the request is legitimate or a potential attack attempt. Such data is used for auto-learning reports, and can serve as the basis for generating inline protection or offline protection profiles.

Auto-learning profiles are designed to be used in conjunction with a protection or detection profile, which is used to detect attacks. Only if attacks are detected can the auto-learning profile accumulate auto-learning data and generate its report. As a result, auto-learning profiles require that you also select a protection or detection profile in the same policy.

Use auto-learning profiles with profiles whose `action` is `alert`.

If `action` is `alert_deny`, the FortiWeb appliance will reset the connection, preventing the auto-learning feature from gathering complete data on the session.

To apply auto-learning profiles, select them within a policy. For details, see `config waf web-protection-profile offline-protection`. Once applied in a policy, the FortiWeb appliance will collect data and generate a report from it. For details, see the *FortiWeb Administration Guide*.

Before configuring an auto-learning profile, first configure any of the following that you want to include in the profile:

- a data type group (see `config server-policy pattern data-type-group`)
- a suspicious URL rule group (see `config server-policy pattern suspicious-url-rule`)
- a URL interpreter (see `config server-policy custom-application application-policy`)

Alternatively, you could generate an auto-learning profile and its required components, and then modify them. For details, see the *FortiWeb Administration Guide*.

You must also disable any globally whitelisted objects. (These will be exempt from scans and autolearning data.) See `config server-policy pattern custom-global-white-list-group`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `learngrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf web-protection-profile autolearning-profile
   edit <auto-learning-profile_name>
      set data-type-group <data-type-group_name>
      set suspicious-url-rule <suspicious-url-rule-group_name>
      set attack-count-threshold <count_int>
      set attack-percent-range <percent_int>
      set analyzer-policy <fortianalyzer-policy_name>
   next
end
```

Variable	Description	Default
`<auto-learning-profile_name>`	Type the name of the auto-learning profile. The maximum length is 35 characters. To display the list of existing profile, type: `edit ?`	No default.
`data-type-group <data-type-group_name>`	Type the name of the data type group for the profile to use. See `config server-policy pattern data-type-group`. The maximum length is 35 characters. To display the list of existing groups, type: `set data-type-group ?` The auto-learning profile will learn about the names, length, and required presence of these types of parameter inputs as described in the data type group.	No default.
`suspicious-url-rule <suspicious-url-rule-group_name>`	Type the name of a suspicious URL rule group to use. See `config server-policy pattern suspicious-url-rule`. The maximum length is 35 characters. To display the list of existing groups, type: `set suspicious-url-rule ?` The auto-learning profile will learn about attempts to access URLs that are typically used for web server or web application administrator logins, such as `admin.php`. Requests from clients for these types of URLs are considered to be a possible attempt at either vulnerability scanning or administrative login attacks, and therefore potentially malicious.	No default.

Variable	Description	Default
attack-count-threshold <count_int>	Type the integer representing the threshold over which the auto-learning profile adds the attack to the server protection rules. The valid range is from 1 to 2,147,483,647.	100
attack-percent-range <percent_int>	Type the integer representing the threshold of the percentage of attacks to total hits over which the auto-learning profile adds the attack to the server protection exceptions. The valid range is from 1 to 10,000.	5
application-policy <policy_name>	Type the name of a custom application policy to use. See config server-policy custom-application application-policy. The maximum length is 35 characters. To display the list of existing application policies, type: set application-policy ?	No default.

Related topics

- config server-policy pattern custom-global-white-list-group
- config server-policy pattern data-type-group
- config server-policy pattern suspicious-url-rule
- config waf web-protection-profile inline-protection
- config server-policy policy
- config system settings

waf web-protection-profile inline-protection

Use this command to configure inline protection profiles.

Inline protection profiles are a set of attack protection settings. The FortiWeb appliance applies the profile when a connection matches a server policy that includes the protection profile. You can use inline protection profiles in server policies for any mode except offline protection.

To apply protection profiles, select them within a server policy. For details, see config server-policy policy.

Before configuring an inline protection profile, first configure any of the following that you want to include in the profile:

- a parameter validation rule (see config waf parameter-validation-rule)
- start pages (see config waf start-pages)
- caching of back-end server responses (see config waf web-cache-policy)
- a URL access policy (see config waf url-access url-access-policy
- a hidden field rule group (see config waf hidden-fields-protection)

- a parameter restriction constraint (see `config waf http-protocol-parameter-restriction`)
- an authentication policy and/or site publisher (see `config waf http-authen http-authen-policy` or `config waf site-publish-helper policy`)
- a brute force login attack sensor (see `config waf brute-force-login`)
- an allowed method exception (see `config waf allow-method-exceptions`)
- a list of manually trusted and black-listed IPs, FortiGuard IP reputation category-based blacklisted IPs, and/or a geographically-based IP blacklist (see `config waf ip-intelligence`, `config server-policy custom-application application-policy` and `config waf geo-block-list`)
- a page order rule (see `config waf page-access-rule`)
- attack signatures (see `config waf signature`)
- a file upload restriction policy (see `config server-policy custom-application application-policy`)
- a URL rewriting policy (see `config waf url-rewrite url-rewrite-policy`
- a DoS protection policy (see `config waf application-layer-dos-prevention`)
- compression rules (see `config waf file-compress-rule`)
- decompression rules (`config waf file-uncompress-rule`)
- a policy that protects vulnerable block cipher implementations for web applications that selectively encrypt inputs without using HTTPS (`config waf padding-oracle`)
- a FortiGate that provides a list of quarantined source IPs (`config system fortigate-integration`)
- a cross-site request forgery (CSRF) protection rule (see `config waf csrf-protection`)
- a cookie security policy (see config waf cookie-security)
- a user tracking policy (see `config waf user-tracking policy`)

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf web-protection-profile inline-protection
   edit <inline-protection-profile_name>
      set http-session-management {enable | disable}
      set http-session-timeout <seconds_int>
      set x-forwarded-for-rule <x-forwarded-for_name>
      set signature-rule {"High Level Security" | "Medium Level Security" |
          "Alert Only" | <signature-set_name>}
      set amf3-protocol-detection {enable | disable}
      set xml-protocol-detection {enable | disable}
      set malformed-xml-check {enable | disable}
      set malformed-xml-check-action {alert | alert_deny | block-period}
      set malformed-xml-block-period <block-period_int>
      set malformed-xml-check-severity {High | Low | Medium}
      set malformed-xml-check-trigger <trigger-policy_name>
      set json-protocol-detection {enable | disable}
      set malformed-json-check {enable | disable}
      set malformed-json-check-action {alert | alert_deny | block-period}
      set malformed-json-block-period <block-period_int>
      set malformed-json-check-severity {High | Medium | Low}
      set malformed-json-check-trigger <trigger-policy_name>
      set custom-access-policy <combo-access_name>
      set padding-oracle <rule_name>
      set csrf-protection <rule_name>
```

```
        set cookie-security-policy <cookie-security_name>
        set parameter-validation-rule <rule_name>
        set hidden-fields-protection <group_name>
        set file-upload-policy <policy_name>
        set http-protocol-parameter-restriction <constraint_name>
        set brute-force-login <sensor_name>
        set url-access-policy <policy_name>
        set page-access-rule <rule_name>
        set start-pages <rule_name>
        set allow-method-policy <policy_name>
        set ip-list-policy <policy_name>
        set geo-block-list-policy <policy_name>
        set application-layer-dos-prevention <policy_name>
        set ip-intelligence {enable | disable}
        set fortigate-quarantined-ips {enable | disable}
        set quarantined-ip-action {alert | alert_deny}
        set quarantined-ip-severity {High | Medium | Low}
        set quarantined-ip-trigger <trigger-policy_name>
        set known-search-engine {enable | disable}
        set url-rewrite-policy <group_name>
        set http-authen-policy <policy_name>
        set site-publisher-helper <policy_name>
        set file-compress-rule <rule_name>
        set file-uncompress-rule <rule_name>
        set web-cache-policy <web-cache-policy_name>
        set user-tracking-policy <user-tracking-policy_name>
        set redirect-url <redirect_fqdn>
        set rdt-reason {enable | disable}
        set data-analysis {enable | disable}
        set comment "<comment_str>"
    next
end
```

Variable	Description	Default
<inline-protection-profile_name>	Type the name of the inline protection profile. The maximum length is 35 characters. To display the list of existing profile, type: edit ?	No default.

Variable	Description	Default
`http-session-management {enable | disable}`	Enable to add an implementation of HTTP sessions, and track their states, using a cookie such as `cookiesession1`. Also configure `http-session-timeout <seconds_int>`. Although HTTP has no inherent support for sessions, a notion of individual HTTP client sessions, rather than simply the source IP address and/or timestamp, is required by some features. For example, you might want to require that a client's first HTTP request always be a login page: the rest of the web pages should be inaccessible if they have not authenticated. Out-of-order requests could represent an attempt to bypass the web application's native 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 could not, by definition, enforce page order. Therefore FortiWeb must keep some record of the first request from that client (the session initiation). It also must record their previous HTTP request(s), until a span of time (the session timeout) has elapsed during which there were no more subsequent requests, after which it would require that the session be initiated again. The session management feature provides such FortiWeb session support. This feature requires that the client support cookies. **Note:** You **must** enable this option: • to enforce the start page rule, page access rule, and hidden fields rule, if any of those are selected. • if you want to include this profile's traffic in the traffic log, in addition to enabling traffic logs in general. For more information, see `config log attack-log` and .	`disable`
`http-session-timeout <seconds_int>`	Type the HTTP session timeout in seconds. The valid range is from 20 to 3,600 seconds. This setting is available only if `http-session-management` is enabled.	`1200`
`x-forwarded-for-rule <x-forwarded-for_name>`	Specify the name of a rule that configures FortiWeb's use of X-Forwarded-For: and X-Real-IP (see `config waf x-forwarded-for`).	No default.

Variable	Description	Default
`signature-rule {"High Level Security" | "Medium Level Security" | "Alert Only" | <signature-set_name>}`	Specify a signature policy to include in the profile (see `config waf signature`). The maximum length is 35 characters. To display the list of existing rules, type: `set server-protection-rule ?` The type of attack that FortiWeb detects determines the attack log messages for this feature. For a list, see `config waf signature`.	No default.
`amf3-protocol-detection {enable | disable}`	Enable to scan requests that use action message format 3.0 (AMF3) for • cross-site scripting (XSS) attacks • SQL injection attacks • common exploits if you have enabled those in the signature set specified by signature-rule {"High Level Security" | "Medium Level Security" | "Alert Only" | <signature-set_name>}. AMF3 is a binary format that Adobe Flash clients can use to send input to server-side software. **Caution:** To scan for attacks or enforce input rules on AMF3, you **must** enable this option. Failure to enable the option will make the FortiWeb appliance unable to scan AMF3 requests for attacks.	`disable`
`xml-protocol-detection {enable | disable}`	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 `POST` requests.	`disable`
`malformed-xml-check {enable | disable}`	Enable to validate that XML elements and attributes in the request's body conforms to the W3C XML 1.1 and/or XML 2.0 standards.Malformed XML, such as without the final > or with multiple >> in the closing tag, is often an attempt to exploit an unhandled error condition in a web application's XHTML or XML parser. This feature is applicable only when `xml-protocol-detection` is `enable`. Attack log messages contain `Illegal XML Format` when this feature detects malformed XML.	`disable`

Variable	Description	Default
`malformed-xml-check-action {alert | alert_deny | block-period}`	Specify the action that FortiWeb takes when it detects a request that contains malformed XML: • `alert` — Accept the request and generate an alert email, a log message, or both. • `alert_deny` — Block the request and generate an alert email, a log message, or both. • `block-period` — Block the XML traffic for a number of seconds. Also configure `malformed-xml-block-period <block-period_int>`.	alert
`malformed-xml-block-period <block-period_int>`	Type the length of time that FortiWeb blocks XML traffic that contains malformed XML, in seconds. The valid range is from 1 to 3,600 seconds.	`60`
`malformed-xml-check-severity {High | Low | Medium}`	Select the severity level to use in logs and reports generated when illegal XML formats are detected.	High
`malformed-xml-check-trigger <trigger-policy_name>`	Type the name of the trigger to apply when illegal XML formats are detected (see `config log trigger-policy`). The maximum length is 35 characters. To display the list of existing trigger policies, type: `set trigger ?`	No default.
`json-protocol-detection {enable | disable}`	Enter `enable` to scan for matches with attack and data leak signatures in JSON data submitted by clients in HTTP requests with `Content-Type:` values `application/json` or `text/json`.	`disable`
`malformed-json-check {enable | disable}`	Enter `enable` to scan for illegal formatting in JSON data.	`disable`
`malformed-json-check-action {alert | alert_deny | block-period}`	Specify the action that FortiWeb takes when it detects a request that contains malformed JSON content: • `alert` — Accept the request and generate an alert email, a log message, or both. • `alert_deny` — Block the request and generate an alert email, a log message, or both. • `block-period` — Block the JSON traffic for a number of seconds. Also configure `malformed-json-block-period`.	No default.

Variable	Description	Default
`malformed-json-block-period <block-period_int>`	Type the length of time that FortiWeb blocks traffic that contains malformed JSON content, in seconds. The valid range is from 1 to 3,600 seconds.	`60`
`malformed-json-check-severity {High | Medium | Low}`	Select the severity level to use in logs and reports that FortiWeb generates when it detects malformed JSON content.	`High`
`malformed-json-check-trigger <trigger-policy_name>`	Type the name of the trigger to apply when FortiWeb detects malformed JSON content. The maximum length is 35 characters. To display the list of existing trigger policies, type: `set trigger ?`	No default.
`custom-access-policy <combo-access_name>`	Type the name of a custom access policy. See `config waf custom-access policy`. The maximum length is 35 characters. To display the list of existing policies, type: `set custom-access-policy ?`	No default.
`padding-oracle <rule_name>`	Type the name of a padding oracle protection rule. See `config waf padding-oracle`. The maximum length is 35 characters. To display the list of existing rule, type: `set padding-oracle ?`	No default.
`csrf-protection <rule_name>`	Select the name of cross-site request forgery protection rule, if any, to apply to matching requests. See `config waf csrf-protection`. Available only when `http-session-management` is `enabled`.	No default.
cookie-security-policy <cookie-security_name>		
`parameter-validation-rule <rule_name>`	Type the name of a parameter validation rule. See `config waf parameter-validation-rule`. The maximum length is 35 characters. To display the list of existing rules, type: `set parameter-validation-rule ?`	No default.

Variable	Description	Default
`hidden-fields-protection <group_name>`	Type the name of a hidden field rule group that you want to apply, if any. See `config waf hidden-fields-protection`. The maximum length is 35 characters. To display the list of existing group, type: `set hidden-fields-protection ?`	No default.
`file-upload-policy <policy_name>`	Type the name of a file upload restriction policy to use, if any. See `config server-policy custom-application application-policy`. The maximum length is 35 characters. To display the list of existing policies, type: `set file-upload-policy ?`	No default.
`http-protocol-parameter-restriction <constraint_name>`	Type the name of an HTTP protocol constraint that you want to apply, if any. See `config waf http-protocol-parameter-restriction`. The maximum length is 35 characters. To display the list of existing profile, type: `set http-protocol-parameter-restriction ?`	No default.
`brute-force-login <sensor_name>`	Type the name of a brute force login attack sensor. See `config waf brute-force-login`. The maximum length is 35 characters. To display the list of existing sensors, type: `set brute-force-login ?`	No default.
`url-access-policy <policy_name>`	Type the name of a url access policy. See `config waf url-access url-access-policy`. The maximum length is 35 characters. To display the list of existing policy, type: `set url-access-policy ?`	No default.
`page-access-rule <rule_name>`	Type the name of a page order rule. See `config waf page-access-rule`. The maximum length is 35 characters. To display the list of existing rule, type: `set page-access-rule ?`	No default.

Variable	Description	Default
`start-pages <rule_name>`	Type the name of a start page rule. See `config waf start-pages`. The maximum length is 35 characters. To display the list of existing rule, type: `set start-pages ?` This setting is available only if `http-session-management` is enabled.	No default.
`allow-method-policy <policy_name>`	Type the name of an allowed method policy. See `config server-policy custom-application application-policy`. The maximum length is 35 characters. To display the list of existing policies, type: `set allow-method-policy ?`	No default.
`ip-list-policy <policy_name>`	Type the name of a trusted IP or blacklisted IP policy. See `config server-policy custom-application application-policy`. The maximum length is 35 characters. To display the list of existing policy, type: `set ip-list-policy ?`	No default.
`geo-block-list-policy <policy_name>`	Type the name of a geographically-based client IP black list that you want to apply, if any. See `config waf geo-block-list`. The maximum length is 35 characters. To display the list of existing group, type: `set geo-block-list-policy ?`	No default.
`application-layer-dos-prevention <policy_name>`	Type the name of an existing DoS protection policy to use with this profile, if any. See `config waf application-layer-dos-prevention`. The maximum length is 35 characters. To display the list of existing profile, type: `set application-layer-dos-prevention ?`	No default.
`ip-intelligence {enable | disable}`	Enable to apply intelligence about the reputation of the client's source IP. Blocking and logging behavior is configured in `config waf ip-intelligence`.	`disable`

Variable	Description	Default
`fortigate-quarantined-ips {enable | disable}`	Enable to detect source IP addresses that a FortiGate unit is currently preventing from interacting with the network and protected systems. To configure communication between the FortiGate and FortiWeb, see `config system fortigate-integration`.	`disable`
`quarantined-ip-action {alert | alert_deny}`	Specify the action that FortiWeb takes if it detects a quarantined IP address: • `alert` — Accept the request and generate an alert email, log message, or both. • `alert_deny` — Block the request and generate an alert, log message, or both.	`alert`
`quarantined-ip-severity {High | Medium | Low}`	Specify the severity that FortiWeb assigns to quarantined IP log messages.	`High`
`quarantined-ip-trigger <trigger-policy_name>`	Type the name of the trigger to apply when FortiWeb detects a quarantined IP (see `config log trigger-policy`). To display the list of existing trigger policies, type: `set trigger ?`	No default.

Variable	Description	Default
known-search-engine {enable | disable}	Enable to allow or block predefined search engines, robots, spiders, and web crawlers according to your settings in the global list. Enable to exempt popular search engines' robots, spiders, and web crawlers from DoS sensors, brute force login sensors, HTTP protocol constraints, and combination rate & access control (called "advanced protection" and "custom policies" in the web UI). 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. 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 will be exempt, enable or disable each search engine in `config server-policy pattern custom-global-white-list-group`. **Note:** X-header-derived client source IPs (see `config waf x-forwarded-for`) 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.	disable
url-rewrite-policy <group_name>	Type the name of a URL rewriting rule set, if any, that will be applied to matching HTTP requests. The maximum length is 35 characters. To display the list of existing policy, type: `set url-rewrite-policy ?` See `config waf url-access url-access-policy`.	No default.
http-authen-policy <policy_name>	Type the name of an HTTP authentication policy, if any, that will be applied to matching HTTP requests. See `config waf http-authen http-authen-policy`. The maximum length is 35 characters. To display the list of existing profile, type: `set http-authen-policy ?` If the HTTP client fails to authenticate, it will receive an HTTP 403 (Access Forbidden) error message.	No default.

Variable	Description	Default
`site-publisher-helper <policy_name>`	Type the name of a site publishing policy, if any, that will be applied to matching HTTP requests. See `config waf site-publish-helper policy`. The maximum length is 35 characters. To display the list of existing profile, type: `set site-publisher-policy ?` If the HTTP client fails to authenticate, it will receive an HTTP 403 (Access Forbidden) error message.	No default.
`file-compress-rule <rule_name>`	Type the name of an existing file compression rule to use with this profile, if any. See `config waf file-compress-rule`. The maximum length is 35 characters. To display the list of existing rule, type: `set file-compress-rule ?`	No default.
`file-uncompress-rule <rule_name>`	Type the name of an existing file uncompression rule to use with this profile, if any. See `config waf file-uncompress-rule`. The maximum length is 35 characters. To display the list of existing rule, type: `set file-uncompress-rule ?`	No default.
`web-cache-policy <web-cache-policy_name>`	Type the name of content caching policy. See `config waf web-cache-policy`. The maximum length is 35 characters. To display the list of existing policies, type: `set web-cache-policy ?`	No default.
`user-tracking-policy <user-tracking-policy_name>`	Enter the name of a user tracking policy. See `config waf user-tracking policy`.	No default.

Variable	Description	Default
redirect-url <redirect_fqdn>	Type a URL including the FQDN/IP and path, if any, to which an HTTP client will be redirected if their HTTP request violates any of the rules in this profile. For example, you could enter `www.example.com/products/`. If you do **not** enter a URL, depending on the type of violation and the configuration, the FortiWeb 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. The maximum length is 255 characters.	No default.
rdt-reason {enable | disable}	Enable to include the reason for URL redirection as a parameter in the URL, such as `reason=DETECT_PARAM_RULE_FAILED`, when traffic has been redirected using redirect-url <redirect_fqdn>. The FortiWeb appliance also adds `fortiwaf=1` to the URL to detect and cancel a redirect loop (when the redirect action recursively triggers an attack event). **Caution**: If you specify a redirect URL that is protected by the FortiWeb appliance, you should enable this option to prevent infinite redirect loops.	No default.
data-analysis {enable | disable}	Enable this to collect data for servers covered by this profile. To view the statistics for collected data, in the web UI, go to **Log&Report > Monitor > Data Analytics**.	disable
comment "<comment_str>"	Type a description or other comment. If the comment contains more than one word or contains an apostrophe, surround the comment in double quotes ("). The maximum length is 199 characters.	No default.

Related topics

- config log trigger-policy
- config server-policy pattern custom-global-white-list-group
- config server-policy policy
- config waf signature
- config waf start-pages
- config waf padding-oracle
- config waf page-access-rule
- config waf parameter-validation-rule
- config waf http-protocol-parameter-restriction

- config waf url-access url-access-policy
- config waf allow-method-exceptions
- config waf application-layer-dos-prevention
- config waf file-compress-rule
- config waf file-uncompress-rule
- config waf brute-force-login
- config waf geo-block-list
- config waf hidden-fields-protection
- config waf http-authen http-authen-policy
- config waf http-protocol-parameter-restriction
- config waf ip-intelligence
- config server-policy custom-application application-policy
- config waf web-cache-exception
- config waf web-cache-policy

waf web-protection-profile offline-protection

Use this command to configure offline protection profiles.

Detection profiles are useful when you want to preview the effects of some web protection features without affecting traffic, or without affecting your network topology.

Unlike protection profiles, a detection profile is designed for use in offline protection mode. Detection profiles cannot be guaranteed to block attacks. They attempt to reset the connection, but due to variable speeds of different routing paths, the reset request may arrive after the attack has been completed. Their primary purpose is to detect attacks, especially for use in conjunction with auto-learning profiles. In fact, if used in conjunction with auto-learning profiles, you **should** configure the detection profile to log only and not block attacks in order to gather complete session statistics for the auto-learning feature. As a result, detection profiles can only be selected in policies whose `deployment-mode` is `offline-detection`, and those policies will only be used by the FortiWeb appliance when its operation mode is `offline-detection`.

Unlike inline protection profiles, offline protection profiles do not support HTTP conversion, cookie poisoning detection, start page rules, and page access rules.

To apply detection profiles, select them within a server policy. For details, see `config server-policy policy`.

Before configuring an offline protection profile, first configure any of the following that you want to include in the profile:

- a file upload restriction policy (see `config server-policy custom-application application-policy`)
- a server protection rule (see `config waf signature`)
- a list of manually trusted and black-listed IPs, FortiGuard IRIS category-based blacklisted IPs, and/or a geographically-based IP blacklist (see `config waf ip-intelligence`, `config server-policy custom-application application-policy` and `config waf geo-block-list`)
- a parameter validation rule (see `config waf parameter-validation-rule`)
- a URL access policy (see `config waf url-access url-access-policy`

- an allowed method exception (see `config waf allow-method-exceptions`)
- a hidden field rule group (see `config waf hidden-fields-protection`)
- a parameter restriction constraint (see `config waf http-protocol-parameter-restriction`)
- a brute force login attack sensor (see `config waf brute-force-login`)
- a decompression rule (see `config waf file-uncompress-rule`)
- a policy that protects vulnerable block cipher implementations for web applications that selectively encrypt inputs without using HTTPS (`config waf padding-oracle`)
- a user tracking policy (see `config waf user-tracking policy`)

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf web-protection-profile offline-protection
   edit <offline-protection-profile_name>
      set http-session-management {enable | disable}
      set http-session-timeout <seconds_int>
      set x-forwarded-for-rule <x-forwarded-for_name>
      set http-session-keyword <key_str>
      set signature-rule {"High Level Security" | "Medium Level Security" |
          "Alert Only" | <signature-set_name>}
      set amf3-protocol-detection {enable | disable}
      set xml-protocol-detection {enable | disable}
      set malformed-xml-check {enable | disable}
      set malformed-xml-check-action {alert | alert_deny | block-period}
      set malformed-xml-block-period <block-period_int>
      set malformed-xml-check-severity {High | Low | Medium}
      set malformed-xml-check-trigger <trigger-policy_name>
      set json-protocol-detection {enable | disable}
      set malformed-json-check {enable | disable}
      set malformed-json-check-action {alert | alert_deny | block-period}
      set malformed-json-block-period <block-period_int>
      set malformed-json-check-severity {High | Medium | Low}
      set malformed-json-check-trigger <trigger-policy_name>
      set custom-access-policy <combo-access_name>
      set padding-oracle <rule_name>
      set parameter-validation-rule <rule_name>
      set hidden-fields-protection <group_name>
      set file-upload-policy <policy_name>
      set http-protocol-parameter-restriction <constraint_name>
      set url-access-policy <policy_name>
      set allow-method-policy <policy_name>
      set brute-force-login <sensor_name>
      set ip-list-policy <policy_name>
      set geo-block-list-policy <policy_name>
      set ip-intelligence {enable | disable}
      set known-search-engine {enable | disable}
      set file-uncompress-rule <rule_name>
      set user-tracking-policy <user-tracking-policy_name>
      set data-analysis {enable | disable}
      set comment "<comment_str>"
   next
end
```

Variable	Description	Default
<offline-protection-profile_name>	Type the name of the offline protection profile. The maximum length is 35 characters. To display the list of existing profile, type: edit ?	No default.
http-session-management {enable | disable}	Enable to track the states of HTTP sessions. Also configure http-session-timeout <seconds_int>. Although HTTP has no inherent support for sessions, a notion of individual HTTP client sessions, rather than simply the source IP address and/or timestamp, is required by some features. For example, you might want to require that a client's first HTTP request always be a login page: the rest of the web pages should be inaccessible if they have not authenticated. Out-of-order requests could represent an attempt to bypass the web application's native 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 could not, by definition, enforce page order. Therefore FortiWeb must keep some record of the first request from that client (the session initiation). It also must record their previous HTTP request(s), until a span of time (the session timeout) has elapsed during which there were no more subsequent requests, after which it would require that the session be initiated again. The session management feature provides such FortiWeb session support. **Note:** This feature requires that the client support cookies. **Note:** You **must** enable this option if you want to include this profile's traffic in the traffic log, in addition to enabling traffic logs in general. For more information, see config log attack-log and .	disable
http-session-timeout <seconds_int>	Type the HTTP session timeout in seconds. The valid range is from 20 to 3,600 seconds. This setting is available only if http-session-management is enabled.	1200

Variable	Description	Default
`x-forwarded-for-rule <x-forwarded-for_name>`	Specify the name of a rule that configures FortiWeb's use of X-Forwarded-For: and X-Real-IP (see `config waf x-forwarded-for`).	No default.
`http-session-keyword <key_str>`	If you want to use an HTTP header other than `Session-Id:` to track separate HTTP sessions, enter the key portion of the HTTP header that you want to use, such as `Session-Num`. The maximum length is 35 characters.	No default.
`signature-rule {"High Level Security" | "Medium Level Security" | "Alert Only" | <signature-set_name>}`	Specify a signature policy to include in the profile (see `config waf signature`). The maximum length is 35 characters. To display the list of existing rules, type: `set server-protection-rule ?` The type of attack that FortiWeb detects determines the attack log messages for this feature. For a list, see `config waf signature`.	No default.
`amf3-protocol-detection {enable | disable}`	Enable to be able to scan requests that use action message format 3.0 (AMF3) for • cross-site scripting (XSS) attacks • SQL injection attacks • common exploits if you have enabled those in the set of signatures specified by signature-rule {"High Level Security" | "Medium Level Security" | "Alert Only" | <signature-set_name>}. AMF3 is a binary format that can be used by Adobe Flash clients to send input to server-side software. **Caution:** To scan for attacks or enforce input rules on AMF3, you **must** enable this option. Failure to enable the option makes the FortiWeb appliance unable to scan AMF3 requests for attacks.	`disable`
`xml-protocol-detection {enable | disable}`	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 `POST` requests.	`disable`

Variable	Description	Default
`malformed-xml-check {enable | disable}`	Enable to validate that XML elements and attributes in the request's body conforms to the W3C XML 1.1 and/or XML 2.0 standards.Malformed XML, such as without the final > or with multiple >> in the closing tag, is often an attempt to exploit an unhandled error condition in a web application's XHTML or XML parser. This feature is applicable only when `xml-protocol-detection` is `enable`. Attack log messages contain `Illegal XML Format` when this feature detects malformed XML.	`disable`
`malformed-xml-check-action {alert | alert_deny | block-period}`	Specify the action that FortiWeb takes when it detects a request that contains malformed XML: • `alert` — Accept the request and generate an alert email, a log message, or both. • `alert_deny` — Block the request and generate an alert email, a log message, or both. • `block-period` — Block the XML traffic for a number of seconds. Also configure malformed-xml-block-period <block-period_int>.	alert
`malformed-xml-block-period <block-period_int>`	Type the length of time that FortiWeb blocks XML traffic that contains malformed XML, in seconds. The valid range is from 1 to 3,600 seconds.	60
`malformed-xml-check-severity {High | Low | Medium}`	Select the severity level to use in logs and reports generated when illegal XML formats are detected.	High
`malformed-xml-check-trigger <trigger-policy_name>`	Type the name of the trigger to apply when illegal XML formats are detected (see `config log trigger-policy`). The maximum length is 35 characters. To display the list of existing trigger policies, type: `set trigger ?`	No default.
`json-protocol-detection {enable | disable}`	Enter `enable` to scan for matches with attack and data leak signatures in JSON data submitted by clients in HTTP requests with `Content-Type:` values `application/json` or `text/json`.	`disable`
`malformed-json-check {enable | disable}`	Enter `enable` to scan for illegal formatting in JSON data.	`disable`

Variable	Description	Default
`malformed-json-check-action {alert | alert_deny | block-period}`	Specify the action that FortiWeb takes when it detects a request that contains malformed JSON content: • `alert` — Accept the request and generate an alert email, a log message, or both. • `alert_deny` — Block the request and generate an alert email, a log message, or both. • `block-period` — Block the JSON traffic for a number of seconds. Also configure `malformed-json-block-period`.	No default.
`malformed-json-block-period <block-period_int>`	Type the length of time that FortiWeb blocks traffic that contains malformed JSON content, in seconds. The valid range is from 1 to 3,600 seconds.	`60`
`malformed-json-check-severity {High | Medium | Low}`	Select the severity level to use in logs and reports that FortiWeb generates when it detects malformed JSON content.	`High`
`malformed-json-check-trigger <trigger-policy_name>`	Type the name of the trigger to apply when FortiWeb detects malformed JSON content. The maximum length is 35 characters. To display the list of existing trigger policies, type: `set trigger ?`	No default.
`custom-access-policy <combo-access_name>`	Type the name of a custom access policy. See `config waf custom-access policy`. The maximum length is 35 characters. To display the list of existing policies, type: `set custom-access-policy ?`	No default.
`padding-oracle <rule_name>`	Type the name of a padding oracle protection rule. See `config waf padding-oracle`. The maximum length is 35 characters. To display the list of existing rule, type: `set padding-oracle ?`	No default.
`parameter-validation-rule <rule_name>`	Type the name of a parameter validation rule. See `config waf parameter-validation-rule`. The maximum length is 35 characters. To display the list of existing rule, type: `set parameter-validation-rule ?`	No default.

Variable	Description	Default
`hidden-fields-protection <group_name>`	Type the name of a hidden field rule group that you want to apply, if any. See `config waf hidden-fields-protection`. The maximum length is 35 characters. To display the list of existing group, type: `set hidden-fields-protection ?`	No default.
`file-upload-policy <policy_name>`	Type the name of a file upload restriction policy. See `config server-policy custom-application application-policy`. The maximum length is 35 characters. To display the list of existing policy, type: `set file-upload-policy ?`	No default.
`http-protocol-parameter-restriction <constraint_name>`	Type the name of an HTTP protocol constraint that you want to apply, if any. See `config waf http-protocol-parameter-restriction`. The maximum length is 35 characters. To display the list of existing constraint, type: `set http-protocol-parameter-restriction ?`	No default.
`url-access-policy <policy_name>`	Type the name of a URL access policy. See `config waf url-access url-access-policy`. The maximum length is 35 characters. To display the list of existing policy, type: `set url-access-policy ?`	No default.
`allow-method-policy <policy_name>`	Type the name of an allowed method policy. See `config server-policy custom-application application-policy`. The maximum length is 35 characters. To display the list of existing policies, type: `set allow-method-policy ?`	No default.
`brute-force-login <sensor_name>`	Type the name of a brute force login attack sensor. See `config waf brute-force-login`. The maximum length is 35 characters. To display the list of existing sensor, type: `edit ?`	No default.

Variable	Description	Default
`ip-list-policy <policy_name>`	Type the name of a trusted IP or blacklisted IP policy. See `config server-policy custom-application application-policy`. The maximum length is 35 characters. To display the list of existing policy, type: `set ip-list-policy ?`	No default.
`geo-block-list-policy <policy_name>`	Type the name of a geographically-based client IP black list that you want to apply, if any. See `config waf geo-block-list`. The maximum length is 35 characters. To display the list of existing group, type: `set geo-block-list-policy ?`	No default.
`ip-intelligence {enable | disable}`	Enable to apply intelligence about the reputation of the client's source IP. Blocking and logging behavior is configured in `config waf ip-intelligence`.	`disable`
`known-search-engine {enable | disable}`	Enable to allow or block predefined search engines, robots, spiders, and web crawlers according to your settings in the global list.	`disable`
`file-uncompress-rule <rule_name>`	Type the name of an existing file decompression rule to use with this profile, if any. See `config waf file-uncompress-rule`. The maximum length is 35 characters. To display the list of existing rule, type: `set file-uncompress-rule ?`	No default.
`user-tracking-policy <user-tracking-policy_name>`	Enter the name of a user tracking policy. See `config waf user-tracking policy`.	No default.
`data-analysis {enable | disable}`	Enable this to collect data for servers covered by this profile. To view the statistics for collected data, in the web UI, go to **Log&Report > Monitor > Data Analytics**.	`disable`
`comment "<comment_str>"`	Type a description or other comment. If the comment contains more than one word or contains an apostrophe, surround the comment in double quotes ("). The maximum length is 199 characters.	No default.

Related topics

- config server-policy policy
- config waf signature
- config waf padding-oracle
- config waf parameter-validation-rule
- config waf url-access url-access-rule
- config waf allow-method-exceptions
- config system settings
- config waf file-uncompress-rule
- config waf brute-force-login
- config waf geo-block-list
- config waf hidden-fields-protection
- config waf http-protocol-parameter-restriction
- config waf ip-intelligence
- config server-policy custom-application application-policy

waf x-forwarded-for

Use this command to configure FortiWeb's use of `X-Forwarded-For:` and `X-Real-IP:`.

For behavior of this feature and requirements, see the *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For more information, see Permissions on page 74.

Syntax

```
config waf x-forwarded-for
   edit <x-forwarded-for_name>
      set block-based-on-original-ip {enable | disable}
      set ip-location {left | right}
      set original-ip-header <http-header-key_str>
      set tracing-original-ip {enable | disable}
      set x-forwarded-proto {enable | disable}
      set x-forwarded-for-support {enable | disable}
      set x-real-ip {enable | disable}
      config ip-list
         edit <entry_index>
            set ip <load-balancer_ip>
         next
      end
   next
end
```

Variable	Description	Default
`<x-forwarded-for_name>`	Type the name of the new or existing group. The maximum length is 63 characters. To display the list of existing groups, type: `edit ?`	No default.
`block-based-on-original-ip {enable | disable}`	Enable to be able to block requests that violate your policies by using the original client's IP derived from this HTTP X-header. When disabled, only attack logs and reports will use the original client's IP.	`disable`
`ip-location {left | right}`	Select whether to extract the original client's IP from either the left or right end of the HTTP X-header line. 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.	`left`
`original-ip-header <http-header-key_str>`	Type the key such as `X-Forwarded-For` `X-Real-IP`, **without** the colon (:), of the X-header that contains the original source IP address of the client. Also configure tracing-original-ip {enable | disable} and, for security reasons, ip <load-balancer_ip>. Maximum length is 255 characters.	No default.
`tracing-original-ip {enable | disable}`	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, **instead of** the `SRC` field in the IP layer. Also configure original-ip-header <http-header-key_str> and, for security reasons, ip <load-balancer_ip>. 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:`. For deployment guidelines and mechanism details, see the *FortiWeb Administration Guide*. **Caution:** 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.	`disable`

Variable	Description	Default
`x-forwarded-proto {enable | disable}`	Enable to add an `X-Forwarded-Proto:` header that indicates the protocol used in the client's original request. Requires reverse proxy mode or true transparent proxy.	`disable`
`x-forwarded-for-support {enable | disable}`	Enable to include the `X-Forwarded-For:` 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. • **Header absent** — Add the header, using the source IP address of the connection. • **Header present** — Verify that the source IP address of the connection is present in this header's list of IP addresses. If it is not, append it. This option can be useful for web servers that log or analyze clients' IP addresses, and support the `X-Forwarded-For:` header. When this option is disabled, from the web server's perspective, all connections appear to be coming from the FortiWeb appliance, which performs network address translation (NAT). But when enabled, the web server can instead analyze this header to determine the source and path of the original client connection. This option applies only when FortiWeb is operating in reverse proxy mode or true transparent proxy.	`disable`
`x-real-ip {enable | disable}`	Enable to include the `X-Real-IP:` 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 x-forwarded-for-support {enable | disable}). Like `X-Forwarded-For:`, 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. This option applies only when FortiWeb is operating in reverse proxy mode or true transparent proxy.	`disable`

Variable	Description	Default
`x-forwarded-proto {enable | disable}`	Enable to add an HTTP header that indicates the service used in the client's original request. 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.	`disable`
`<entry_index>`	Type the index number of the individual entry in the table. The valid range is from 1 to 9,223,372,036,854,775,807. Each list can contain a maximum of 256 IP addresses.	No default.
`ip <load-balancer_ip>`	Type the IP address of a load balancer or proxy that is in front of the FortiWeb appliance (between the client and FortiWeb). To apply anti-spoofing measures and improve security, FortiWeb trusts the contents of the HTTP header that you specify in original-ip-header <http-header-key_str> **only** if the packet arrived from one of the IP addresses you specify here. It regards original-ip-header <http-header-key_str> from other IP addresses as potentially spoofed. For packets from other IP addresses, FortiWeb ignores the `X-Forwarded-For:` header and uses the source IP address in the IP header as the client source address. This IP address is displayed in the attack log message.	No default.

Example

The following example defines a X-Forwarded-For rule that adds `X-Forwarded-For: , X-Real-IP:`, and `X-Forwarded-Proto:` headers to traffic that FortiWeb forwards to a back-end server. It enables FortiWeb to use the HTTP X-Header to identify and block the original client's IP. To protect against XFF spoofing, it also specifies the trusted load-balancer 192.168.1.105 in the X-Forwarded-For IP list.

```
config waf x-forwarded-for
   edit "load-balancer1"
      set x-forwarded-for-support enable
      set tracing-original-ip enable
      set original-ip-header X-FORWARDED-FOR
      set x-real-ip enable
      set x-forwarded-proto enable
      config ip-list
         edit 1
            set ip 192.168.1.105
```

```
        next
      end
      set block-based-on-original-ip enable
    next
  end
```

wvs policy

Use this command to define a web vulnerability scan policy. The policy enables you to set the frequency of the vulnerability scan, schedule the scan, and choose a format for the scan report. The policy also enables you to select an email policy that determines who receives the scan report.

Before you can complete a web vulnerability scan policy, you must first configure a scan profile using the FortiWeb web UI and a scan schedule using either the web UI or the command `config wvs schedule`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wvsgrp` area. For more information, see Permissions on page 74.

Syntax

```
config wvs policy
  edit wvs policy
    set type {runonce | schedule}
    set schedule <wvs-schedule_name>
    set profile <wvs-profile_name>
    set email <email-policy_name>
    set report_format {html mht pdf rtf text}
    set runtime <count_int>
  next
end
```

Variable	Description	Default
`<wvs-policy_name>`	Type the name of a new or existing web vulnerability scan policy. The maximum length is 35 characters. To display the list of existing policies, type: `edit ?`	No default.
`type {runonce | schedule}`	Select either: • `runonce` — Run the scan immediately after you complete the policy. • `schedule` — Run the scan on a schedule. Also configure analyzer-policy <fortianalyzer-policy_name>.	`runonce`

Variable	Description	Default
`schedule <wvs-schedule_name>`	Type the name of an existing web vulnerability scan schedule. See `config wvs schedule`. The maximum length is 35 characters. To display the list of existing schedules, type: `set schedule ?` This setting is applicable only if `type` is `schedule`.	No default.
`profile <wvs-profile_name>`	Type the name of an existing web vulnerability scan profile.	No default.
`email <email-policy_name>`	Type the name of an existing email policy. See `config log email-policy`. When the scan completes, the FortiWeb appliance will send email in the specified format to the email addresses in the policy. The maximum length is 35 characters. To display the list of existing policy, type: `set email ?`	No default.
`report_format {html mht pdf rtf text}`	Select one or more file formats of the report to attach when emailing it.	`html`
`runtime <count_int>`	Not configurable. To reset the value to zero, enter: `set runtime 0`	No default.

Example

The following example defines a recurring vulnerability scan with email report output in RTF and text format.

```
config wvs policy
   edit "wvs-policy1"
      set type schedule
      set schedule "wvs-schedule1"
      set report_format rtf text
      set profile "wvs-profile1"
      set email "EmailPolicy1"
   next
end
```

Related topics

- `config wvs profile`
- `config wvs schedule`

wvs profile

Use this command to display the names of web vulnerability scan profiles.

This command can only be used to display the names of the profiles. It cannot configure the profiles. To create a web vulnerability scan profile, you must use the web UI.

A web vulnerability scan (WVS) profile defines the web server to scan, as well as the specific vulnerabilities to scan for. The WVS profiles are associated with WVS policies, which determine when to perform the scan and how to publish the results of the scan defined by the profile.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wvsgrp` area. For more information, see Permissions on page 74.

Syntax

```
config wvs profile
   get
   show
end
```

Example

This example displays the names of all configured web vulnerability scan profiles.

```
config wvs profile
get
```

Output:

```
== [ WVS-Profile1 ]
name: WVS-Profile1
== [ WVS-Profile2 ]
name: WVS-Profile2
```

Example

This example displays the names of all configured web vulnerability scan profiles, using configuration file syntax.

```
config wvs profile
show
```

Output:

```
config wvs profile
edit "WVS-Profile1"
next
edit "WVS-Profile2"
next
end
```

Related topics

- config wvs policy
- config wvs schedule

wvs schedule

Use this command to schedule a web vulnerability scan.

Vulnerability scanning can detect known vulnerabilities on your web servers and web applications, helping you to design protection profiles. Vulnerability scans start from an initial directory, then scan for vulnerabilities in web pages located in the same directory or subdirectory as the initial URL.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wvsgrp` area. For more information, see Permissions on page 74.

Syntax

```
config wvs schedule
   edit <schedule_name>
      set type {recurring | onetime}
      set date <time_str> <date_str>
      set time <time_str>
      set wday {Sunday Monday Tuesday Wednesday Thursday Friday Saturday}
   next
end
```

Variable	Description	Default
`<schedule_name>`	Type the name of new or existing WVS schedule. The maximum length is 35 characters. To display the list of existing schedule, type: `edit ?`	No default.
`type {recurring | onetime}`	Select either: • `onetime` — Run the scan only when an administrator manually initiates it. Also configure date <time_str> <date_str>. • `recurring` — Run the scan periodically, on a schedule. Also configure time <time_str> and wday {Sunday Monday Tuesday Wednesday Thursday Friday Saturday} .	`onetime`

Variable	Description	Default
`date <time_str> <date_str>`	For a one-time web vulnerability scan, enter the time and date for the scan to run. The time format is `hh:mm` and the date format is `yyyy/mm/dd`, where: • `hh` is the hour according to a 24-hour clock • `mm` is the minute • `yyyy` is the year • `mm` is the month • `dd` is the day Year range is 2001-2050. This only applies if `type` is `onetime`.	No default.
`time <time_str>`	Specify the time the vulnerability scan is to be performed. The time format is `hh:mm`, where: • `hh` is the hour according to a 24-hour clock • `mm` is the minute This only applies if `type` is `recurring`.	No default.
`wday {Sunday Monday Tuesday Wednesday Thursday Friday Saturday}`	For a recurring scan only, enter one or more days of the week the scan is to be performed. This setting only applies if `type` is `recurring`.	No default.

Example

The following example schedules a recurring vulnerability scan to run every Sunday and Thursday at 1:00 AM.

```
config wvs schedule
   edit "WVS-schedule1"
      set type recurring
      set time 01:00
      set wday Sunday Thursday
   next
end
```

Related topics

- config wvs profile
- config wvs policy

diagnose

The `diagnose` commands display diagnostic information that help you troubleshoot problems. These commands do not have an equivalent in the web UI.

This chapter describes the following commands:

diagnose debug

diagnose debug application autolearn

diagnose debug application detect

diagnose debug application dssl

diagnose debug application fds

diagnose debug application hasync

diagnose debug application hatalk

diagnose debug application http

diagnose debug application miglogd

diagnose debug application mulpattern

diagnose debug application proxy

diagnose debug application ustack

diagnose debug application waf-fds-update

diagnose debug comlog

diagnose debug cli

diagnose debug cmdb

diagnose debug application proxy-error

diagnose debug application snmp

diagnose debug application ssl

diagnose debug application sysmon

diagnose debug console timestamp

diagnose debug crashlog

diagnose debug dnsproxy list

diagnose debug emerglog

diagnose debug flow filter

diagnose debug flow reset

diagnose debug flow filter module-detail

diagnose hardware check

diagnose debug flow trace

diagnose debug flow trace

diagnose debug info

diagnose debug init

diagnose hardware cpu

diagnose debug reset

diagnose debug upload

diagnose hardware harddisk

diagnose hardware interrupts

diagnose hardware logdisk info

diagnose hardware mem

diagnose hardware nic

diagnose hardware raid list

diagnose index

diagnose log

diagnose network arp

diagnose network ip

diagnose network route	diagnose policy	diagnose system ha sync-stat
diagnose network rtcache	diagnose system flash	diagnose system kill
diagnose network sniffer	diagnose system ha file-stat	diagnose system mount
diagnose network tcp list	diagnose system ha mac	diagnose system top
diagnose network udp list	diagnose system ha status	diagnose system update info

debug

Use this command to turn debug log output on or off.

Debug logging 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.

By default, the most verbose logging that is available from the web UI for any log type is the **Information** severity level. Due to their usually unnecessary nature, logs at the severity level of **Debug** are disabled and hidden. They can only be enabled and viewed from the CLI. Typically this is done only if your configuration seems to be correct, you cannot diagnose the problem without more information, and possibly suspect that you may have found either a hardware failure or software bug.

To generate debug logs, you must:

1. Set the verbosity level for the specific module whose debugging information you want to view, via a debug log command such as:

   ```
   debug application hasync [{-1 | 0 | 1 | 2 | 4 | 8}]
   ```

2. If necessary configure any filters specific to the module whose debugging information you are viewing, such as:

   ```
   debug flow filter server-ip 10.0.0.10
   ```

3. If necessary start debugging specific to the module, such as:

   ```
   debug flow trace start
   ```

4. Enable debug logs overall. To do this, enter:

   ```
   debug enable
   ```

5. View the debug logs. For convenience, debugging logs are immediately output to your local console display or terminal emulator, but debug log files can also be uploaded to a server. For more complex issues or bugs, this

may be required in order to send debug information to Fortinet Technical Support. To do this, use the command:

```
debug upload
```

Debug logs will be generated only if the application is running. To verify this, use `diagnose system top` . Otherwise, use `diagnose debug crashlog` instead.

6. The CLI will display debug logs as they occur until you either:

   - Disable it by either typing:

     `diagnose debug disable`
     or setting all modules' debug log verbosity back to `0`. To reset all verbosity levels simultaneously, you can use the command:

     `diagnose debug reset`

   - Close your terminal emulator, thereby ending your administrative session.
   - Send a termination signal to the console by pressing Ctrl+C.
   - Reboot the appliance. To do this, you can use the command:

     `execute reboot`
     To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug {enable | disable}
```

Variable	Description	Default
`debug {enable | disable}`	Select whether to enable or disable recording of logs at the debug severity level.	`disable`

Related topics

- `diagnose debug application autolearn`
- `diagnose debug application detect`
- `diagnose debug application dssl`
- `diagnose debug application fds`
- `diagnose debug application hasync`
- `diagnose debug application hatalk`
- `diagnose debug application http`
- `diagnose debug application miglogd`
- `diagnose debug application mulpattern`
- `diagnose debug application proxy`
- `diagnose debug application proxy-error`

- diagnose debug application snmp
- diagnose debug application ssl
- diagnose debug application sysmon
- diagnose debug application ustack
- diagnose debug application waf-fds-update
- diagnose debug cli
- diagnose debug crashlog
- diagnose debug flow trace
- diagnose debug upload
- diagnose log

debug application autolearn

Use this command to view and set the verbosity level of debug logs for auto-learning.

Before you can see any debug logs, you must first enable debug log output using the command debug.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application autolearn [{autolearn_int}]
```

Variable	Description	Default
`autolearn [{autolearn_int}]`	Specifies the verbosity level to output to the CLI display after the command executes. Valid range is 0 to 7, where 0 disables debug logs for auto-learning and 7 generates the most verbose logging. If you omit the number, the CLI displays the current verbosity level. For example: `autolearn debug level is 0`	`0`

Related topics

- diagnose debug
- diagnose debug console timestamp
- diagnose debug info
- diagnose debug reset
- diagnose debug upload

debug application detect

Use this command to set the verbosity level of debug logs for intrusion detection.

Before you can see any debug logs, you must first enable debug log output using the command `diagnose debug`.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application detect [{0-7}]
```

Variable	Description	Default
`detect [{0-7}]`	Optionally, type the number that specifies the verbosity level to output to the CLI display after the command executes. Valid range is 0 to 7, where 0 disables debug logs for intrusion detection and 7 generates the most verbose logging. If you omit the number, the CLI displays the current verbosity level: `detect debug level is 0`	`0`

Related topics

- `diagnose debug`
- `diagnose debug console timestamp`
- `diagnose debug info`
- `diagnose debug reset`
- `diagnose debug upload`

debug application dssl

Use this command to set the verbosity level of debug logs for SSL inspection (temporary decryption in order to enforce policies). SSL inspection is used only when FortiWeb is operating in a mode that supports it, such as transparent inspection mode or offline protection mode.

Before you will be able to see any debug logs, you must first enable debug log output using the command `diagnose debug`.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application dssl [{0-7}]
```

Variable	Description	Default
`dssl [{0-7}]`	Optionally, type the number that specifies the verbosity level to output to the CLI display after the command executes. Valid range is 0 to 7, where 0 disables debug logs for SSL inspection and 7 generates the most verbose logging. If you omit the number, the CLI displays the current verbosity level. For example: `dssl debug level is 0`	`0`

Related topics

- `diagnose debug`
- `diagnose debug console timestamp`
- `diagnose debug info`
- `diagnose debug reset`
- `diagnose debug upload`

debug application fds

Use this command to set the verbosity level of debug logs for update requests to the Fortinet Distribution Network (FDN).

Before you will be able to see any debug logs, you must first enable debug log output using the command `diagnose debug`.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application fds [{0-7}]
```

Variable	Description	Default
`fds [{0-7}]`	Optionally, type the number that specifies the verbosity level to output to the CLI display after the command executes. Valid range is 0 to 7, where 0 disables debug logs for FDN updates and 7 generates the most verbose logging. If you omit the number, the CLI displays the current verbosity level. For example: `fds debug level is 0`	`0`

Related topics

- `diagnose debug`
- `diagnose debug console timestamp`
- `diagnose debug info`
- `diagnose debug reset`
- `diagnose debug upload`

debug application hasync

Use this command to set the verbosity level and type of debug logs for HA synchronization.

Before you will be able to see any debug logs, you must first enable debug log output using the command `diagnose debug`.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application hasync [{-1 | 0 | 1 | 2 | 4 | 8}]
```

Variable	Description	Default
`hasync [{-1 | 0 | 1 | 2 | 4 | 8}]`	Optionally, type the number indicating the verbosity level and type of debugging messages to output to the CLI display after the command executes. • -1 — Display all messages. • 0 — Do not display messages. • 1 — Display application messages such as MD5 checksums for the configuration, and confirmation that the standby appliance received the synchronized data. • 2 — Display network transmission messages, such as ARP broadcasts and bridge down/up status changes. • 4 — Display packet transmission messages. • 8 — Display messages about configuration file (fwb_system.conf) merges. If you omit the number, the CLI displays the current verbosity level: `hasync debug level is 0`	0

Example

This example enables diagnostic debug logging in general, then specifically enables packet transmission logging of the HA synchronization daemon, `hasyncd`.

```
diagnose debug enable
diagnose debug application hasync level 4
```

The CLI displays output such as the following until the command is terminated:

```
FortiWeb # (ha_sync.c : 624) : No element in ha send queue
(ha_send_queue.c : 184) : add request to ha sendqueue success
(ha_send_queue.c : 184) : add request to ha sendqueue success
(ha_send_queue.c : 242) : read send request from local, len = 447
(ha_send_queue.c : 242) : read send request from local, len = 450
(ha_sync.c : 637) : Got an element from ha send queue
(ha_sync.c : 454) : msglen : 23, msgbuf : config system dns
end

(ha_sync_send.c : 475) : total cnt : 1, cur cnt : 0
(ha_sync_send.c : 357) : send buf len = 171
(ha_sync_send.c : 383) : sent conf(0) return 171 bytes
(ha_sync_send.c : 406) : Send conf success from [hbdev], and got reply
(ha_sync.c : 637) : Got an element from ha send queue
(ha_sync.c : 454) : msglen : 26, msgbuf : config system global
end

(ha_sync_send.c : 475) : total cnt : 1, cur cnt : 0
(ha_sync_send.c : 357) : send buf len = 174
(ha_sync_send.c : 383) : sent conf(0) return 174 bytes
(ha_sync_send.c : 406) : Send conf success from [hbdev], and got reply
(ha_sync.c : 624) : No element in ha send queue
```

```
(ha_sync.c : 624) : No element in ha send queue
(ha_sync.c : 624) : No element in ha send queue
(ha_send_queue.c : 184) : add request to ha sendqueue success
(ha_send_queue.c : 242) : read send request from local, len = 424
(ha_sync.c : 637) : Got an element from ha send queue
(ha_sync_send.c : 475) : total cnt : 1, cur cnt : 0
(ha_sync_send.c : 357) : send buf len = 178
(ha_sync_send.c : 383) : sent conf(0) return 178 bytes
(ha_sync_send.c : 406) : Send conf success from [hbdev], and got reply
(ha_sync.c : 624) : No element in ha send queue
(ha_sync.c : 624) : No element in ha send queue
(ha_sync_recv.c : 362) : Got an valid packet, len = 180
(ha_sync_recv.c : 759) : Enter Fun : sync_recv_msg
(ha_sync_recv.c : 248) : Enter Fun : _sync_packet_check_msg, buflen = 180
(ha_sync_recv.c : 262) : msg body ssid : AC6C02
(ha_sync_recv.c : 285) : add new pkt_ss_id to last_pkt_ss_id[8]
(ha_sync_recv.c : 780) : We recved an valid SYNC_MSG(29) packet
(ha_send_queue.c : 184) : add request to ha sendqueue success
(ha_send_queue.c : 242) : read send request from local, len = 440
(ha_send_queue.c : 184) : add request to ha sendqueue success
(ha_send_queue.c : 242) : read send request from local, len = 424
(ha_sync.c : 637) : Got an element from ha send queue
(ha_sync.c : 454) : msglen : 16, msgbuf : 2â¢O
(ha_sync_send.c : 475) : total cnt : 1, cur cnt : 0
(ha_sync_send.c : 357) : send buf len = 164
(ha_sync_send.c : 383) : sent conf(0) return 164 bytes
(ha_sync_send.c : 406) : Send conf success from [hbdev], and got reply
(ha_sync.c : 637) : Got an element from ha send queue
(ha_sync_send.c : 475) : total cnt : 1, cur cnt : 0
(ha_sync_send.c : 357) : send buf len = 178
(ha_sync_send.c : 383) : sent conf(0) return 178 bytes
(ha_sync_send.c : 406) : Send conf success from [hbdev], and got reply
```

The results indicate that, initially, the MD5 configuration hash did not indicate any configuration changes (`No element in ha send queue`). But then an administrator changed the configuration, perhaps through the web UI, and the appliance detected changes to its DNS (`msgbuf : config system dns`) and global (`msgbuf : config system global`) settings. The active appliance then sent the changes to the standby appliance (`Send conf success from [hbdev], and got reply`); causes of success or failure is detailed by other debugging messages, such as the number of items in the synchronization queue (`total cnt : 1, cur cnt : 0`), and the number of bytes transferred from the synchronization buffer (`send buf len = 178`).

Related topics

- `diagnose debug`
- `diagnose debug console timestamp`
- `diagnose debug info`
- `diagnose debug reset`
- `diagnose debug upload`

debug application hatalk

Use this command to set the verbosity level and type of debug logs for HA heartbeats.

Before you will be able to see any debug logs, you must first enable debug log output using the command `diagnose debug`.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application hatalk [{-1 | 0 | 1 | 2}]
```

Variable	Description	Default
`[{-1 | 0 | 1 | 2}]`	Optionally, type the number indicating the verbosity level and type of debugging messages to output to the CLI display after the command executes. • -1 — Display all messages. • 0 — Do not display messages. • 1 — Display application messages such as MD5 checksums for the configuration, and confirmation that the standby appliance received the synchronized data. • 2 — Display network transmission messages, such as ARP broadcasts and bridge down/up status changes. If you omit the number, the CLI displays the current verbosity level: `hatalk debug level is 0`	0

Example

This example enables diagnostic debug logging in general, then specifically enables complete debug logging of the HA heartbeat daemon, `hatalkd`.

```
diagnose debug enable
diagnose debug application hatalk -1
```

The CLI displays output such as the following until the command is terminated:

```
FortiWeb # (ha_hb.c : 176) : mem-table[0]:
(ha_hb.c : 61) : member name : wasp
(ha_hb.c : 62) : member pcnt : 0
(ha_hb.c : 63) : member pri : 5
(ha_hb.c : 64) : member sn : FV-1KC3R11700136
(ha_hb.c : 65) : member age : 11209
(ha_hb.c : 66) : member role : 1
(intf_check.c : 273) : clicfg->monitor_count : 1, count : 1
(ha_hb_send.c : 85) : sock : 26, sendlen : 264(head: 88, mem(2) 88)
```

```
(ha_hb_send.c : 104) : Send HB buf success.
(ha_hb.c : 83) : Enter Function : get_master_sn
(ha_hb.c : 756) : ------------------------
(ha_hb.c : 760) : ==> HB..., I'am (Master) master is : FV-1KC3R11700094
(ha_hb.c : 637) : update my status info : FV-1KC3R11700094
(ha_hb.c : 871) : Enter Fun : hb_packet_check
(ha_hb.c : 897) : mysn : FV-1KC3R11700094(0), comesn : FV-1KC3R11700136(1)
(ha_hb_recv.c : 446) : Got an valid HB packet(port3), len : 176
(ha_hb_recv.c : 451) : come from : FV-1KC3R11700136
(ha_hb_recv.c : 104) : fill ha member to local
(ha_hb_recv.c : 251) : slave (FV-1KC3R11700136) arrived ...
(ha_hb_recv.c : 342) : An exist slave device arrive...
(ha_hb_recv.c : 512) : sockfd1 : 200(UP), sockfd2 : 0(DOWN)
(ha_hb.c : 159) : Enter Function : print_member_tab
(ha_hb.c : 166) : total cnt : 2
```

(output truncated)

```
(main.c : 1005) : send short cli msg to :
FV-1KC3R11700136
(main.c : 1349) : switch MASTER -> SLAVE
(main.c : 1350) : block ARP
(main.c : 1219) : HA device into Slave mode
(main.c : 1220) : device block ARP
(main.c : 1121) : Get BrgInfo, my brgCnt = 0
```

The results indicate that the HA cluster is named `wasp` (group ID 0, HA link over port3). It is formed by the active appliance `FV-1KC3R11700094` (device priority 5) and the standby appliance `FV-1KC3R11700136`. The two appliances then switched rules — that is, a failover occurred.

Related topics

- `diagnose debug`
- `diagnose debug console timestamp`
- `diagnose debug info`
- `diagnose debug reset`
- `diagnose debug upload`

debug application http

Use this command to set the verbosity level of debug logs for the HTTP protocol parser. This parser module dissects the HTTP headers and content body for analysis by other modules such as rewriting, HTTP protocol constraints, server information disclosure, and attack signature matching.

If the debug logs indicate that the HTTP protocol parser may be encountering an error condition, you can temporarily disable it and allow packets to bypass it to verify if this is the case. See noparse {enable | disable} in `config server-policy policy`.

Before you will be able to see any debug logs, you must first enable debug log output using the command `diagnose debug`.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application http [{0-7}]
```

Variable	Description	Default
`http [{0-7}]`	Optionally, type the number that specifies the verbosity level to output to the CLI display after the command executes. Valid range is 0 to 7, where 0 disables debug logs for the HTTP protocol parser and 7 generates the most verbose logging. If you omit the number, the CLI displays the current verbosity level. For example: `http debug level is 0`	`0`

Related topics

- `diagnose debug`
- `diagnose debug console timestamp`
- `diagnose debug info`
- `diagnose debug reset`
- `diagnose debug upload`
- `diagnose debug flow trace`

debug application miglogd

Use this command to set the verbosity level of debug logs for the log daemon, `miglogd`.

Before you will be able to see any debug logs, you must first enable debug log output using the command `diagnose debug`.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application miglogd [{0-7}]
```

Variable	Description	Default
`miglogd [{0-7}]`	Optionally, type the number that specifies the verbosity level to output to the CLI display after the command executes. Valid range is 0 to 7, where 0 disables debug logs for the log daemon and 7 generates the most verbose logging. If you omit the number, the CLI displays the current verbosity level. For example: `miglogd debug level is 0`	`0`

Related topics

- `diagnose debug`
- `diagnose debug console timestamp`
- `diagnose debug info`
- `diagnose debug reset`
- `diagnose debug upload`
- `execute db rebuild`

debug application mulpattern

Use this command to set the verbosity level of debug logs for the pattern matching module.

Before you will be able to see any debug logs, you must first enable debug log output using the command `diagnose debug`.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application mulpattern [{0-7}]
```

Variable	Description	Default
`mulpattern [{0-7}]`	Optionally, type the number that specifies the verbosity level to output to the CLI display after the command executes. Valid range is 0 to 7, where 0 disables debug logs for the pattern matching module and 7 generates the most verbose logging. If you omit the number, the CLI displays the current verbosity level. For example: `mulpattern debug level is 0`	`0`

Related topics

- `diagnose debug`
- `diagnose debug console timestamp`
- `diagnose debug info`
- `diagnose debug reset`
- `diagnose debug upload`

debug application proxy

Use this command to set the verbosity level of debug logs for flow through the XML application proxy.

Before you will be able to see any debug logs, you must first enable debug log output using the command `diagnose debug`.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application proxy [{0-7}]
```

Variable	Description	Default
`proxy [{0-7}]`	Optionally, type the number that specifies the verbosity level to output to the CLI display after the command executes. Valid range is 0 to 7, where 0 disables debug logs for the XML application proxy flow and 7 generates the most verbose logging. If you omit the number, the CLI displays the current verbosity level. For example: `proxy debug level is 0`	`0`

Related topics

- diagnose debug
- diagnose debug console timestamp
- diagnose debug info
- diagnose debug reset
- diagnose debug upload

debug application proxy-error

Use this command to set the verbosity level of debug logs for errors in the XML application proxy.

Before you will be able to see any debug logs, you must first enable debug log output using the command diagnose debug.

To use this command, your administrator account's access control profile requires only r permission in any profile area.

Syntax

```
diagnose debug application proxy-error [{-1 | 0}]
```

Variable	Description	Default
proxy-error [{-1 | 0}]	Optionally, type the number that specifies the verbosity level to output to the CLI display after the command executes. Valid range is 0 to 7, where 0 disables debug logs for XML application proxy errors and 7 generates the most verbose logging. If you omit the number, the CLI displays the current verbosity level. For example: proxy-error debug level is 0	0

Related topics

- diagnose debug
- diagnose debug console timestamp
- diagnose debug info
- diagnose debug reset
- diagnose debug upload

debug application snmp

Use this command to debug the SNMP daemon.

Syntax

```
diagnose debug application snmp <snmp_int>
```

Variable	Description	Default
`snmp <snmp_int>`	Specifies the verbosity level to output to the CLI display after the command executes. Valid range is 0 to 7, where 0 disables SNMP debugging and 7 generates the most verbose logging. If you omit the number, the CLI displays the current verbosity level: `snmp debug level is 0`	`0`

Related topics

- `diagnose debug`
- `diagnose debug console timestamp`
- `diagnose debug info`
- `diagnose debug reset`
- `diagnose debug upload`

debug application ssl

Use this command to set the verbosity level of debug logging for SSL/TLS offloading. SSL offloading is supported only when the FortiWeb appliance is operating in reverse proxy mode or true transparent proxy mode.

Before you will be able to see any debug logs, you must first enable debug log output using the command `diagnose debug`.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug application ssl [{0-7}]
```

Variable	Description	Default
`ssl [{0-7}]`	Specifies the verbosity level to output to the CLI display after the command executes. Valid range is 0 to 7, where 0 disables debug logging of SSL/TLS offloading and 7 generates the most verbose logging. If you omit the number, the CLI displays the current verbosity level. For example: `ssl debug level is 0`	0

Example

This example enables diagnostic debug logging overall, then specifically enables debug logging for SSL in reverse proxy mode.

```
diagnose debug enable
diagnose debug application ssl
```

Related topics

- `diagnose debug`
- `diagnose debug console timestamp`
- `diagnose debug info`
- `diagnose debug reset`
- `diagnose debug upload`

debug application sysmon

Use this command to debug the system monitor.

Syntax

```
diagnose debug application sysmon <sysmon_int>
```

Variable	Description	Default
`sysmon <sysmon_int>`	Specifies the Sysmon debug level. Valid range is 0 to 7, where 0 disables system monitor debugging and 7 generates the most verbose logging. If you omit the number, the CLI displays the current verbosity level. For example: `sysmon debug level is 0`	0

Related topics

- diagnose debug
- diagnose debug console timestamp
- diagnose debug info
- diagnose debug reset
- diagnose debug upload

debug application ustack

Use this command to set the verbosity level of debug logs for the user-space TCP/IP connectivity stack.

Before you will be able to see any debug logs, you must first enable debug log output using the command diagnose debug.

To use this command, your administrator account's access control profile requires only r permission in any profile area.

Syntax

```
diagnose debug application ustack [{0-7}]
```

Variable	Description	Default
ustack [{0-7}]	Specifies the verbosity level to output to the CLI display after the command executes. Valid range is 0 to 7, where 0 disables debug logging of the user-space TCP/IP connectivity stack and 7 generates the most verbose logging. If you omit the number, the CLI displays the current verbosity level. For example: `ustack debug level is 0`	0

Related topics

- diagnose debug
- diagnose debug console timestamp
- diagnose debug info
- diagnose debug reset
- diagnose debug upload

debug application waf-fds-update

Use this command to debug the FortiGuard service update processs.

Syntax

```
diagnose debug application waf-fds-update <fds-update_int>
```

Variable	Description	Default
`waf-fds-update <fds-update_int>`	Specifies the verbosity level to output to the CLI display after the command executes. Valid range is 0 to 7, where 0 disables FortiGuard Distribution Server (FDS) update debugging and 7 generates the most verbose logging. If you omit the number, the CLI displays the current verbosity level. For example: `waf-fds-update debug level is 0`	`0`

Related topics

- `diagnose debug`
- `diagnose debug console timestamp`
- `diagnose debug info`
- `diagnose debug reset`
- `diagnose debug upload`

debug cli

Use this command to set the debug level for the command line interface (CLI).

Before you will be able to see any debug logs, you must first enable debug log output using the command `diagnose debug`.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug cli [{0-7}]
```

Variable	Description	Default
`cli [{0-7}]`	Optionally, type the number that specifies the verbosity level to output to the CLI display after the command executes. Valid range is 0 to 7, where 0 disables debug logs for the CLI and 7 generates the most verbose logging. If you omit the number, the CLI displays the current verbosity level. For example: `cli debug level is 0`	`3`

Related topics

- `diagnose debug`
- `diagnose debug console timestamp`
- `diagnose debug info`
- `diagnose debug reset`
- `diagnose debug upload`

debug cmdb

Use this command to enable the debug log for the configuration management database (CMDB).

Before you will be able to see any debug logs, you must first enable debug log output using the command `diagnose debug`.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug cmdb
```

Related topics

- `diagnose debug`
- `diagnose debug console timestamp`
- `diagnose debug info`
- `diagnose debug reset`
- `diagnose debug upload`

debug comlog

Use this command to enable or disable saving to disk of kernel or daemon core dump logs when you press the NMI button on the appliance. This button is not available on all models. For details, see the *FortiWeb NMI & COMlog Technical Note* and your model's QuickStart Guide.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug comlog daemon enable
diagnose debug comlog kernel enable
diagnose debug comlog daemon show
diagnose debug comlog kernel show
diagnose debug comlog daemon clear
diagnose debug comlog kernel clear
diagnose debug comlog info
```

Related topics

- `diagnose debug reset`
- `diagnose debug info`

debug console timestamp

Use this command to enable or disable the timestamp in debug logs.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug console timestamp [{enable | disable}]
```

Variable	Description	Default
`timestamp [{enable | disable}]`	Type `enable` to add timestamps to debug output or `disable` to remove them. If you omit the selection, the CLI displays the current timestamp status: `console timestamp is disabled.`	`disable`

Related topics

- diagnose debug reset
- diagnose debug info

debug crashlog

Use this command to show crash logs from application proxies that have call back traces, segmentation faults, or memory register dumps, or to delete the crash log.

To use this command, your administrator account's access control profile requires only r permission in any profile area.

Syntax

```
diagnose debug crashlog show
diagnose debug crashlog clear
```

Example

```
diagnose debug crashlog show
```

Output similar to the following appears in the CLI:

```
2011-02-08 06:20:46 <18632> firmware FortiWeb-1000B 4.20,build0403,110131
2011-02-08 06:20:46 <18632> application proxy
2011-02-08 06:20:46 <18632> *** signal 11 (Segmentation fault) received ***
2011-02-08 06:20:46 <18632> Register dump:
2011-02-08 06:20:46 <18632> RAX: 00000000 RBX: 00000001 RCX: 00000001 RDX:
    00000001
2011-02-08 06:20:46 <18632> RSI: 008d91a4 RDI: 00000000 RBP: 2b8f90ee2b10 RSP:
    0072af60
2011-02-08 06:20:46 <18632> RIP: 008d8660 EFLAGS: 2b8f9aaa0010
2011-02-08 06:20:46 <18632> CS: 86b0 FS: 0000 GS: 008d
2011-02-08 06:20:46 <18632> Trap: 7fff26859ee0 Error: 008d8710 OldMask:
    00440f90
2011-02-08 06:20:46 <18632> CR2: 00010202
2011-02-08 06:20:46 <18632> Backtrace:
2011-02-08 06:20:46 <18632> [0x008d8660] => /bin/xmlproxy (g_proxy+0x00000000)
2011-02-08 06:20:46 proxy received SEGV signal - 11
```

debug dnsproxy list

Use this command to display the DNS cache that stores the results of resolving all fully qualified domain names in the server pools.

To use this command, your administrator account's access control profile requires only r permission in any profile area.

Syntax

```
diagnose debug dnsproxy list
```

Example

```
diagnose debug dnsproxy list
```

If the domain specified for the server pool member is `www.example.org` and has resolved to `10.20.5.12`, output similar to the following is displayed:

```
www.example.org
10.20.5.12
10:20::5:12
```

Related topics

- `config system dns`

debug emerglog

Use this command to view or erase disk read-only error logs.

Syntax

```
diagnose debug emerglog {show | clear}
```

Variable	Description	Default
{show | clear}	Type `show` to view disk read-only error logs. Type `clear` to delete error logs.	No default

debug flow filter

Use these commands to generate only packet flow debug logs that match your filter criteria, such as a specific destination IP address. You can also use these commands to delete the packet flow debug log filter, so that all packet flow debug logs are generated.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug flow filter reset
diagnose debug flow filter client-ip <source_ipv4 | source_ipv6>
diagnose debug flow filter server-ip <destination_ipv4 | destination_ipv6>
```

Variable	Description	Default
`client-ip <source_ipv4 | source_ipv6>`	Type the source (`SRC`) IP address of connections. This will generate only packet flow debug log messages involving that source IP address. **Note:** This filter operates at the IP layer, **not** the HTTP layer. If a load balancer or other web proxy is deployed in front of FortiWeb, and therefore all connections for HTTP requests appear to originate from this IP address, configuring this filter will have no effect. Similarly, if multiple clients share an Internet connection via NAT or explicit web proxy, configuring this filter will only isolate connections that share this IP address. It will **not** be able to filter out a single client based on individual HTTP sessions from that IP.	No default.
`server-ip <destination_ipv4 | destination_ipv6>`	Type the destination (`DST`) IP address of the connection, either the: • virtual server on FortiWeb (if FortiWeb is operating in reverse proxy mode) • protected web server on the back end (all other operation modes) This will generate only packet flow debug log messages involving that server IP address.	No default.

Related topics

- `diagnose debug flow trace`

debug flow filter module-detail

Use this command to include or exclude debug logs from each FortiWeb feature module as the packet is processed when generating packet flow debug logs. This can be useful if you suspect that a module is encountering errors, or need to know which module is dropping the packet.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug flow filter module-detail {on | off}
```

Variable	Description	Default
`module-detail {on | off}`	Select whether to include (`on`) or exclude (`off`) details from each module that processes the packet.	No default.

Related topics

- `diagnose debug flow trace`
- `diagnose debug flow reset`

debug flow reset

Use this command to reset the configuration of packet flow debug log messages.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug flow reset
```

Related topics

- `diagnose debug flow filter`
- `diagnose debug flow filter module-detail`

debug flow trace

Use this command to trace the flow of packets through the FortiWeb appliance's processing modules and network stack.

Before you can see any debug logs, you must first enable debug log output using the command `diagnose debug`.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug flow trace {start | stop}
```

Variable	Description	Default
`trace {start | stop}`	Select whether to enable (`start`) or disable (`stop`) the recording of packet flow trace debug log messages.	No default.

Example

This example configures a filter based on the packet destination IP 172.120.20.48, enables messages from each packet processing module, enables packet flow traces, then finally begins generating the debug logs that are enabled for output (in this case, only packet trace debug logs).

Because the filters are configured **before** debug logging is enabled, the administrator can type the filter without being interrupted by debug log output to the CLI.

```
diagnose debug flow filter server-ip 172.20.120.48
diagnose debug flow flow module-detail on
diagnose debug flow trace start
diagnose debug enable
```

Output:

```
FortiWeb # session_id=251 packet_id=0 policy_name=policy1 msg="Receive packet from client
    172.20.120.225:49428"
session_id=251 packet_id=0 msg="HTTP parsing client packet success"
session_id=251 packet_id=0 policy_name="policy1" msg="
Module name:WAF_IP_LIST_CHECK, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_X_FORWARD_FOR_PROCESS, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_GEO_BLOCK_LIST, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_PROTECTED_SERVER_CHECK, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_ALLOW_METHOD_PROCESS, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_HTTP_ACTIVE_SCRIPT, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_HTTP_SESSION_MANAGEMENT, Execution:4, Process error:1, Action:ACCEPT
Module name:WAF_HTTP_DOS_PREVENTION, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_LAYER4_DOS_PREVENTION, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_HTTP_AUTHENTICATION, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_GLOBAL_WHITE_LIST, Execution:4, Process error:0, Action:ACCEPT
Module name:WAF_URL_ACCESS_POLICY, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_BRUCE_FORCE_LOGIN, Execution:3, Process error:0, Action:ACCEPT
Module name:HTTP_CONSTRAINTS, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_COOKIE_POISON, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_START_PAGES, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_PAGE_ACCESS_RULE, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_FILE_UPLOAD_RESTRICTION_POLICY, Execution:3, Process error:0,
    Action:ACCEPT
Module name:ROBOT_CONTROL_PROCESS, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_PARAMETWER_VALIDATION_PROCESS, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_CHUNK_DECODE, Execution:3, Process error:2, Action:ACCEPT
Module name:WAF_FILE_UNCOMPRESS, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_SIG_DETECT_PROCESS, Execution:4, Process error:1, Action:ACCEPT
Module name:WAF_HIDDEN_FIELD_PROCESS, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_URL_REWRITING, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_FILE_COMPRESS, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_CERTIFICATE_FORWARD, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_AUTOLEARN, Execution:4, Process error:0, Action:ACCEPT
Module name:WAF_HTTP_STATISTIC, Execution:3, Process error:0, Action:ACCEPT
"
session_id=502 packet_id=0 policy_name=policy1 msg="Receive packet from client
    172.20.120.225:49429"
session_id=502 packet_id=0 msg="HTTP parsing client packet success"
session_id=502 packet_id=0 policy_name="policy1" msg="
Module name:WAF_IP_LIST_CHECK, Execution:3, Process error:0, Action:ACCEPT
```

```
Module name:WAF_X_FORWARD_FOR_PROCESS, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_GEO_BLOCK_LIST, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_PROTECTED_SERVER_CHECK, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_ALLOW_METHOD_PROCESS, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_HTTP_ACTIVE_SCRIPT, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_HTTP_SESSION_MANAGEMENT, Execution:4, Process error:1, Action:ACCEPT
Module name:WAF_HTTP_DOS_PREVENTION, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_LAYER4_DOS_PREVENTION, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_HTTP_AUTHENTICATION, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_GLOBAL_WHITE_LIST, Execution:4, Process error:1, Action:ACCEPT
Module name:WAF_URL_ACCESS_POLICY, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_BRUCE_FORCE_LOGIN, Execution:1, Process error:0, Action:ACCEPT
Module name:HTTP_CONSTRAINTS, Execution:1, Process error:0, Action:ACCEPT
Module name:WAF_COOKIE_POISON, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_START_PAGES, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_PAGE_ACCESS_RULE, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_FILE_UPLOAD_RESTRICTION_POLICY, Execution:3, Process error:0,
    Action:ACCEPT
Module name:ROBOT_CONTROL_PROCESS, Execution:1, Process error:0, Action:ACCEPT
Module name:WAF_PARAMETWER_VALIDATION_PROCESS, Execution:1, Process error:0, Action:ACCEPT
Module name:WAF_CHUNK_DECODE, Execution:3, Process error:2, Action:ACCEPT
Module name:WAF_FILE_UNCOMPRESS, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_SIG_DETECT_PROCESS, Execution:1, Process error:0, Action:ACCEPT
Module name:WAF_HIDDEN_FIELD_PROCESS, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_URL_REWRITING, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_FILE_COMPRESS, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_CERTIFICATE_FORWARD, Execution:3, Process error:0, Action:ACCEPT
Module name:WAF_AUTOLEARN, Execution:4, Process error:0, Action:ACCEPT
Module name:WAF_HTTP_STATISTIC, Execution:3, Process error:0, Action:ACCEPT
"
session_id=0 packet_id=0 policy_name=policy1 msg="Receive packet from client
    172.20.120.48:47368"
session_id=1 packet_id=0 policy_name=policy1 msg="Receive packet from client
    172.20.120.48:59682"
session_id=252 packet_id=0 policy_name=policy1 msg="Receive packet from client
    172.20.120.48:47376"
session_id=503 packet_id=0 policy_name=policy1 msg="Receive packet from client
    172.20.120.48:59687"
session_id=754 packet_id=0 policy_name=policy1 msg="Receive packet from client
    172.20.120.48:47382"
session_id=2 packet_id=0 policy_name=policy1 msg="Receive packet from client
    172.20.120.48:47385"
session_id=253 packet_id=0 policy_name=policy1 msg="Receive packet from client
    172.20.120.48:47387"
diag debug disable

FortiWeb #
```

Session lines contain the name of the matching server policy (`policy_name`), the packet identifier (`packet_ID`), and TCP session ID (`session_id`), as well as a log message (`msg`) indicating one or more of the following:

- the source IP address and port number of the packet (e.g. `Receive packet from client 172.20.120.225:49428`)
- the success or failure of FortiWeb's HTTP parser's attempt to analyze the HTTP headers and payload of the packet into pieces that can be scanned or modified by modules (e.g. `HTTP parsing client packet success` or `Packet dropped by detection module,and module number=11`)

If the debug logs indicate that the HTTP protocol parser may be encountering an error condition, you can temporarily disable it and allow packets to bypass it to verify if this is the case. See noparse {enable | disable} in `config server-policy policy`.

If enabled, module lines contain messages from each FortiWeb feature module as it processes the packet (e.g. `Module name:WAF_PROTECTED_SERVER_CHECK` for the feature that tests for an allowed `Host:` name in the request). The module logs are displayed in their order of execution (for details, see the *FortiWeb Administration Guide*). These messages indicate:

- whether or not the module executed, and if not, the reason (e.g. `Execution:1`)
- processing errors, if any (e.g. `Process error:0`)
- whether a module has allowed or blocked the packet (e.g. `Action:ACCEPT` or `Action:FOLLOWUP_ACCEP`)

For non-execution reasons, possible status codes are:

- `Execution:1` — The module is disabled, and therefore is being skipped.
- `Execution:2` — The module is not supported in the current deployment mode, and therefore is being skipped.
- `Execution:3` — The client IP address is whitelisted, and therefore the module is being skipped.
- `Execution:4` — URL access policy has caused the module to be skipped.

Related topics

- `config server-policy policy`
- `config server-policy server-pool`
- `config server-policy custom-application application-policy`
- `config waf url-access url-access-rule`
- `diagnose policy`
- `diagnose debug application http`
- `diagnose debug flow filter`
- `diagnose debug flow filter module-detail`
- `diagnose debug`

debug info

Use this command to display a list of debug log settings.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug info
```

Example

```
diagnose debug application ssl 8
diagnose debug application dssl 8
```

```
diagnose debug application ustack 8
diagnose debug info
```

Output similar to the following appears in the CLI:

```
debug output: disable
console timestamp: disable
ssl debug level: 8
ustack debug level: 8
dssl debug level: 8
CLI debug level: 3
```

If you have not modified any verbosity levels, only this default output appears:

```
FortiWeb # diagnose debug info
debug output: disable
console timestamp: disable
CLI debug level: 3
```

Related topics

- diagnose debug reset
- diagnose debug
- diagnose debug console timestamp
- diagnose debug application autolearn
- diagnose debug application detect
- diagnose debug application dssl
- diagnose debug application fds
- diagnose debug application hasync
- diagnose debug application hatalk
- diagnose debug application http
- diagnose debug application miglogd
- diagnose debug application mulpattern
- diagnose debug application proxy
- diagnose debug application proxy-error
- diagnose debug application ssl
- diagnose debug application ustack
- diagnose debug cli

debug init

Syntax

```
diagnose debug init [{enable | disable}]
```

Variable	Description	Default
`init [{enable | disable}]`	Select whether to enable (`start`) or disable (`stop`) the recording of packet flow trace debug log messages. If you omit the selection, the CLI displays the current timestamp status: `init output: disabled`	No default.

debug reset

Use this command to reset all debug log settings to default settings for the currently installed firmware version. If you have not upgraded or downgraded the firmware, this restores the factory default settings.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug reset
```

Related topics

- diagnose debug info
- diagnose debug console timestamp
- diagnose debug application autolearn
- diagnose debug application detect
- diagnose debug application dssl
- diagnose debug application fds
- diagnose debug application hasync
- diagnose debug application hatalk
- diagnose debug application http
- diagnose debug application miglogd
- diagnose debug application mulpattern
- diagnose debug application proxy
- diagnose debug application proxy-error
- diagnose debug application ssl
- diagnose debug application ustack
- diagnose debug cli

debug upload

Use this command to upload debug logs to an FTP server. This can be used if you want to view logs outside of the CLI, or if you need to provide debug log files to Fortinet Technical Support.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area.

Syntax

```
diagnose debug upload <delay_int> <delay_int> <delay_int> <delay_int>
```

Variable	Description	Default
<ftp_ipv4>	Enter the IP address or domain name of the FTP server.	No default.
<user_str>	Enter a valid user account name to log in to the FTP server.	No default.
<password_str>	Enter the password for the user account.	No default.
<upload-dir_str>	Enter the directory path on the FTP server where FortiWeb will upload files.	No default.

Example

```
diagnose debug upload 10.1.1.5 user1 1passw0Rd C:/uploads
```

Related topics

- diagnose debug
- execute db rebuild

hardware check

Use this command to check the appliance hardware for errors. (In the case of FortiWeb-VM, this command checks virtual hardware — the vCPUs.)

For example, to troubleshoot a logging problem, use the following command to check the log disk for errors:

```
diagnose hardware check logdisk
```

If the disk does not pass the check, it is likely the source of the problem.

Syntax

```
diagnose hardware check {all |cp8 |cpu |logdisk | memory |nic}
```

Variable	Description	Default
`{all |cp8 |cpu |logdisk | memory |nic}`	Enter the type of hardware to check, or enter `all` to check all hardware. For FortiWeb-VM versions, the `cp8` option is not available.	No default.

Example

The following command checks the log disk:

```
diagnose hardware check logdisk
```

Output similar to the following appears in the CLI:

```
logdisk check Pass
size Pass 1952
disk-number Pass 2
raid-level Pass raid1
```

hardware cpu

Use this command to display a list of hardware specifications on the FortiWeb appliance for CPUs. (In the case of FortiWeb-VM, this command displays virtual hardware information — the vCPUs.)

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
diagnose hardware cpu [list]
```

Example

```
diagnose hardware cpu list
```

Output similar to the following appears in the CLI:

```
processor : 0
vendor_id : GenuineIntel
cpu family : 6
model : 23
model name : Intel(R) Xeon(R) CPU E5405 @ 2.00GHz
stepping : 10
cpu MHz : 1995.056
cache size : 6144 KB
physical id : 0
```

```
siblings : 4
core id : 0
cpu cores : 4
fpu : yes
fpu_exception : yes
cpuid level : 13
wp : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36
    clflush dts acpi mmx fxsr sse sse2 ss ht tm syscall nx lm constant_tsc pni monitor ds_
    cpl vmx tm2 cx16 xtpr lahf_lm
bogomips : 3994.51
clflush size : 64
cache_alignment : 64
address sizes : 38 bits physical, 48 bits virtual
power management:
```

Related topics

- `diagnose system top`
- `diagnose hardware mem`
- `get system performance`

hardware fail-open

Fail-to-wire/bypass behavior is available for specific models only. See `config system fail-open`.

hardware harddisk

Use this command to display a list of hard disks and their capacity in megabytes (MB) in the FortiWeb appliance. (In the case of FortiWeb-VM, this will instead be for virtual hardware.)

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
diagnose hardware harddisk [list]
```

Example

```
diagnose hardware harddisk list
```

Output similar to the following appears in the CLI:

```
name size(M)
sda 625.56
sdb 32212.25
```

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 it does not appear, you can reboot and attempt to run a file system check to fix the file system and mount it.

Similarly FortiWeb 3000D shows:

```
name size(M)
sda 1999844.15
sdb 2055.21
```

Related topics

- `diagnose hardware logdisk info`
- `diagnose hardware raid list`
- `diagnose system flash`
- `diagnose system mount`
- `get system performance`

hardware interrupts

Use this command to display input/output (I/O) interrupt requests (IRQs) on the FortiWeb appliance. (In the case of FortiWeb-VM, this will instead be for virtual hardware.)

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
diagnose hardware interrupts [list]
```

Example

```
diagnose hardware interrupts list
```

Output similar to the following appears in the CLI:

```
CPU0
0: 225 IO-APIC-edge timer
1: 597 IO-APIC-edge i8042
2: 0 XT-PIC-XT-PIC cascade
12: 6 IO-APIC-edge i8042
14: 0 IO-APIC-edge ide0
15: 0 IO-APIC-edge ide1
16: 151462 IO-APIC-fasteoi vmxnet ether
17: 1080446 IO-APIC-fasteoi ioc0, vmxnet ether
18: 357613 IO-APIC-fasteoi vmxnet ether
19: 150107 IO-APIC-fasteoi vmxnet ether
```

```
NMI: 0 Non-maskable interrupts
LOC: 103791489 Local timer interrupts
SPU: 0 Spurious interrupts
PMI: 0 Performance monitoring interrupts
IWI: 0 IRQ work interrupts
RES: 0 Rescheduling interrupts
CAL: 0 Function call interrupts
TLB: 0 TLB shootdowns
MCE: 0 Machine check exceptions
MCP: 346 Machine check polls
ERR: 0
MIS: 0
```

Related topics

- `get system performance`

hardware logdisk info

Use this command to display the capacity, partitions, mount status, and RAID level (if any) of the hard disk FortiWeb uses to store logs and other data. For FortiWeb-VM, information for virtual hardware (the vDisk) is displayed.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
diagnose hardware logdisk info
```

Example

This example shows normal output for a FortiWeb-VM installation: there is no RAID, and it has been allocated a 40 GB vDisk. If the disk were mounted as read-only, this would indicate that the disk had failed to mount normally, and would be the cause if no new log messages were being recorded.

```
diagnose hardware logdisk info
```

The CLI displays output that is similar to the following:

```
disk number: 1
disk[0] size: 31.46GB
raid level: no raid exists
partition number: 1
mount status: read-write
```

Related topics

- `diagnose hardware harddisk`
- `diagnose log`

- diagnose system mount
- get system performance

hardware mem

Use this command to display the usage statistics of ephemeral memory (RAM), including swap pages and shared memory (Shmem), on the FortiWeb appliance. (In the case of FortiWeb-VM, this will instead be for virtual hardware — the vRAM.)

To use this command, your administrator account's access control profile must have at least r permission to the sysgrp area. For more information, see Permissions on page 74.

Syntax

```
diagnose hardware mem [list]
```

Example

```
diagnose hardware mem list
```

Output similar to the following appears in the CLI:

```
MemTotal: 1026808 kB
MemFree: 397056 kB
Buffers: 121248 kB
Cached: 86112 kB
SwapCached: 0 kB
Active: 324664 kB
Inactive: 66608 kB
Active(anon): 186544 kB
Inactive(anon): 8856 kB
Active(file): 138120 kB
Inactive(file): 57752 kB
Unevictable: 46008 kB
Mlocked: 46008 kB
SwapTotal: 0 kB
SwapFree: 0 kB
Dirty: 1564 kB
Writeback: 0 kB
AnonPages: 229920 kB
Mapped: 12632 kB
Shmem: 11488 kB
Slab: 36564 kB
SReclaimable: 6552 kB
SUnreclaim: 30012 kB
KernelStack: 640 kB
PageTables: 8820 kB
NFS_Unstable: 0 kB
Bounce: 0 kB
WritebackTmp: 0 kB
CommitLimit: 513404 kB
Committed_AS: 1216900 kB
VmallocTotal: 34359738367 kB
```

```
VmallocUsed: 38960 kB
VmallocChunk: 34359682723 kB
DirectMap4k: 8192 kB
DirectMap2M: 1040384 kB
```

Related topics

- diagnose policy
- diagnose system flash
- diagnose system top
- get system performance

hardware nic

Use this command to display a list of hardware specifications for the network interface card (NIC) physical ports on the FortiWeb appliance. (In the case of FortiWeb-VM, this will instead be for virtual hardware — the vNICs — and therefore the driver will be a virtual driver such as `vmxnet`, and the interrupt will be a virtual IRQ address.)

If the FortiWeb's network hardware has failed, this command can help to detect it. For example, if you know that the network cable is good and the configuration is correct, but this command displays `Link detected: no`), the physical network port may be broken.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
diagnose hardware nic [list [<interface_name>]]
```

Variable	Description	Default

[<interface_name>]	Optionally, type the name of a physical network interface, such as `port1`, to display its link status, configuration, hardware information, status, and connectivity statistics such as collision errors.
	If you omit the name of a NIC port, the CLI returns a list of all physical network interfaces, as well as the loopback interface (`lo`):
	`lo`
	`port1`
	`port2`
	`port3`
	`port4`
	Note: The detected physical link status from this command is **not** the same as its configured administrative status.
	For example, even though you have used config system interface to configure port1 with `set status down`, if the cable is physically plugged in, `diagnose hardware nic list port1` will indicate correctly that the link is up (`Link detected: yes`).
		No default.

Example

```
diagnose hardware nic list
```

Output similar to the following appears in the CLI:

```
driver vmxnet
version 2.0.9.0
firmware-version N/A
bus-info 0000:00:11.0

Supported ports TP
Supported link modes 1000baseT/Full
Supports auto-negotiation: No
Advertised link modes: Not reported
Advertised auto-negotiation: No

Speed: 1000Mb/s
Duplex: Full
Port: Twisted Pair
PHYAD 0
Transceiver: internal
Auto-negotiation off
Link detected yes

Link encap Ethernet
HWaddr 00:0C:29:FE:2B:47
INET addr 10.1.1.221
Bcast 10.1.1.221
```

```
Mask 255.255.255.255
FLAG UP BROADCAST RUNNING MULTICAST
MTU 1500
MEtric 1
Outfill 0
Keepalive 6846704

Interrupt 18
Base address 0x1400

RX packets 171487
RX errors 167784
RX dropped 0
RX overruns 0
RX frame 0
TX packets 202724
TX errors 0
TX dropped 0
TX overruns 0
TX carrier 0
TX collisions 0
TX queuelen 1000
RX bytes 72772373 (69.4 Mb)
TX bytes 32288070 (30.7 Mb)
```

Related topics

- `config system interface`
- `diagnose debug application ustack`
- `diagnose hardware interrupts`
- `diagnose network ip`
- `diagnose network sniffer`
- `diagnose network tcp list`
- `diagnose network udp list`
- `diagnose system ha mac`
- `execute traceroute`
- `get system performance`

hardware raid list

Use this command to run a diagnostic test of each hard disk in the RAID array that FortiWeb has. It also displays the capacity and RAID level. (Because FortiWeb-VM has no RAID, this command is not applicable to it.)

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
diagnose hardware raid list
```

Example

```
diagnose hardware raid list
```

Output similar to the following (from a FortiWeb 3000D) appears in the CLI window:

```
disk-number size(M) level
0(OK),1(OK), 1877274 raid1
```

Related topics

- config system raid
- diagnose hardware harddisk
- diagnose system mount
- execute create-raid level
- execute create-raid rebuild
- get system performance

index

Use this command to view (`list`) or clear logs, or to examine (`show`) or configure logs.

To use this command, your administrator account's access control profile must have `rw` or `w` permission to the `loggrp` area. For more information, see Permissions on page 74.

Syntax

```
diagnose index all show
diagnose index all clear
diagnose index {alog | dlog | elog | tlog} clear
diagnose index {alog | dlog | elog | tlog} list <index_int>
diagnose index {alog | dlog | elog | tlog} set <queue_int>
diagnose index {alog | dlog | elog | tlog} show
```

Variable	Description	Default
`index {alog | dlog | elog | tlog}`	Select which log files to view or affect: • `alog` — Attack logs. • `dlog` — Debug logs. • `elog` — Event logs. • `tlog` — Traffic logs.	No default.
`list <index_int>`	Type the number of most recent logs to display.	No default.
`set <queue_int>`	Type the maximum length of the log before it is flushed and written to disk. The valid range is from 0 to 32768.	No default.

Example

This example displays a list of logs processed.

```
diagnose index all show
```

Related topics

- config log attack-log
- config log event-log
- config log traffic-log
- diagnose debug
- diagnose hardware logdisk info

log

Use this command to view (list) or clear log messages, or to examine (show) or configure logging queues.

To use this command, your administrator account's access control profile must have rw or w permission to the loggrp area. For more information, see Permissions on page 74.

Syntax

```
diagnose log {all | alog | dlog | elog | tlog} [show | start | stop]
```

Variable	Description	Default
log {all | alog | dlog | elog | tlog}	Select which log files to view: • all — All logs. • alog — Attack logs. • dlog — Debug logs. • elog — Event logs. • tlog — Traffic logs.	No default.
[show | start | stop]	Displays the log messages or specifies a time to start or stop logging.	

Example

This example sets a time to start the display of log messages, displays log information starting at that time, and stops the display of log messages. The appliance's responses are displayed in **bold**.

```
FortiWeb # dia log all start
start tracking log
FortiWeb # dia log all show
      time span starts from 2014-07-31 18:31:53.000000
         Total time span is 10.754097 seconds
         Time spent on waiting is 10.527346 seconds
```

```
            Time spent on preprocessing is 0.000000 seconds
            event log processed: 0
            traffic log processed: 0
            attack log processed: 0
    FortiWeb # dia log all stop
    stop tracking log
```

Related topics

- config log attack-log
- config log event-log
- config log traffic-log
- diagnose debug
- diagnose hardware logdisk info

network arp

Use this command to add or delete an address resolution protocol (ARP) table entry, or to display the ARP table. The ARP table is used to resolve the IP addresses that correspond to a network interface card's physical MAC address, thereby determining which IP addresses can be reached directly through a link.

To use this command, your administrator account's access control profile must have `rw` or `w` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
diagnose network arp add <delay_int> <delay_int> <delay_int>
diagnose network arp delete <delay_int> <delay_int> <delay_int>
diagnose network arp list
```

Variable	Description	Default
<interface_name>	Type the name of the interface to add or delete from the ARP table.	No default.
{<interface_ipv4> | interface_ipv6>}	Type the IP address of the interface.	No default.
<mac-address_hex>	Type the MAC address of the interface.	No default.

Example

This example displays a list of ARP table entries and then deletes one.

```
diagnose network arp list
   IP address HW type Flags HW address Mask Device
   172.20.120.29 0x1 0x2 00:13:72:38:72:21 * port1
   172.20.120.26 0x1 0x2 00:26:2D:24:B7:D3 * port2
diagnose network arp delete port2 172.20.120.26 00:26:2D:24:B7:D3
```

Related topics

- diagnose network route
- diagnose network ip
- config router static
- config system interface

network ip

Use these commands to add or delete a network interface, loopback interface, or virtual server (which functions somewhat like a virtual network interface) IP address, or to list the table of network interface IPs.

Back up the configuration before deleting a network interface table entry (see execute backup full-config). FortiWeb presents no confirmation message, and in some cases such as the loopback interface, provides no undelete mechanism.

To use this command, your administrator account's access control profile must have rw or w permission to the sysgrp area. For more information, see Permissions on page 74.

Syntax

```
diagnose network ip add <interface_name> {<interface_ipv4> | interface_ipv6}
    {<interface_ipv4mask> |<interface_v6mask>}
diagnose network ip delete <interface_name> {<interface_ipv4> | interface_ipv6}
diagnose network ip list
```

Variable	Description	Default
<interface_name>	Type the name of the interface to add or delete from the network interface table.	No default.
{<interface_ipv4> | interface_ipv6}	Type the IP address of the network interface.	No default.
{<interface_ipv4mask> |<interface_v6mask>}	Type the subnet mask.	No default.

Example

This example displays a list of enabled network interfaces, including the loopback (lo)

```
diagnose network ip list
```

Output:

```
1 IP 127.0.0.1/255.255.255.0 lo
2 IP 172.20.120.47/255.255.255.0 port1
2 IP 10.1.1.221/255.255.255.255 port1
```

```
4 IP 192.168.1.27/255.255.255.0 port3
```

Example

This example deletes the IP of a virtual server on port2.

```
diagnose network ip delete port1 10.1.1.221
```

Related topics

- diagnose network route
- diagnose network arp
- config system interface

network route

Use this command to add or delete a route in the routing table, or to list the routing table.

Unlike router all, this command displays **all** individual entries, including automatically configured routes for the loopback interface (127.0.0.1) and VLANs, and also displays each route's priority. Unlike diagnose network rtcache, it displays all known routes, regardless of whether they have been recently used.

Do not delete routes unless you are sure. FortiWeb does not ask you to confirm the deletion, and there is no undelete mechanism. For example, if you accidentally delete a loopback interface route, you must recreate it manually.

To use this command, your administrator account's access control profile must have rw or w permission to the sysgrp area. For more information, see Permissions on page 74.

Syntax

```
diagnose network route add {<source_ipv4mask> | <source_ipv6mask>} <delay_int>
    {<destination_ipv4mask> | <destination_ipv6mask>} <delay_int> <delay_
    int><priority_int>
diagnose network route delete {<source_ipv4mask> | <source_ipv6mask>} <delay_int>
    {<destination_ipv4mask> | <destination_ipv6mask>} <delay_int> <delay_int>
    <priority_int>
```

Variable	Description	Default
{<source_ipv4mask> | <source_ipv6mask>}	Type the IP address and network mask of the source, separated by a space.	No default.
<interface_name>	Type the name of the interface to add or delete from the routing table.	No default.
{<destination_ipv4mask> | <destination_ipv6mask>}	Type the IP address and network mask of the source, separated by a space.	No default.

Variable	Description	Default
{<gateway_ipv4> | <gateway_ipv6>}	Enter the IP address of the next hop router (sometimes called a gateway) to which this route sends packets.	No default.
<priority_int>	Enter the priority of the route in the routing table. The lower the number the higher the priority. The value can be an integer from 1 to 255.	0

Example

This example displays the routing table.

```
tab=255 0.0.0.0/0.0.0.0/0->192.168.1.0/32/4 gwy=0.0.0.0 prio=0 prefsrc=192.168.1.27 type=3
    scope=fd proto=2
tab=255 0.0.0.0/0.0.0.0/0->172.20.120.0/32/2 gwy=0.0.0.0 prio=0 prefsrc=172.20.120.47
    type=3 scope=fd proto=2
tab=255 0.0.0.0/0.0.0.0/0->10.1.1.221/32/2 gwy=0.0.0.0 prio=0 prefsrc=10.1.1.221 type=2
    scope=fe proto=2
tab=255 0.0.0.0/0.0.0.0/0->10.1.1.221/32/2 gwy=0.0.0.0 prio=0 prefsrc=10.1.1.221 type=3
    scope=fd proto=2
tab=255 0.0.0.0/0.0.0.0/0->127.0.0.255/32/1 gwy=0.0.0.0 prio=0 prefsrc=127.0.0.1 type=3
    scope=fd proto=2
tab=255 0.0.0.0/0.0.0.0/0->192.168.1.255/32/4 gwy=0.0.0.0 prio=0 prefsrc=192.168.1.27
    type=3 scope=fd proto=2
tab=255 0.0.0.0/0.0.0.0/0->192.168.1.27/32/4 gwy=0.0.0.0 prio=0 prefsrc=192.168.1.27
    type=2 scope=fe proto=2
tab=255 0.0.0.0/0.0.0.0/0->172.20.120.255/32/2 gwy=0.0.0.0 prio=0 prefsrc=172.20.120.47
    type=3 scope=fd proto=2
tab=255 0.0.0.0/0.0.0.0/0->172.20.120.47/32/2 gwy=0.0.0.0 prio=0 prefsrc=172.20.120.47
    type=2 scope=fe proto=2
tab=255 0.0.0.0/0.0.0.0/0->127.0.0.0/32/1 gwy=0.0.0.0 prio=0 prefsrc=127.0.0.1 type=3
    scope=fd proto=2
tab=255 0.0.0.0/0.0.0.0/0->127.0.0.1/32/1 gwy=0.0.0.0 prio=0 prefsrc=127.0.0.1 type=2
    scope=fe proto=2
tab=255 0.0.0.0/0.0.0.0/0->127.0.0.0/24/1 gwy=0.0.0.0 prio=0 prefsrc=127.0.0.1 type=2
    scope=fe proto=2
tab=254 0.0.0.0/0.0.0.0/0->192.168.1.0/24/4 gwy=0.0.0.0 prio=0 prefsrc=192.168.1.27 type=1
    scope=fd proto=2
tab=254 0.0.0.0/0.0.0.0/0->172.20.120.0/24/2 gwy=0.0.0.0 prio=0 prefsrc=172.20.120.47
    type=1 scope=fd proto=2
tab=254 0.0.0.0/0.0.0.0/0->0.0.0.0/0/2 gwy=172.20.120.2 prio=2 prefsrc=0.0.0.0 type=1
    scope=00 proto=14
```

Example

This example adds a route to the routing table.

```
diagnose network route add 10::/64 port1 10:200::1/64 port1 10::1 0
```

Related topics

- get router all
- execute ping

- execute ping6
- execute traceroute
- diagnose network rtcache
- config router static

network rtcache

Use this command to display the routing cache.

Unlike diagnose network route, this command displays the cache of the most recently used routes, **not** necessarily the entire configuration. (You may have configured many routes, and these configurations will be saved to disk and appear in diagnose network route, but rarely used ones will **not** usually appear in the route cache, which keeps recently used routes in RAM for performance reasons.)

To use this command, your administrator account's access control profile must have rw or w permission to the sysgrp area. For more information, see Permissions on page 74.

Syntax

```
diagnose network rtcache list
```

Example

This example displays the ARP cache.

```
172.20.120.52(port1)->255.255.255.255(lo) via 0.0.0.0, pri 0 prot 0 scope 0, ref 0 lastuse
    3181 expires 0 error 0 used 855
172.20.120.100(port3)->172.20.120.255(lo) via 0.0.0.0, pri 0 prot 0 scope 0, ref 0 lastuse
    434 expires 0 error 0 used 0
172.20.120.230(port1)->255.255.255.255(lo) via 0.0.0.0, pri 0 prot 0 scope 0, ref 0
    lastuse 47386 expires 0 error 0 used 7
10.0.1.1(none)->10.0.1.1(lo) via 0.0.0.0, pri 0 prot 0 scope 0, ref 0 lastuse 223 expires
    0 error 0 used 29551
0.0.0.0(none)->10.0.1.1(lo) via 0.0.0.0, pri 0 prot 0 scope 0, ref 0 lastuse 223 expires 0
    error 0 used 7387
::(none)->::1(lo) via ::, pri 0 prot 0 scope 0 ref 1 lastuse 155845 expires 0 error 0 used
    417
::(none)->2607:f0b0:f:420:20c:29ff:fe4d:3ad3(lo) via ::, pri 0 prot 0 scope 0 ref 1
    lastuse 354923 expires 0 error 0 used 1
::(none)->2607:f0b0:f:420:20c:29ff:fe4d:3ae7(lo) via ::, pri 0 prot 0 scope 0 ref 1
    lastuse 2590615 expires 0 error 0 used 0
::(none)->2607:f0b0:f:420:20c:29ff:fe4d:3af1(lo) via ::, pri 0 prot 0 scope 0 ref 1
    lastuse 2590615 expires 0 error 0 used 0
::(none)->2607:f0b0:f:420::(port1) via ::, pri 256 prot 0 scope 0 ref 0 lastuse 2590616
    expires 214715722 error 0 used 0
::(none)->ff00::(port4) via ::, pri 256 prot 0 scope 0 ref 0 lastuse 2590615 expires 0
    error 0 used 0
::(none)->ff00::(lo) via ::, pri -1 prot 0 scope 0 ref 1 lastuse 449431651 expires 0 error
    -101 used 1
```

Example

This example adds a route to the routing table.

```
diagnose network route add vlan2 160.1.12.0 255.0.0.0 172.20.01.169 32 3 verify
```

Related topics

- get router all
- execute ping
- execute ping6
- execute traceroute
- diagnose network route
- config router static

network sniffer

Use this command to perform a packet trace on one or more network interfaces.

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. Packet capture output appears on your CLI display until you stop it by pressing Ctrl+C, or until it reaches the number of packets that you have specified to capture.

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.

If your FortiWeb model uses Data Plane Development Kit (DPDK) for packet processing (for example, models 3000E, 3010E and 4000E) and is operating in offline protection mode, you cannot use this command with ports that are configured as data capture ports. To use the command with this type of port, disable the corresponding server policy or configure the policy with a different data capture port.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
diagnose network sniffer [{any | <interface_name>} [{none | '<filter_str>'} [{1 |
    2 | 3} [<packets_int>]]]]
```

Variable	Description	Default
{any | <interface_name>}	Type the name of a network interface whose packets you want to capture, such as port1, or type any to capture packets on all network interfaces. If you omit this and the following parameters for the command, the command captures all packets on all network interfaces.	No default.
{none | '<filter_str>'}	Type either none to capture all packets, or type a filter that specifies which protocols and port numbers that you do or do not want to capture, such as 'tcp port 25'. Surround the filter string in quotes ('). Filters use tcpdump syntax: '[[src|dst] host {<host1_fqdn> | <host1_ipv4>}] [and|or] [[src|dst] host {<host2_fqdn> | <host2_ipv4>}] [and|or] [[arp|ip|gre|esp|udp|tcp] port <port1_int>] [and|or] [[arp|ip|gre|esp|udp|tcp] port <port2_int>]' To display only the traffic between two hosts, specify the IP addresses of both hosts. To display only forward or reply packets, indicate which host is the source, and which is the destination. For example, to display UDP port 1812 traffic between 1.example.com and either 2.example.com or 3.example.com, you would enter: 'udp and port 1812 and src host 1.example.com and dst \(2.example.com or 2.example.com \)'	none

Variable	Description	Default
{1 | 2 | 3}	Type one of the following integers indicating the depth of packet headers and payloads to capture: • 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) • fragment offset • options bits • 2 — All of the output from 1, plus the packet payload in both hexadecimal and ASCII. • 3 — All of the output from 2, plus the the link layer (Ethernet) header. For troubleshooting purposes, Fortinet Technical Support may request the most verbose level (3).	1
<packets_int>	Type the number of packets to capture before stopping. If you do not specify a number, the command will continue to capture packets until you press Ctrl+C.	Packet capture continues until you press Ctrl + C.

Example

The following example captures three packets of traffic from any port number or protocol and between any source and destination (a filter of none), which passes through the network interface named port1. The capture uses a

low level of verbosity (indicated by `1`).

Commands that you would type are highlighted in bold; responses from the FortiWeb appliance are not bolded.

```
FortiWeb# diagnose network sniffer port1 none 1 3
filters=[none]
0.918957 192.168.0.1.36701 -> 192.168.0.2.22: ack 2598697710
0.919024 192.168.0.2.22 -> 192.168.0.1.36701: psh 2598697710 ack 2587945850
0.919061 192.168.0.2.22 -> 192.168.0.1.36701: psh 2598697826 ack 2587945850
```

If you are familiar with the TCP protocol, you may notice that the packets are from the middle of a TCP connection. Because port 22 is used (highlighted above in bold), which is the standard port number for SSH, the packets might be from an SSH session.

Example

The following example captures packets traffic on TCP port 80 (typically HTTP) between two hosts, 192.168.0.1 and 192.168.0.2. The capture uses a low level of verbosity (indicated by `1`). Because the filter does not specify either host as the source or destination in the IP header (`src` or `dst`), the sniffer captures both forward and reply traffic.

Commands that you would type are highlighted in bold; responses from the FortiWeb appliance are not bolded.

```
FortiWeb# diagnose network sniffer packet port1 'host 192.168.0.2 or host 192.168.0.1 and
    tcp port 80' 1
```

A specific number of packets to capture is not specified. As a result, the packet capture continues until the administrator presses Ctrl+C. The sniffer then confirms that five packets were seen by that network interface. Below is a sample output.

```
192.168.0.2.3625 -> 192.168.0.1.80: syn 2057246590
192.168.0.1.80 -> 192.168.0.2.3625: syn 3291168205 ack 2057246591
192.168.0.2.3625 -> 192.168.0.1.80: ack 3291168206
192.168.0.2.3625 -> 192.168.0.1.80: psh 2057246591 ack 3291168206
192.168.0.1.80 -> 192.168.0.2.3625: ack 2057247265
5 packets received by filter
0 packets dropped by kernel
```

Example

The following example captures 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`).

The number of packets to capture is not specified, so the packet capture continues until the administrator presses Ctrl+C. The sniffer then states how many 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.

Commands that you would type are highlighted in bold; responses from the FortiWeb appliance are not bolded.

```
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............
```

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 in 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

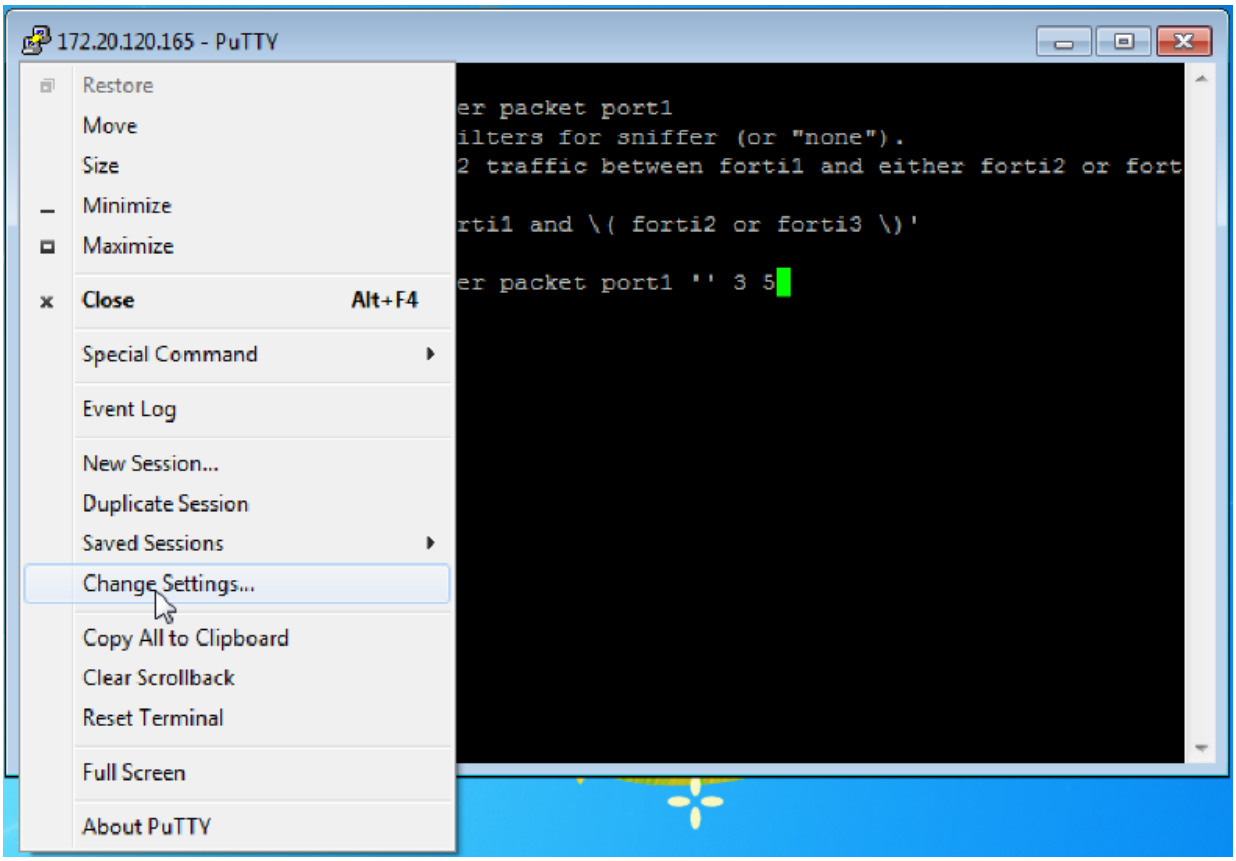
- terminal emulation software such as PuTTY
- a plain text editor such as Notepad
- a Perl interpreter
- network protocol analyzer software such as Wireshark

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 Connecting to the CLI on page 61.
3. Type the packet capture command, such as:

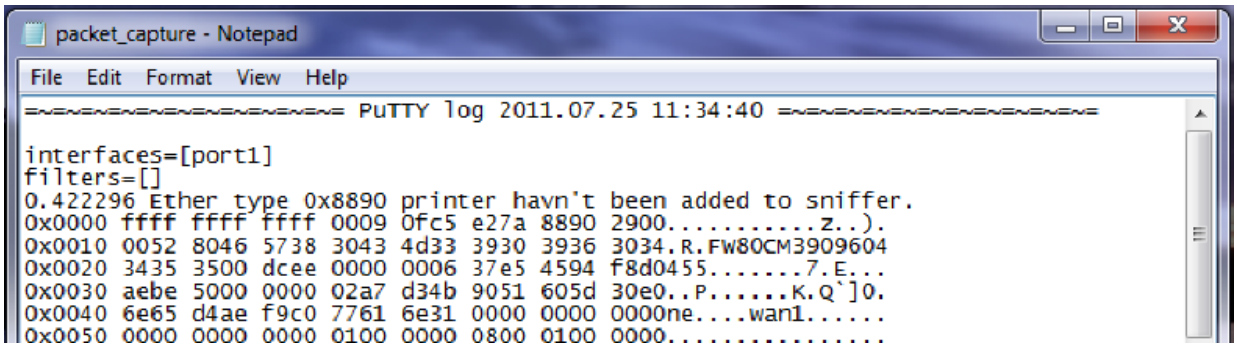
   ```
   diag network sniffer packet port1 'tcp port 443' 3 100
   ```

   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 FortiMail 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 2016/9/29.07.25 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 Ethereal) 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:

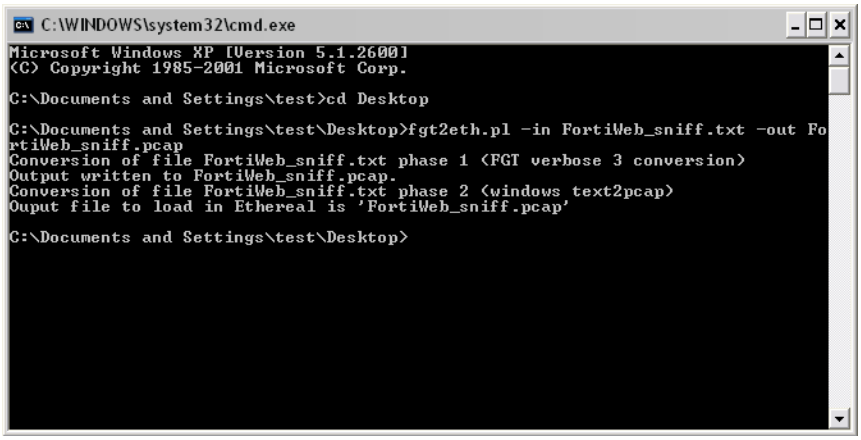
Methods to open a command prompt vary by operating system.
On Windows XP, go to **Start > Run** and enter `cmd`.
On Windows 7, click the Start (Windows logo) menu to open it, then enter `cmd`.

```
fgt2eth.pl -in packet_capture.txt -out packet_capture.pcap
```

where:

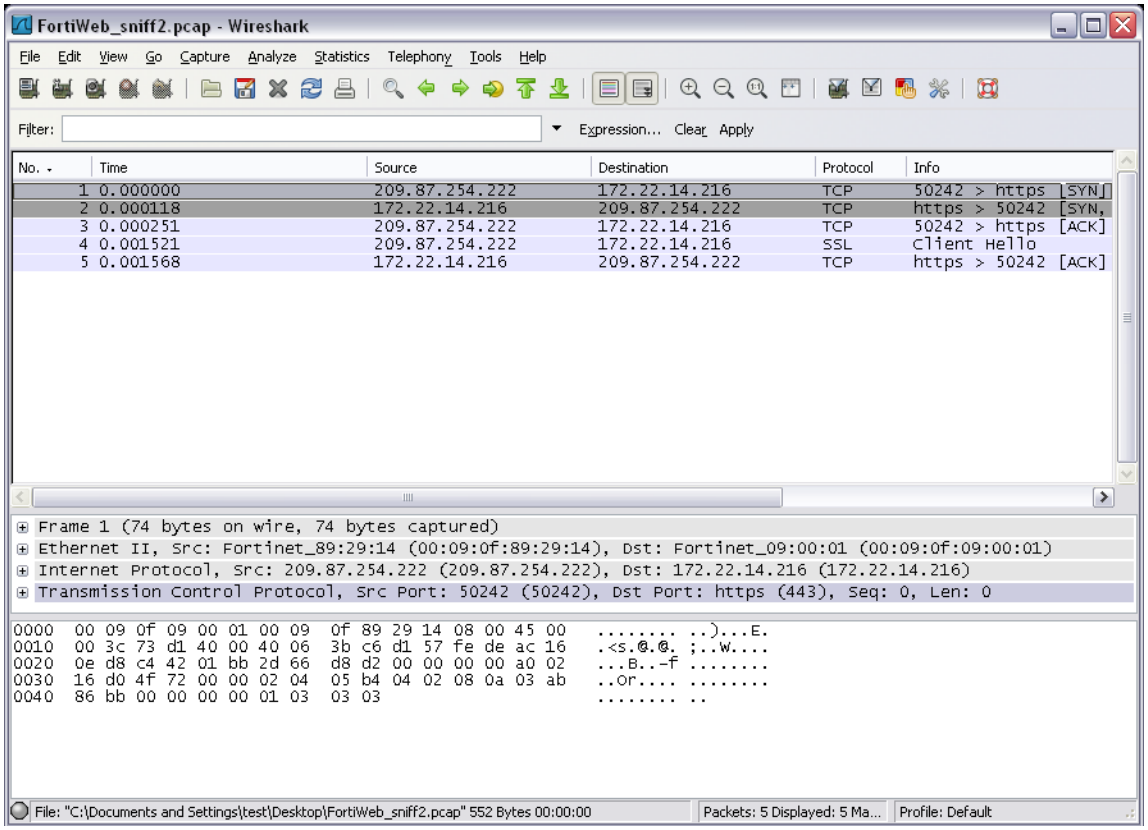
- `fgt2eth.pl` is the name of the conversion script; include the path relative to the current directory, which is indicated by the command prompt
- `packet_capture.txt` is the name of the packet capture's output file; include the directory path relative to your current directory
- `packet_capture.pcap` 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

Converting sniffer output to .pcap format



15. Open the converted file in your network protocol analyzer application. For further instructions, see the documentation for that application.

Viewing sniffer output in Wireshark



For additional information on packet capture, see the Fortinet Knowledge Base article Using the FortiOS built-in packet sniffer.

network tcp list

Use this command to view a list of TCP raw socket details, including:

- `sl` — Kernel socket hash slot.
- `local_address` — IP address and port number pair of the local FortiWeb network interface in hexadecimal, such as `DD01010A:0050`.
- `rem_address` — Remote host's network interface and port number pair. If not connected, this will contain `00000000:0000`.
- `st` — TCP state code (e.g. `OA` for listening, `01` for established, or `06` for timeout wait)
- `tx_queue` — Kernel memory usage by the transmission queue.
- `rx_queue` — Kernel memory usage by the retransmission queues.
- `tr`, `tm-> when`, `retrnsmt` — Kernel socket state debugging information.
- `uid` — User ID of the socket's creator (on FortiWeb, always `0`).
- `timeout` — Connection timeout.
- `inode` — Pseudo-file system i-node of the process.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
diagnose network tcp list
```

Example

```
diagnose network tcp list
sl local_address rem_address st tx_queue rx_queue tr tm->when retrnsmt uid timeout inode
0: DD01010A:0050 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 333597 1
    ffff88003b825880 299 0 0 2 -1
1: 2F7814AC:0050 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 228018 1
    ffff88003b824680 299 0 0 2 -1
2: 1B01A8C0:0050 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 2692 1
    ffff88003b6ec6c0 299 0 0 2 -1
3: 0100007F:0050 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 2691 1
    ffff88003b6eccc0 299 0 0 2 -1
4: 00000000:0016 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 2433 1
    ffff88003b489280 299 0 0 2 -1
5: 00000000:0017 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 2400 1
    ffff88003b489880 299 0 0 2 -1
6: 0100007F:22B8 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 2687 1
    ffff88003b488680 299 0 0 2 -1
7: DD01010A:01BB 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 333598 1
    ffff88003bbf3940 299 0 0 2 -1
8: 2F7814AC:01BB 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 228017 1
    ffff88003b824080 299 0 0 2 -1
9: 1B01A8C0:01BB 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 2689 1
    ffff88003b6ed8c0 299 0 0 2 -1
10: 0100007F:01BB 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 2688 1
    ffff88003b488080 299 0 0 2 -1
11: 00000000:208D 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 2441 1
    ffff88003b488c80 299 0 0 2 -1
```

```
12: 2F7814AC:0016 E17814AC:FEF2 01 00000000:00000000 02:000909FE 00000000 0 0 272209 4
    ffff88003bbf2d40 20 3 1 5 -1
```

Related topics

- diagnose network arp
- diagnose network ip
- diagnose debug application ustack

network udp list

Use this command to view a list of UDP raw socket details, including:

- sl — Kernel socket hash slot.
- local_address — IP address and port number pair of the local FortiWeb network interface in hexadecimal, such as DD01010A:0050.
- rem_address — Remote host's network interface and port number pair. If not connected, this will contain 00000000:0000.
- st — TCP state code in hexadecimal (e.g. 0A for listening, 01 for connection established, or 06 for waiting for data)
- tx_queue — Kernel memory usage by the transmission (Tx) queue.
- rx_queue — Kernel memory usage by the retransmission (Rx) queues. (This is not used by UDP, since the protocol itself does not support retransmission.)
- tr, tm-> when, retrnsmt — Kernel socket state debugging information. (These are not used by UDP, since the protocol itself does not support retransmission.)
- uid — User ID of the socket's creator (on FortiWeb, always 0).
- timeout — Connection timeout.
- inode — Pseudo-file system inode of the process.
- ref, pointer — Pseudo-file system references.

To use this command, your administrator account's access control profile must have at least r permission to the sysgrp area. For more information, see Permissions on page 74.

Syntax

```
diagnose network udp list
```

Example

```
diagnose network udp list
sl local_address rem_address st tx_queue rx_queue tr tm->when retrnsmt uid timeout inode
    ref pointer drops
307: 00000000:00A1 00000000:0000 07 00000000:00000000 00:00000000 00000000 0 0 2498 2
    ffff88003acba080 0
447: 00000000:3F2D 00000000:0000 07 00000000:00000000 00:00000000 00000000 0 0 2874 2
    ffff88003acbac80 0
```

Related topics

- `diagnose network arp`
- `diagnose network ip`
- `diagnose debug application ustack`

policy

Use this command to view the process ID, live sessions, and traffic statistics associated with a server policy.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
diagnose policy pserver list <policy_name>
diagnose policy session {list <policy_name>}
diagnose policy traffic {list <policy_name>}
diagnose policy traffic {list <policy_name>}
diagnose policy period-blockip {list <policy_name>}
diagnose policy period-blockip {delete <policy_name>}{ipv4 | ipv6}
```

Variable	Description	Default
`pserver list <policy_name>`	Displays the status of physical servers covered by the policy.	No default.
`session {list <policy_name>}`	Displays IP session information for TCP and UDP connections.	No default.
`traffic {list <policy_name>}`	Displays traffic throughput (bandwidth usage) information.	No default.
`period-blockip {list <policy_name>}`	Displays client IP addresses whose requests are temporarily blocked because the client violated a rule in the specified policy with an **Action** value of **Period Block**.	No default.
`period-blockip {delete <policy_name>}{ipv4 | ipv6}`	Unblocks the specified client IP address that FortiWeb has blocked because it violated a rule in the specified policy with an **Action** value of **Period Block**. (FortiWeb can still block the address because it violates a rule in a different policy.)	No default.
`<policy_name>`	Type the name of an existing server policy.	No default.

Example

This example shows the output of the `pserver list` command. The `alive` value indicates the status of the server health check:

Server health check (`alive`) values

Integer	Health check status	Health Check Status icon in Policy Status dashboard
0	failed	red
1	passed	green
2	disabled	grey

```
diagnose policy pserver list Policy1
policy(Policy1)
server-pool(FWB_server_pool):
total = 1
server[0]
id: 1
ip: 10.20.1.22
port: 80
alive: 2
session: 0
status: 1
```

Related topics

- `config server-policy policy`
- `diagnose network ip`
- `diagnose debug flow filter`
- `get system performance`

system flash

Use this command to change the currently active firmware partition or to display partition information stored on the flash drive.

FortiWeb appliances have 2 partitions that each contain a firmware image: one is the primary and one is the backup. If the FortiWeb appliance is unable to successfully boot using the primary firmware partition, it may boot using the alternative firmware partition. The second partition can contain another version of the firmware.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see Permissions on page 74.

Syntax

```
diagnose system flash default <partition_int>
```

```
diagnose system flash list
```

Variable	Description	Default
<partition_int>	Type the number of the partition that will be used as the primary firmware partition during the **next** reboot or startup. The other partition will become the backup firmware partition.	No default.

Example

This example lists the partition settings.

```
diagnose system flash list
```

Below is a sample output.

```
Image# Version TotalSize(KB) Used(KB) Use% Active
1 FV-1KB-4.30-FW-build0521-110120 38733 33125 86% No
2 FV-1KB-4.30-FW-build0522-110112 38733 33125 86% Yes
3 836612 16980 2 % No
```

Related topics

- execute restore image
- get system status

system ha file-stat

Use this command to display the current status of FortiGuard subscription services files and the MD5 checksum for system and configuration files.

Syntax

```
diagnose system ha file-stat
```

Example

Below is a sample output.

```
FortiWeb Security Service:
      1970-01-01 expired
      Last Update Time: 1999-11-30 Method: Manual
      Signature Build Number-0.00109
FortiWeb Antivirus Service:
      1970-01-01 expired
      Last Update Time: 2011-12-07 Method: Manual
      Regular Virus Database Version-14.00922
      Extended Virus Database Version-14.00922
FortiWeb IP Reputation Service:
      1970-01-01 expired
      Last Update Time: 1999-11-30 Method: Manual
```

```
      Signature Build Number-1.00020
System files MD5SUM: B0EF0DBDA19A22296BA4000893B134B7
CLI files MD5SUM: 6C1F56E27BF995C83691A375838BCA24
```

Related topics

- execute ha disconnect
- execute ha manage
- diagnose system ha status
- get system status
- config system global

system ha mac

Use this command to display the virtual MAC addresses and link statuses of each network interface of appliances in the HA group.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
diagnose system ha mac
```

Example

This example indicates that the links are "up" (`linkfail=0`) for port1 and port3 on the currently active appliance in the HA pair. While operating in HA, the network interfaces are using a Layer 1 data link (MAC) address that begins with the hexadecimal string `00:09:0F:09:00:`.

```
diagnose system ha mac
```

Below is a sample output.

```
HA mac msg
name=port1, phyindex=0, 00:09:0F:09:00:01, linkfail=0
name=port2, phyindex=1, 00:09:0F:09:00:02, linkfail=1
name=port3, phyindex=2, 00:09:0F:09:00:03, linkfail=0
name=port4, phyindex=3, 00:09:0F:09:00:04, linkfail=1
```

Related topics

- execute ha disconnect
- execute ha manage
- diagnose system ha status
- get system status
- config system ha

system ha status

Use this command to display the HA group ID, as well as the serial number, role (active or standby), and device priority of each appliance belonging to the HA cluster.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
diagnose system ha status
```

Example

This example lists the HA group ID, serial numbers, and device priorities.

```
diagnose system ha status
```

Below is a sample output.

```
HA information

Model=FV-1KD-5.30-FW-build0431, Mode=a-p Group=2 Debug=0

HA group member information: is_manage_master=1.
FV-1KD3A13800012, Master, 4, 0, 196417
FV-1KD3A13800091, Slave, 6, 0, 185787
```

In this example, in the information for `FV-1KD3A13800012, 4` is the priority of the appliance and `0` is the number of ports that have been down.

If the value of the priority or ports down is 100, the parameter is "invalid". For example, if the appliance has not yet joined the HA cluster.

Related topics

- `execute ha disconnect`
- `execute ha manage`
- `diagnose system ha status`
- `get system status`
- `config system global`

system ha sync-stat

Use this command to display the status of the high availability (HA) synchronization process.

Syntax

```
diagnose system ha sync-stat
```

Example

Below is a sample output.

```
FortiWeb Security Service:
      2016-01-02
      Last Update Time: 2014-08-11 Method: Manual
      Signature Build Number-0.00108
FortiWeb Antivirus Service:
      2016-01-02
      Last Update Time: 2014-08-11 Method: Manual
      Regular Virus Database Version-22.00639
      Extended Virus Database Version-22.00606
FortiWeb IP Reputation Service:
      2016-01-02
      Last Update Time: 2014-08-11 Method: Manual
      Signature Build Number-1.00708
System files MD5SUM: 3098ABBBFA3B21E119FEC7D8BBD744B6
CLI files MD5SUM: C2D40C9E43F4D7E5B9FC882E9ADE7484
```

Related topics

- `execute ha disconnect`
- `execute ha manage`
- `diagnose system ha status`
- `get system status`
- `config system global`

system kill

Use this command to terminate a process currently running on FortiWeb, or send another signal from the FortiWeb OS to the process.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see Permissions on page 74.

Syntax

```
diagnose system kill <delay_int> <delay_int>
```

Variable	Description	Default
<signal_int>	Type the ID of the signal to send to the process. This in an integer between 1 and 32. Some common signals are: • 1 — Varies by the process's interpretation, such as re-read configuration files or re-initialize (hang up; SIGHUP). For example, the FortiWeb web UI verifies its configuration files, then restarts gracefully. • 2 — Request termination by simulating the pressing of the interrupt keys, such as Ctrl + C (interrupt; SIGINT). • 3 — Force termination immediately and do a core dump (quit; SIGQUIT). • 9 — Force termination immediately (kill; SIGKILL). • 15 — Request termination by inter-process communication (terminate; SIGTERM).	No default.
<pid_int>	Type the process ID where the signal is sent to. To list all current process IDs, use diagnose system top .	No default.

Related topics

- diagnose system top
- diagnose hardware cpu
- diagnose hardware mem
- get system performance

system mount

Use this command to display a list of mounted file systems, including their available disk space, disk usage, and mount locations.

To use this command, your administrator account's access control profile must have either w or rw permission to the mntgrp area. For more information, see Permissions on page 74.

Syntax

```
diagnose system mount list
```

Example

```
diagnose system mount list
```

Output from a FortiWeb 3000D:

```
Filesystem 1M-blocks Used Available Use% Mounted on
/dev/ram0 97 87 10 89% /
none 4823 0 4823 0% /tmp
none 16077 0 16077 0% /dev/shm
/dev/sdb1 189 45 134 25% /data
/dev/sdb3 961 17 895 1% /home
/dev/sda1 1877275 271 1781644 0% /var/log
```

Related topics

- diagnose hardware logdisk info
- diagnose hardware raid list

system top

Use this command to view a list of the most system-intensive processes and to change the refresh rate.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see Permissions on page 74.

Syntax

```
diagnose system top [<delay_int> [<delay_int>]]
```

Variable	Description	Default
<delay_int>	Type the process list refresh interval in seconds.	5
<max-lines>	Set the maximum number of top processes to display.	All processes are shown.

Once you execute this command, it continues to run and display in the CLI window until you enter `q` (quit).

While the command is running, you can press `Shift + P` to sort the five columns of data by CPU usage (the default) or `Shift + M` to sort by memory usage.

Example

This example displays a list of the top FortiWeb processes and sets the update interval at 10 seconds.

```
diagnose system top 10
```

Below is a sample output.

```
Run Time: 0 days, 0 hours and 48 minutes
0U, 0S, 100I; 1002T, 496F
xmlproxy 152 S 1.3 4.7
updated 54 S 0.1 0.3
monitord 57 S 0.1 0.3
sys_monito 58 S 0.1 0.3
```

```
xmlproxy 56 S 0.0 8.2
alertmail 76 S 0.0 4.6
cli 396 S 0.0 1.2
cli 301 S 0.0 1.2
cmdbsvr 43 S 0.0 1.0
httpsd 147 S 0.0 1.0
cli 403 R 0.0 0.9
data_analy 60 S 0.0 0.6
httpsd 308 S 0.0 0.6
cli 379 S 0.0 0.5
hasync 63 S 0.0 0.4
hatalk 62 S 0.0 0.4
synconf 64 S 0.0 0.4
al_daemon 59 S 0.0 0.3
miglogd 53 S 0.0 0.3
```

The first line indicates the up time. The second line lists the processor and memory usage, where the parameters from left to right mean:

- U — Percent of user CPU usage (in this case 0%)
- S — Percent of system CPU usage (in this case 0%)
- I — Percentage of CPU idle (in this case 100%)
- T — Total memory in kilobytes (in this case 2008 KB)
- F — Available memory in kilobytes (in this case 445 KB)

The five columns of data provide the process name (such as `updated`), the process ID (`pid`), the running status, the CPU usage, and the memory usage. The status values are:

- S — Sleeping (idle)
- R — Running
- Z — Zombie (crashed)
- < — High priority
- N — Low priority

Related topics

- `diagnose system kill`
- `diagnose hardware cpu`
- `diagnose hardware mem`
- `get system performance`

system update info

Use this command to display recent error messages and the following information about FortiGuard signatures, IP lists, and engine packages and the geography-to-IP mapping database:

- Current version
- Time of last update
- Next scheduled update time
- Previous version history

Syntax

```
diagnose system update info
```

Example

```
FortiWeb signature
----------
Version: 0.00146
Expiry Date: Thu Jan 01 1970
Last Update Date: Sat Dec 05 11:00:46 2015
Next Update Date: Wed Jan 13 11:00:00 2016

Historical versions
----------
0.00146
0.00144
0.00144
0.00144
0.00139

FortiWeb GEODB
----------
Version: GEO-533LITE 20141104
Expiry Date: N/A
Last Update Date: Tue Dec 01 10:53:35 2015
Next Update Date: N/A
Historical versions
----------
GEO-533LITE 20141007
N/A

Regular Antivirus
----------
Version: 30.00946
Expiry Date: Thu Mar 13 2014
Last Update Date: Sat Dec 05 11:03:30 2015
Next Update Date: Wed Jan 13 11:00:00 2016
Historical versions
----------
30.00859
30.00785
30.00698
29.00326
29.00302
29.00279
29.00256
14.00922

Extended Antivirus
----------
Version: 30.00871
Expiry Date: Thu Mar 13 2014
Last Update Date: Sat Dec 05 11:03:30 2015
Next Update Date: Wed Jan 13 11:00:00 2016
```

```
Historical versions
----------
30.00708
30.00540
29.00219
14.00922

IP Reputation
----------
Version: 2.00649
Expiry Date: Thu Jan 01 1970
Last Update Date: Sat Dec 05 11:00:46 2015
Next Update Date: Wed Jan 13 11:00:00 2016

Historical versions
----------
2.00642
2.00635
2.00628
2.00596
2.00594
2.00592
2.00590
1.00020

Latest errors
----------
Wed Jan 13 10:04:02 2016 Failed to establish connection with 192.168.100.205:443 when install
anti-virus packages.
Wed Jan 13 10:03:02 2016 Failed to establish connection with 192.168.100.205:443 when install
essential packages.
Wed Jan 13 10:02:00 2016 Failed to establish connection with 192.168.100.205:443 when install
anti-virus packages.
Wed Jan 13 10:01:00 2016 Failed to establish connection with 192.168.100.205:443 when install
essential packages.
Wed Jan 13 09:04:06 2016 Failed to establish connection with 192.168.100.205:443 when install
anti-virus packages.
Wed Jan 13 09:03:06 2016 Failed to establish connection with 192.168.100.205:443 when install
essential packages.
Wed Jan 13 09:02:04 2016 Failed to establish connection with 192.168.100.205:443 when install
anti-virus packages.
Wed Jan 13 09:01:04 2016 Failed to establish connection with 192.168.100.205:443 when install
essential packages.
Wed Jan 13 08:04:07 2016 Failed to establish connection with 192.168.100.205:443 when install
anti-virus packages.
Wed Jan 13 08:03:07 2016 Failed to establish connection with 192.168.100.205:443 when install
essential packages.
```

execute

The `execute` command has an immediate and decisive effect on your FortiWeb appliance and, for that reason, should be used with care. Unlike `config` commands, most `execute` commands do not result in any configuration change.

This chapter describes the following commands:

- `execute backup cli-config`
- `execute backup full-config`
- `execute certificate ca`
- `execute certificate crl`
- `execute certificate inter-ca`
- `execute certificate local`
- `execute create-raid level`
- `execute create-raid rebuild`
- `execute date`
- `execute db rebuild`
- `execute erase-disk`
- `execute factoryreset`
- `execute factoryreset`
- `execute formatlogdisk`
- `execute ha disconnect`
- `execute ha manage`
- `execute ha md5sum`
- `execute ha synchronize`
- `execute ping`
- `execute ping6`
- `execute ping-options`
- `execute ping6-options`
- `execute reboot`
- `execute restore config`
- `execute restore image`
- `execute restore secondary-image`
- `execute restore vmlicense`
- `execute session-cleanup`
- `execute shutdown`
- `execute telnet`
- `execute telnettest`
- `execute time`
- `execute traceroute`
- `execute update-now`

backup cli-config

Use this command to manually back up the configuration file to a TFTP server.

This method does **not** include uploaded files such as:

- private keys
- certificates
- error pages
- WSDL files
- W3C Schema
- vulnerability scan settings

If your configuration has these files, use either a full TFTP or FTP/SFTP backup instead. See `execute backup full-config` or `config system backup`.

This command does **not** include settings that remain at their default values for the currently installed version of the firmware. If you require a backup that includes those settings, instead use `execute backup full-config`.

Alternatively, you can back up the configuration to an FTP or SFTP server. See `config system backup`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute backup cli-config tftp <filename_str>  <tftp_ipv4> {entire | profile}
    [<password_str>]
```

Variable	Description	Default
`<filename_str>`	Type the name of the file to be used for the backup file, such as `FortiWeb_backup.conf`.	No default.
`<tftp_ipv4>`	Type the IP address of the TFTP server.	No default.
`{entire | profile}`	Select either: • `entire` — Back up the core configuration file only. **Note:** This is not literally the entire configuration. It only contains the core configuration file, comprised of a CLI script. It does **not** include uploaded files such as error pages and private keys. • `profile` — Back up only the web protection profiles.	

Variable	Description	Default
[<password_str>]	Type a password for use when encrypting the backup file using 128-bit AES. If you do not provide a password, the backup file will be stored as clear text. **Caution:** Remember the password or keep it in a secure location. You will be required to enter the same password when restoring an encrypted backup file. If you forget or lose the password, you will not be able to use that encrypted backup file.	No default.

Example

This example uploads the FortiWeb appliance's system configuration to a file named `fweb.cfg` on a TFTP server at IP address 192.168.1.23. The file will not be password-encrypted.

```
execute backup cli-config tftp fweb.cfg 192.168.1.23 entire
```

Related topics

- execute backup full-config
- execute restore config
- config system backup

backup full-config

Use this command to manually back up the entire configuration file, **including** those settings that remain at their default values, to a TFTP server.

Fortinet strongly recommends that you password-encrypt this backup, and store it in a secure location. This backup 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.

Alternatively, you can back up the configuration to an FTP or SFTP server. See config system backup.

This backup includes settings that remain at their default values increases the file size of the backup, but may be useful in some cases, such as when you want to compare the default settings with settings that you have configured.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute backup full-config tftp <filename_str>  <tftp_ipv4> [<password_str>]
```

Variable	Description	Default
<filename_str>	Type the name of the file to be used for the backup file, such as FortiWeb_backup.conf.	No default.
<tftp_ipv4>	Type the IP address of the TFTP server.	No default.
[<password_str>]	Type a password for use when encrypting the backup file using 128-bit AES. If you do not provide a password, the backup file will be stored as clear text. **Caution:** Remember the password or keep it in a secure location. You will be required to enter the same password when restoring an encrypted backup file. If you forget or lose the password, you will not be able to use that encrypted backup file.	No default.

Example

This example uploads the FortiWeb appliance's entire configuration, including uploaded error page and HTTPS certificate files, to a file named fweb.cfg on a TFTP server at IP address 192.168.1.23. The file is encrypted with the password P@ssword1.

```
execute backup full-config tftp fweb.cfg 192.168.1.23 P@ssword1
```

Related topics

- execute backup cli-config
- config system backup

certificate ca

Use this command to upload a trusted CA certificate.

Certificate authorities (CAs) validate and sign others' certificates. FortiWeb determines whether a client or device's certificate is genuine by comparing the CA's signature and the copy of the CA certificate that you have uploaded. If they are made by the same private key, the CA's signature is genuine, and therefore the client or device's certificate is legitimate.

Syntax

```
execute certificate ca import {tftp | auto} {<vdom_name> | root} <cert_name>
    {<tftp_ipv4> | <scep_url>} [<ca_id>]
```

Variable	Description	Default
{tftp | auto}	Use one of the following options to specify the location of the CA certificate: • tftp — From a TFTP server. • auto — From a SCEP (Simple Certificate Enrollment Protocol) server.	No default.
{<vdom_name> | root}	Specifies the administrative domain (ADOM) that the certificate applies to. If ADOMs are not enabled, specify root.	No default.
<cert_name>	If the certificate is located on a TFTP server, the name of the certificate file.	No default.
{<tftp_ipv4> | <scep_url>}	If the certificate is located on a TFTP server, the IP address of the server. If the source of the certificate is a SCEP server, the URL of the server.	No default.
<ca_id>	Optionally, if the source of the certificate is a SCEP server, you can use a CA identifier to specify a specific CA.	No default.

Example

This example uploads the trusted CA certificate file ca.cer from the TFTP server 192.168.1.23.

```
execute certificate ca import tftp root ca.cer 192.168.1.23
```

This example uploads the trusted CA certificate file from the SCAEP server at http://10.0.0.31/certsrv/mscep/mscep.dll.

Related topics

- config system certificate ca
- execute certificate crl
- execute certificate inter-ca
- execute certificate local

certificate crl

Use this command to install a Certificate Revocation List (CRL).

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).

Syntax

```
execute certificate crl import {tftp | auto | http} {<vdom_name> | root} <crl_name>
    {<tftp_ipv4> | <scep_url> | <http_url>}
```

Variable	Description	Default
`{tftp | auto | http}`	Use one of the following options to specify the location of the CRL to upload to FortiWeb: • `tftp` — A TFTP server. • `auto` — A SCEP (Simple Certificate Enrollment Protocol) server. • `http` — An HTTP server.	No default.
`{<vdom_name> | root}`	Specifies the administrative domain (ADOM) that the CRL applies to. If ADOMs are not enabled, specify `root`.	No default.
`<crl_name>`	If the source of the CRL is a TFTP server, the name of the CRL file.	No default.
`{<tftp_ipv4> | <scep_url> | <http_url>}`	If the source of the CRL is a TFTP server, the IP address of the server. If the source of the CRL is a SCEP server, the URL of the server. If the source of the CRL is an HTTP server, the URL of the server.	No default.

Example

This example uploads the CRL file `Cert31.crl` from the TFTP server `192.168.1.23`.

```
execute certificate crl import tftp root Cert31.crl 192.168.1.23
```

This example uploads the CRL file `Cert31.crl` from the HTTP server `10.0.0.31`.

```
execute certificate crl import http root http://10.0.0.31/certsrv/CertEnroll/Cert31.crl
```

This example uploads a CRL file from the SCEP server at `http://155.229.15.173/cert/scep`.

```
execute certificate crl import auto root http://155.229.15.173/cert/scep
```

Related topics

- config system certificate crl
- execute certificate ca
- execute certificate inter-ca
- execute certificate local

certificate inter-ca

Use this command to upload an intermediate CA's certificate.

If a server certificate is signed by an intermediate (non-root) certificate authority rather than a root CA, before the client trusts the server's certificate, you must demonstrate a link with trusted root CAs. This mechanism proves that the server's certificate is genuine. Otherwise, the server certificate may cause the end-user's web browser to display certificate warnings.

Syntax

```
execute certificate inter-ca import {tftp | auto} {<vdom_name> | root} <cert_name>
    {<tftp_ipv4> | <scep_url>} [<ca_id>]
```

Variable	Description	Default
{tftp | auto}	Use one of the following options to specify the location of the certificate to upload to FortiWeb: • tftp — A TFTP server. • auto — A SCEP (Simple Certificate Enrollment Protocol) server.	No default.
{<vdom_name> | root}	Specifies the administrative domain (ADOM) that the certificate applies to. If ADOMs are not enabled, specify root.	No default.
<cert_name>	If the certificate is located on a TFTP server, the name of the certificate file.	No default.
{<tftp_ipv4> | <scep_url>}	If the certificate is located on a TFTP server, the IP address of the server. If the source of the certificate is a SCEP server, the URL of the server.	No default.
<ca_id>	Optionally, if the source of the certificate is a SCEP server, you can use a CA identifier to specify a specific CA.	No default.

Example

This example uploads the certificate file `ca.cer` from the TFTP server `192.168.1.23`.

```
execute certificate inter-ca import tftp root ca.cer 192.168.1.23
```

This example uploads the certificate file from the SCEP server at `http://10.0.0.31/certsrv/mscep/mscep.dll`.

```
execute certificate inter-ca import auto root http://10.0.0.31/certsrv/mscep/mscep.dll
```

Related topics

- `config system certificate intermediate-certificate`
- `execute certificate ca`
- `execute certificate crl`
- `execute certificate local`

certificate local

Use this command to upload a server certificate from a TFTP server. You also use it to upload a client certificate for FortiWeb.

For more information about server certificates, see `config system certificate local`.

Syntax

```
execute certificate local {cert | pkcs12-cert} import tftp {<vdom_name> | root}
    <cert_name> <key_name> <password_str>
```

Variable	Description	Default
`{cert | pkcs12-cert}`	Use one of the following options to specify the type of certificate file to upload: • `cert` — An unencrypted certificate in PEM format. The key is in a separate file. • `pkcs12-cert` — A PKCS #12 encrypted certificate with key.	No default.
`{<vdom_name> | root}`	Specifies the administrative domain (ADOM) that the certificate applies to. If ADOMs are not enabled, specify `root`.	`root`
`<cert_name>`	Specifies the name of the certificate file.	No default.

Variable	Description	Default
<key_name>	If the certificate is unencrypted with the key in a separate file, specifies the key file to upload with the certificate.	No default.
<tftp_ipv4>	Specifies the IP address of the TFTP server.	No default.
<password_str>	If the certificate is encrypted, specify the password that was used to encrypt the file. If the certificate is not encrypted, FortiWeb ignores this value.	No default.

Example

This example uploads the certificate file `pc40.crt` and its key file `pc40.key` from the TFTP server `192.168.1.23`. The certificate is encrypted using the password `fortinet`.

```
execute certificate local cert import tftp root pc40.crt pc40.key 192.168.1.23 fortinet
```

This example uploads the certificate file `frompc31.pfx` from the TFTP server `192.168.1.23`. The certificate is encrypted using the password `fortinet`.

```
execute certificate local pkcs12-cert import tftp root frompc31.pfx 192.168.1.23 fortinet
```

Related topics

- `config system certificate local`
- `execute certificate ca`
- `execute certificate crl`
- `execute certificate inter-ca`

create-raid level

Use the this command to initialize the RAID.

Currently, only RAID level 1 is supported, and only on FortiWeb-1000B, 1000C, 3000C/CFsx, 3000E, and 4000E shipped with FortiWeb 4.0 MR1 or later.

On older appliances that have been upgraded to FortiWeb 4.0 MR1, RAID cannot be activated.

Back up any data before initializing the array.

Back up the data regularly. RAID is not a substitute for regular backups. RAID 1 (mirroring) is designed to improve hardware fault tolerance, but cannot negate all risks.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute create-raid level {raid1}
```

Variable	Description	Default
`level {raid1}`	Type the RAID level. Currently, only RAID level 1 is supported.	`raid1`

Related topics

- `config system raid`
- `diagnose hardware raid list`
- `execute create-raid rebuild`

create-raid rebuild

Use the this command to rebuild the RAID.

Currently, only RAID level 1 is supported, and only on FortiWeb-1000B, 1000C, 3000C/CFsx, 3000E, and 4000E shipped with FortiWeb 4.0 MR1 or later.

On older appliances that have been upgraded to FortiWeb 4.0 MR1, RAID cannot be activated.

Back up the data regularly. RAID is not a substitute for regular backups. RAID 1 (mirroring) is designed to improve hardware fault tolerance, but cannot negate all risks.

Rebuilding the array due to disk failure may result in some loss of packet log data.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute create-raid rebuild
```

Example

This example rebuilds the RAID array.

```
execute create-raid rebuild
```

The CLI displays the following:

```
This operation will clear all data on disk :0!
Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays additional messages.

Related topics

- system raid
- hardware raid list

date

Use this command to display or set the system date.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute date [<date_str>]
```

Variable	Description	Default
`date [<date_str>]`	Type the current date for the FortiWeb appliance's time zone, using the format `yyyy-mm-dd`, where: • `yyyy` is the year. Valid years are `2001` to `2037`. • `mm` is the month. Valid months are `01` to `12`. • `dd` is the day of the month. Valid days are `01` to `31`. If you do not specify a date, the command returns the current system date. Shortened values, such as `06` instead of `2006` for the year or `1` instead of `01` for the month or day, are not valid.	No default.

Example

This example sets the date to 17 September 2011:

```
execute date 2011-09-17
```

Related topics

- `execute time`
- `config system global`

db rebuild

Use this command to rebuild the FortiWeb appliance's internal database that it uses to store log messages.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute db rebuild
```

Related topics

- `execute formatlogdisk`
- `diagnose debug application miglogd`
- `diagnose debug upload`

erase-disk

Use this command to erase the hard disk or flash memory.

This command requires a console connection to the appliance and is available only when Federal Information Processing Standards (FIPS) and Common Criteria (CC) compliant mode is enabled (see `config system fips-cc`).

Syntax

```
execute erase-disk { flash | disk } [<erase-times> ]
```

Variable	Description	Default
`{ flash | disk }`	Specify whether to erase the flash memory or the hard disk.	No default.
`<erase-times>`	Enter the number of times to overwrite the specified memory with random data. Valid values are 1 to 35.	`1`

factoryreset

Use this command to reset the FortiWeb appliance to its default settings for the currently installed firmware version. If you have not upgraded or downgraded the firmware, this restores factory default settings.

Back up your configuration first. This command resets all changes that you have made to the FortiWeb appliance's configuration file and reverts the system to the default values for the firmware version. Depending on the firmware version, this could include factory default settings for the IP addresses of network interfaces. For information on creating a backup, see `execute backup cli-config`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute factoryreset
```

Related topics

- `execute backup cli-config`
- `execute backup full-config`
- `execute restore config`

formatlogdisk

Use this command to clear the logs from the FortiWeb appliance's hard disk and reformat the disk.

This operation deletes all locally stored log files.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

When you execute this command, the FortiWeb appliance displays the following message:

```
This operation will clear all data on the log disk and take a few minutes according to
    the disk size!!
Do you want to continue? (y/n)
```

Syntax

```
execute formatlogdisk
```

Related topics

- `execute db rebuild`

ha disconnect

Use this command to manually force a FortiWeb appliance to leave the HA group, **without** unplugging any cables. This can be useful, for example, if you need to remove a standby appliance from the HA cluster in order to configure it for standalone operation, and want to do so **without** disrupting traffic, and without unplugging cables.

Behavior varies by which appliance you eject:

- **Active** — Failover occurs. The standby remains as a member of the HA group, and will elect itself as the new active appliance, assuming all of the HA cluster's configured IP addresses and traffic processing duties.

- **Standby** — No failover occurs. The active appliance remains actively processing traffic.

To ensure that you can re-connect to the ejected appliance's GUI or CLI via a remote network connection (not only via its local console), this command requires that you specify an IP address and port name that will become its new management interface. By default, it will be accessible via HTTP, HTTPS, SSH, and telnet. (All other network interfaces on the ejected appliance will be brought down and reset to 0.0.0.0/0.0.0.0. To configure them, you must connect to the ejected appliance's GUI or CLI.)

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute ha disconnect <serial-number_str> <interface_name> <interface_ipv4mask>
```

Variable	Description	Default
`disconnect <serial-number_str>`	Type the serial number of the FortiWeb appliance that you want to disconnect from the cluster. To display the serial number of each appliance in the HA group, type: `execute ha disconnect ?`	No default.
`<interface_name>`	Type the name of the network interface, such as `port1`, that will be configured as the ejected appliance's management interface.	No default.
`<interface_ipv4mask>`	Type the IP address and netmask that will be configured as the ejected appliance's management interface.	No default.

Example

This example ejects the standby appliance whose serial number is FV-1KC3R11111111, assigning its port1 to be the web UI/GUI interface, reachable at 10.0.0.1.

```
execute ha disconnect FV-1KC3R11111111 port1 10.0.0.1/24
```

After the command completes, to reconfigure the ejected appliance, you could then use either a web browser or SSH client to connect to 10.0.0.1 in order to reconfigure it for standalone operation.

Related topics

- `execute ha disconnect`
- `execute ha manage`
- `execute ha md5sum`
- `diagnose system ha status`
- `diagnose system ha mac`
- `get system status`
- `config system global`

ha manage

Use this command to log in to another appliance in the HA group via the HA link. In most cases, you log into a standby appliance (also called the secondary, or slave) from the main (primary or master) appliance, but you can also use a standby appliance to access the main appliance.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute ha manage <cluster-index>
```

Variable	Description	Default
`<cluster-index>`	Specifies an index value that the FortiWeb HA feature assigns to a cluster member based on its serial number. The cluster member with the highest serial number has a cluster index of 0, the one with the second-highest serial number has a cluster index of 1, and so on. To display the index numbers of the cluster members, enter the following command: `execute ha manage ?`	No default.

Example

In this example, you are logged in to the main appliance.

```
execute ha manage ?
<id>    please input peer box index.
<2>     Subsidary unit FV-1KD3A12345678
<3>     Subsidary unit FV-1KD3A11345678
```

The cluster index and serial number of the appliance you are currently logged in to is not displayed.

Enter `3` to connect to the standby appliance with serial number FV-1KD3A11345678. The CLI prompt changes to the host name of this unit and the login prompt is displayed.

To return to the primary unit, type `exit`.

Related topics

- `execute ha disconnect`
- `execute ha md5sum`
- `execute ha synchronize`
- `diagnose system ha status`

- diagnose system ha mac
- config system global

ha md5sum

Use this command to retrieves the CLI system configuration MD5 from the two appliances in a HA cluster.

This information allows you to confirm whether HA configuration is synchronized.

Syntax

```
execute ha md5sum
```

Example

Below is a sample output.

```
CLI configuration MD5SUM :
[master]:555393AE023104AB41C195F6B1CCD177
[slave ]:555393AE023104AB41C195F6B1CCD177

System configuration MD5SUM :
[master]:39B9A403673ABB7333A5EC6BAD9BEE25
[slave ]:39B9A403673ABB7333A5EC6BAD9BEE25
```

Related topics

- execute ha disconnect
- execute ha manage
- config system global

ha synchronize

Use this command to manually control the synchronization of configuration files and FortiGuard service-related packages from the active HA appliance to the standby appliance.

Typically, most HA synchronization happens automatically, whenever changes are made. However, in some cases, you may want to use this command to manually initiate full or partial HA synchronization.

- To delay synchronization to a more convenient time if you are planning to make large batch changes, and therefore delayed synchronization is preferable for network performance reasons
- To manually force synchronization of files that are not automatically synchronized
- To trigger automatic synchronization if it has been interrupted due to HA link failure, daemon crashes, etc.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute ha synchronize {all | avupd | cli | geodb | sys}
execute ha synchronize {start | stop}
```

Variable	Description	Default
`synchronize {all | avupd | cli | geodb | sys}`	Select which part of the configuration and/or FortiGuard service-related packages to synchronize. • `all` — Entire configuration, including CLI configuration, system files, and signature databases. • `avupd` — Only the FortiGuard Antivirus service package, including the virus signatures, scan engine, and proxy. • `cli` — Only the core CLI configuration file (fwb_system.conf). (You can use the `show` command to view the contents of the configuration file.) • `geodb` — Only the geography-to-IP address mappings. Similar to firmware, these can be downloaded from the Fortinet Technical Support web site. • `sys` — Only the IP Reputation Database (IRDB) and system files such as X.509 certificates. **Note:** This command has no effect if you use the command `execute ha synchronize stop`. to pause it manually.	No default.
`synchronize {start | stop}`	Select whether to start or stop synchronization.	No default.

Example

This example shows how to manually synchronize the virus signature and engine package to the standby appliance.

```
FortiWeb # execute ha synchronize avupd
starting synchronize with HA master...
```

Related topics

- `execute ha disconnect`
- `execute ha manage`
- `execute ha md5sum`
- `config system global`

ping

Use this command to perform an ICMP `ECHO` request (also called a ping) to a host by specifying its fully qualified domain name (FQDN) or IPv4 address, using the options configured by ping-options.

Pings are often used to test IP-layer connectivity during troubleshooting.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute ping {<host_fqdn> | <host_ipv4>}
```

Variable	Description	Default
`ping {<host_fqdn> | <host_ipv4>}`	Type either the IPv4 address or fully qualified domain name (FQDN) of the host.	No default.

Example

This example pings a host with the IP address 172.16.1.10.

```
execute ping 172.16.1.10
```

The CLI displays the following:

```
PING 172.16.1.10 (172.16.1.10): 56 data bytes
    64 bytes from 172.16.1.10: icmp_seq=0 ttl=128 time=0.5 ms
    64 bytes from 172.16.1.10: icmp_seq=1 ttl=128 time=0.2 ms
    64 bytes from 172.16.1.10: icmp_seq=2 ttl=128 time=0.2 ms
    64 bytes from 172.16.1.10: icmp_seq=3 ttl=128 time=0.2 ms
    64 bytes from 172.16.1.10: icmp_seq=4 ttl=128 time=0.2 ms
--- 172.16.1.10 ping statistics ---
    5 packets transmitted, 5 packets received, 0% packet loss
    round-trip min/avg/max = 0.2/0.2/0.5 ms
```

The results indicate that a route exists between the FortiWeb appliance and 172.16.1.10. It also indicates that during the sample period, there was no packet loss, and the average response time was 0.2 milliseconds.

Example

This example pings a host with the IP address 10.0.0.1.

```
execute ping 10.0.0.1
```

The CLI displays the following:

```
PING 10.0.0.1 (10.0.0.1): 56 data bytes
```

After several seconds, no output appears. The administrator halts the ping by pressing Ctrl+C. The CLI displays the following:

```
--- 10.0.0.1 ping statistics ---
```

```
5 packets transmitted, 0 packets received, 100% packet loss
```

The results indicate the host may be down, or there is no route between the FortiWeb appliance and 10.0.0.1. To determine the point of failure along the route, further diagnostic tests are required, such as `execute traceroute`.

Related topics

- `config system interface`
- `config server-policy vserver`
- `execute ping-options`
- `execute ping6`
- `execute telnettest`
- `execute traceroute`
- `diagnose network ip`
- `diagnose hardware nic`
- `diagnose network sniffer`

ping6

Use this command to perform an ICMP `ECHO` request (also called a ping) to a host by specifying its IPv6 address, using the options configured by `execute ping-options`.

Pings are often used to test IP-layer connectivity during troubleshooting.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute ping6 {<host_fqdn> | <host_ipv6>}
```

Variable	Description	Default
`ping6 {<host_fqdn> | <host_ipv6>}`	Type either the IP address or fully qualified domain name (FQDN) of the host.	No default.

Example

This example pings a host with the IP address 2001:0db8:85a3:::8a2e:0370:7334.

```
execute ping6 2607:f0b0:f:420::
```

The CLI displays the following:

```
PING 2607:f0b0:f:420:: (2607:f0b0:f:420::): 56 data bytes
```

After several seconds, no output appears. The administrator halts the ping by pressing Ctrl+C. The CLI displays the following:

```
--- 2607:f0b0:f:420:: ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

The results indicate the host may be down, or there is no route between the FortiWeb appliance and 2607:f0b0:f:420::. To determine the point of failure along the route, further diagnostic tests are required, such as traceroute on page 624.

Related topics

- config system interface
- config server-policy vserver
- execute ping6-options
- execute telnettest
- execute traceroute
- diagnose network ip
- diagnose hardware nic
- diagnose network route
- diagnose network sniffer

ping-options

Use these commands to configure the behavior of the ping command.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute ping-options data-size <bytes_int>
execute ping-options df-bit {yes | no}
execute ping-options pattern <bufferpattern_hex>
execute ping-options repeat-count <repeat_int>
execute ping-options source {auto | <interface_ipv4>}
execute ping-options timeout <seconds_int>
execute ping-options tos {<service_type>}
execute ping-options ttl <hops_int>
execute ping-options validate-reply {yes | no}
execute ping-options view-settings
```

Variable	Description	Default
data-size <bytes_int>	Enter datagram size in bytes. This allows you to send out packets of different sizes for testing the effect of packet size on the connection. If you want to configure the pattern that will be used to buffer small datagrams to reach this size, also configure pattern <bufferpattern_hex>.	56

Variable	Description	Default
`df-bit {yes | no}`	Enter either `yes` to set the DF bit in the IP header to prevent the ICMP packet from being fragmented, or enter `no` to allow the ICMP packet to be fragmented.	`no`
`pattern <bufferpattern_hex>`	Enter a hexadecimal pattern, such as `00ffaabb`, to fill the optional data buffer at the end of the ICMP packet. The size of the buffer is determined by `data-size <bytes_int>`.	No default.
`repeat-count <repeat_int>`	Enter the number of times to repeat the ping.	`5`
`source {auto | <interface_ipv4>}`	Select the network interface from which the ping is sent. Enter either `auto` or a FortiWeb network interface IP address.	auto
`timeout <seconds_int>`	Enter the ping response timeout in seconds.	`2`
`tos {<service_type>}`	Enter the IP type-of-service option value, either: • `default` — Do not indicate. (That is, set the TOS byte to 0.) • `lowcost` — Minimize cost. • `lowdelay` — Minimize delay. • `reliability` — Maximize reliability. • `throughput` — Maximize throughput.	`default`
`ttl <hops_int>`	Enter the time-to-live (TTL) value.	`64`
`validate-reply {yes | no}`	Select whether or not to validate ping replies.	`no`
`view-settings`	Display the current ping option settings.	No default.

Example

This example sets the number of pings to three and the source IP address to 10.10.10.1, then views the ping options to verify their configuration.

```
execute ping-option repeat-count 3
execute ping-option source 10.10.10.1
execute ping-option view-settings
```

The CLI would display the following:

```
Ping Options:
 Repeat Count: 3
 Data Size: 56
 Timeout: 2
 TTL: 64
 TOS: 0
 DF bit: unset
```

```
Source Address: 10.10.10.1
Pattern:
Pattern Size in Bytes: 0
Validate Reply: no
```

Related topics

- execute ping
- execute traceroute

ping6-options

Use these commands to configure the behavior of the execute ping6 command.

To use this command, your administrator account's access control profile must have at least r permission to the sysgrp area. For more information, see Permissions on page 74.

Syntax

```
execute ping6-options data-size <bytes_int>
execute ping6-options pattern <bufferpattern_hex>
execute ping6-options repeat-count <repeat_int>
execute ping6-options source {auto | <interface_ipv4>}
execute ping6-options timeout <seconds_int>
execute ping6-options tos {<service_type>}
execute ping6-options ttl <hops_int>
execute ping6-options validate-reply {yes | no}
execute ping6-options view-settings
```

Variable	Description	Default
data-size <bytes_int>	Enter datagram size in bytes.This allows you to send out packets of different sizes for testing the effect of packet size on the connection. If you want to configure the pattern that will be used to buffer small datagrams to reach this size, also configure pattern <bufferpattern_hex>.	56
pattern <bufferpattern_hex>	Enter a hexadecimal pattern, such as 00ffaabb, to fill the optional data buffer at the end of the ICMP packet. The size of the buffer is determined by data-size <bytes_int>.	No default.
repeat-count <repeat_int>	Enter the number of times to repeat the ping.	5
source {auto | <interface_ipv6>}	Select the network interface from which the ping is sent. Enter either auto or a FortiWeb network interface IP address.	auto
timeout <seconds_int>	Enter the ping response timeout in seconds.	2

Variable	Description	Default
`tos {<service_type>}`	Enter the IP type-of-service option value, either: • `default` — Do not indicate. (That is, set the TOS byte to 0.) • `lowcost` — Minimize cost. • `lowdelay` — Minimize delay. • `reliability` — Maximize reliability. • `throughput` — Maximize throughput.	`default`
`ttl <hops_int>`	Enter the time-to-live (TTL) value.	`64`
`validate-reply {yes | no}`	Select whether or not to validate ping replies.	`no`
`view-settings`	Display the current ping option settings.	No default.

Example

This example sets the number of pings to 3, then views the ping options to verify their configuration.

```
execute ping6-option repeat-count 3
execute ping6-option view-settings
```

The CLI would display the following:

```
IPV6 Ping Options:
Repeat Count: 3
Data Size: 56
Timeout: 2
Interval: 1
TTL: 64
TOS: 0
Source Address: auto
Pattern:
Pattern Size in Bytes: 0
Validate Reply: no
```

Related topics

- `execute ping6`
- `execute traceroute`

reboot

Use this command to restart the FortiWeb appliance.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute reboot
```

Example

This example shows the reboot command in action.

```
execute reboot
```

The CLI displays the following:

```
This operation will reboot the system !
Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following:

```
System is rebooting...
```

If you are connected to the CLI through a local console, the CLI displays messages while the reboot is occurring.

If you are connected to the CLI through the network, the CLI will not display any notification while the reboot is occurring, as this occurs after the network interfaces have been shut down. Instead, you may notice that the connection is terminated. Time required by the reboot varies by many factors, such as whether or not hard disk verification is required, but may be several minutes.

Related topics

- `execute shutdown`
- `get system performance`

restore config

Use this command to restore the configuration from a configuration backup file on an TFTP server, or to install primary or backup firmware.

Back up the configuration before restoring the configuration. This command restores configuration changes only, and does not affect settings that remain at their default values. Default values may vary by firmware version. For backup commands, see `execute backup cli-config` and `execute backup full-config`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute restore config tftp <filename_str>  <tftp_ipv4> [<password_str>]
```

Variable	Description	Default
<filename_str>	Type the name of the backup or firmware image file.	No default.
<tftp_ipv4>	Type the IP address of the TFTP server.	No default.
[<password_str>]	Type the password that was used to encrypt the backup file, if any. If you do not provide a password, the backup file must have been stored as clear text.	No default.

Example

This example downloads a configuration file named backup.conf from the TFTP server, 192.168.1.23, to the FortiWeb appliance. The backup file was encrypted with the password P@ssword1.

```
execute restore config tftp backup.conf 192.168.1.23 P@ssword1
```

The FortiWeb appliance then applies the configuration backup and reboots.

Related topics

- execute backup full-config
- execute restore config
- execute restore image
- execute restore secondary-image

restore image

Use this command to install firmware on the primary partition and reboot.

Back up the configuration before installing new firmware. Installing new firmware can change default settings and reset settings that are incompatible with the new version. For backup commands, see execute backup full-config and execute backup cli-config.

Unlike installing firmware via TFTP during a boot interrupt, installing firmware using this command will attempt to preserve settings and files, and not necessarily restore the FortiWeb appliance to its firmware/factory default configuration.

To use this command, your administrator account's access control profile must have either w or rw permission to the mntgrp area. For more information, see Permissions on page 74.

Syntax

```
execute restore image ftp <filename_str>  <ftp_ipv4>
```

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

Variable	Description	Default
<filename_str>	Type the name of the firmware image file.	No default.
<ftp_ipv4>	Type the IP address of the TFTP server.	No default.
<tftp_ipv4>	Type the IP address of the FTP server.	No default.

Example

This example installs a firmware file named `firmware.out` from the TFTP server, 192.168.1.23, to the FortiWeb appliance.

```
execute restore image tftp firmware.out 192.168.1.23
```

The FortiWeb appliance downloads the firmware file, installs it, and reboots.

Related topics

- execute backup cli-config
- execute backup full-config
- execute restore config
- execute restore secondary-image
- diagnose system flash
- get system status

restore secondary-image

Use this command to install backup firmware on the secondary partition and reboot.

Back up the configuration before installing new firmware. Installing new firmware can change default settings and reset settings that are incompatible with the new version. For backup commands, see backup full-config on page 595 and backup cli-config on page 593.

Unlike installing firmware via TFTP during a boot interrupt, installing firmware using this command will attempt to preserve settings and files, and not necessarily restore the FortiWeb appliance to its firmware/factory default configuration.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute restore secondary-image ftp <filename_str>  <ftp_ipv4>
execute restore secondary-image tftp <filename_str>  <tftp_ipv4>
```

Variable	Description	Default
<filename_str>	Type the name of the firmware image file.	No default.
<ftp_ipv4>	Type the IP address of the FTP server.	No default.
<tftp_ipv4>	Type the IP address of the TFTP server.	No default.

Example

This example installs a firmware file named `firmware.out` from the TFTP server, 192.168.1.23, to the FortiWeb appliance.

```
execute restore secondary-image tftp firmware.out 192.168.1.23
```

The FortiWeb appliance downloads the firmware file, installs it, and reboots.

Related topics

- execute backup cli-config
- execute backup full-config
- execute restore config
- execute restore image
- diagnose system flash
- get system status

restore vmlicense

Use this command to upload a FortiWeb-VM license file from an FTP or TFTP server.

After you enter the command, FortiWeb prompts you to confirm the upload.

After the license is authenticated successfully, the following message is displayed:

```
"*ATTENTION*: license registration status changed to 'VALID', please logout and re-login"
```

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see Permissions on page 74.

For more information on FortiWeb-VM licenses, see the *FortiWeb-VM Install Guide*.

Syntax

```
execute restore vmlicense {ftp | tftp} <license-file_str>  {<ftp_ipv4> | <user_
    str>:<password_str>@<ftp_ipv4> | <tftp_ipv4>}
```

Variable	Description	Default
{ftp | tftp}	Specify whether to connect to the server using file transfer protocol (FTP) or trivial file transfer protocol (TFTP).	No default.
<license-file_str>	The name of the license file.	No default.
<ftp_ipv4>	The IP address of the FTP server.	No default.
<user_str>	The user name that FortiWeb uses to authenticate with the server.	No default.
<password_str>	The password for the account specified by <user_str>.	No default.
<tftp_ipv4>	The IP address of the TFTP server.	No default.

Example

This example uploads the license file `FVVM040000010871.lic` from the TFTP server 192.168.1.23 to the FortiWeb appliance.

```
execute restore vmlicense tftp FVVM040000010871.lic 192.168.1.23
```

The FortiWeb appliance uploads the file, and then prompts you to log out and log in again.

session-cleanup

Use this command to immediately clean up all sessions.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute session-cleanup
```

shutdown

Use this command to prepare the FortiWeb appliance to be powered down by halting the software, clearing all buffers, and writing all cached data to disk.

Power off the FortiWeb appliance only after issuing this command. Unplugging or switching off the FortiWeb appliance without issuing this command could result in data loss.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute shutdown
```

Example

This example shows the reboot command in action.

```
execute shutdown
```

The CLI displays the following:

```
This operation will halt the system
(power-cycle needed to restart)!Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following:

```
System is shutting down...(power-cycle needed to restart)
```

If you are connected to the CLI through a local console, the CLI displays a message when the shutdown is complete.

If you are connected to the CLI through the network, the CLI will not display any notification when the shutdown is complete, as this occurs after the network interfaces have been shut down. Instead, you may notice that the connection times out.

Related topics

- `execute reboot`

telnet

Use this command to open a Telnet connection to a server using IPv4 to port 23.

Telnet connections are not secure. Eavesdroppers could easily obtain your administrator password. Only use telnet over a trusted, physically secured network, such as a direct connection between your computer and the appliance.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute telnet <host_ipv4>
```

Variable	Description	Default
`telnet <host_ipv4>`	Type the IP address of the host.	No default.

Example

This example Telnets to a host with the IP address 172.16.1.10.

```
execute telnet 172.16.1.10
login: admin
Password: *******
```

Related topics

- `execute telnettest`
- `execute ping`
- `execute ping6`

telnettest

Use this command to open a Telnet connection to a server using an IPv4 or IPv6 address or fully qualified domain name (FQDN). This command can be useful for troubleshooting (for example, when the server does not support the HTTP versions, methods, headers, and so on, that the client uses).

Telnet connections are not secure. Eavesdroppers could easily obtain your administrator password. Only use Telnet over a trusted, physically secured network, such as a direct connection between your computer and the appliance, and from the appliance to the server.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute telnettest {<host_ipv4> | <host_ipv6> | <host_fqdn>}
```

Variable	Description	Default
`telnettest {<host_ipv4> | <host_ipv6> | <host_fqdn>}`	Type the IP address or fully qualified domain name (FQDN) of the host.	No default.

Example

This example Telnets to a host with the IPv4 address 172.16.1.10 on port 80, the IANA standard port for HTTP.

```
FortiWeb# exec telnettest 172.16.1.10:80
Connected

GET /

Entering interactive mode. Type CTRL-D to exit.
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>501 Method Not Implemented</title>
</head><body>
<h1>Method Not Implemented</h1>
<p>Get to /index.html not supported.<br />
</p>
<hr>
<address>Apache/2.2.22 (Unix) DAV/2 mod_ssl/2.2.22 OpenSSL/0.9.8x Server at irene.local
    Port 80</address>
</body></html>
Connection closed.

Connection status to 172.16.1.10 port 80:
Connecting to remote host succeeded.
```

Related topics

- execute telnet
- execute ping
- execute ping6

time

Use this command to display or set the system time.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute time [<time_str>]
```

Variable	Description	Default
`time [<time_str>]`	Type the current date for the FortiWeb appliance's time zone, using the format `hh:mm:ss`, where: • `hh` is the hour. Valid hours are `00` to `23`. • `mm` is the minute. Valid minutes are `00` to `59`. • `ss` is the second. Valid seconds are `00` to `59`. If you do not specify a time, the command returns the current system time. Shortened values, such as `1` instead of `01` for the hour, are valid. For example, you could enter either `01:01:01` or `1:1:1`.	No default.

Example

This example sets the system time to 15:31:03:

```
execute time 15:31:03
```

Related topics

- `execute date`
- `config system global`

traceroute

Use this command to use ICMP to test the connection between the FortiWeb appliance and another network device, and display information about the time required for network hops between the device and the FortiWeb appliance.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute traceroute {<host_fqdn> | <host_ipv4>}
```

Variable	Description	Default
`traceroute {<host_fqdn> | <host_ipv4>}`	Type either the IP address or fully qualified domain name (FQDN) of the host.	No default.

Example

This example tests connectivity between the FortiWeb appliance and docs.fortinet.com. In this example, the trace times out after the first hop, indicating a possible connectivity problem at that point in the network.

```
FortiWeb# execute traceroute docs.fortinet.com
traceroute to docs.fortinet.com (65.39.139.196), 30 hops max, 38 byte packets
1  172.16.1.200 (172.16.1.200) 0.324 ms 0.427 ms 0.360 ms
 2  * * *
```

Example

This example tests the availability of a network route to the server example.com.

```
execute traceroute example.com
```

The CLI displays the following:

```
traceroute to example.com (192.168.1.10), 32 hops max, 72 byte packets
1 172.16.1.2  0 ms 0 ms 0 ms
2  10.10.10.1  <static.isp.example.net> 2 ms 1 ms 2 ms
3  10.20.20.1   1 ms  5 ms 1 ms
4  10.10.10.2  <core.isp.example.net> 171 ms 186 ms 14 ms
5  10.30.30.1  <isp2.example.net> 10 ms 11 ms 10 ms
6  10.40.40.1  73 ms 74 ms 75 ms
7 192.168.1.1  79 ms 77 ms 79 ms
8 192.168.1.2 73 ms 73 ms 79 ms
9 192.168.1.10 73 ms 73 ms 79 ms
10 192.168.1.10 73 ms 73 ms 79 ms
```

Example

This example attempts to test connectivity between the FortiWeb appliance and example.com. However, the FortiWeb appliance could not trace the route, because the primary or secondary DNS server that the FortiWeb appliance is configured to query could not resolve the FQDN `example.com` into an IP address, and it therefore did not know to which IP address it should connect. As a result, an error message is displayed.

```
FortiWeb# execute traceroute example.com
traceroute: unknown host example.com
Command fail. Return code 1
```

To resolve the error message in order to perform connectivity testing, the administrator would first configure the FortiWeb appliance with the IP addresses of DNS servers that can resolve the FQDN `example.com`. For details, see `execute system dns`.

Related topics

- `execute ping`
- `execute ping-options`
- `diagnose network ip`
- `diagnose hardware nic`
- `diagnose network sniffer`

update-now

Use this command to initiate an update of the predefined robots, data types, suspicious URLS, and attack signatures used by your FortiWeb appliance.

FortiWeb appliances receive updates from the FortiGuard Distribution Network (FDN). The FDN is a world-wide network of FortiGuard Distribution Servers (FDS). FortiWeb appliances connect to the FDN by connecting to the FDS nearest to the FortiWeb appliance by its configured time zone.

The time required for the update varies with the availability of the updates, the size of the updates, and the speed of the FortiWeb appliance's network connection. If event logging is enabled, and the FortiWeb appliance cannot connect successfully, it will log the message `update failed, failed to connect any fds servers!` or `FortiWeb is unauthorized`

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For more information, see Permissions on page 74.

Syntax

```
execute update-now
```

get

The `get` command displays parts of your FortiWeb appliance's configuration in the form of a list of settings and their values.

Unlike `show`, `get` displays **all** settings, even if they are still in their default state.

For example, you might get the current DNS settings:

```
get system dns
primary : 172.16.95.19
secondary : 0.0.0.0
domain : example.com
```

Notice that the command displays the setting for the secondary DNS server, even though it has not been configured, or has reverted to its default value.

Also unlike `show`, unless used from within an object or table, `get` requires that you specify the object or table whose settings you want to display.

For example, at the root prompt, this command would be valid:

```
get system dns
```

and this command would **not** be valid:

```
get
```

Like `show`, depending on whether or not you have specified an object, `get` may display one of two different outputs, either the configuration:

- that you have just entered but not yet saved, or
- as it currently exists on the flash disk, respectively.

For example, immediately after configuring the secondary DNS server setting but **before** saving it, `get` displays two different outputs (differences highlighted in bold):

```
FortiWeb# config system dns
FortiWeb (dns)# set secondary 192.168.1.10
FortiWeb (dns)# get
primary : 172.16.95.19
secondary : 192.168.1.10
domain : example.com
FortiWeb (dns)# get system dns
primary : 172.16.95.19
secondary : 0.0.0.0
domain : example.com
```

The first output from `get` indicates the value that you have configured but not yet saved; the second output from `get` indicates the value that was last saved to disk.

If you were to now enter `end`, saving your setting to disk, `get` output for both syntactical forms would again match. However, if you were to enter `abort` at this point and discard your recently entered secondary DNS setting instead of saving it to disk, the FortiWeb appliance's configuration would therefore match the second output, not the first.

If you have entered settings but cannot remember how they differ from the existing configuration, the two different forms of `get`, with and without the object name, can be a useful way to remind yourself.

Most `get` commands, such as `get system dns`, are used to display configured settings. You can find relevant information about such commands in the corresponding config commands in the `config` chapter.

Other `get` commands, such as `get system performance`, are used to display system information that is **not** configurable. This chapter describes this type of `get` command.

The get commands require at least read (r) permission to applicable administrator profile groups.

This chapter describes the following commands.

`get router all`
`get system fortisandbox-statistics`
`get system logged-users`
`get system performance`
`get system status`
`get waf signature-rules`

Although not explicitly shown in this section, for all config commands, there are related `get` and show commands which display that part of the configuration. `get` and `show` commands use the same syntax as their related `config` command, unless otherwise mentioned. For syntax examples and descriptions of each configuration object, field, and option, see config on page 89

When ADOMs are enabled, and if you log in as `admin`, the top level of the shell changes: the two top level items are `get global` and `get vdom`.

- `get global` displays settings that only `admin` or other accounts with the **prof_admin** access profile can change.
- `get vdom` displays 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.

router all

Use this command to display the list of configured and implied static routes.

Syntax

```
get router all
```

Example

```
get router all
```

Output such as the following appears in the CLI. In this case, only 172.20.120.0 was a static route configured by an administrator using `config router static`. The other routes are implied by the IP addresses of the virtual servers (10.1.1.10 listening on port2) and network interfaces (192.168.1.25 for port3).

```
IP Mask Gateway Distance Device
172.20.120.0 255.255.255.0 0.0.0.0 0 port1
10.1.1.221 255.255.255.255 0.0.0.0 0 port2
192.168.1.0 255.255.255.0 0.0.0.0 0 port3
```

Related topics

- `config router static`
- `diagnose network route`

system fortisandbox-statistics

Displays a count of uploaded files that FortiSandbox has evaluated in the past 7 days, by evaluation result.

FortiWeb organized the statistics using the following categories:

- detected (total malicious files detected)
- clean
- risk-low (total low-risk malicious files detected)
- risk-medium (total medium-risk malicious files detected)
- risk-high (total high-risk malicious files detected)

Syntax

```
get system fortisandbox-statistics
```

Example

```
FortiWeb # get system fortisandbox-statistics
detected : 0
clean : 0
risk-low : 0
risk-medium : 0
risk-high : 0
```

Related topics

- `config system fortisandbox`
- `config waf file-upload-restriction-policy`
- `config log reports`

system logged-users

Lists which administrator accounts are currently logged in to the FortiWeb appliance via the local console, web UI, or CLI (including through the JavaScript-based **CLI Console** widget of the web UI). It also displays the login time of that administrative session.

For information on allowing only one administrator to be logged in at any given time, see `config system global`.

Syntax

```
get system logged-users
```

Example

```
get system logged-users
Logged in users: 2
INDEX USERNAME TYPE FROM TIME
0 admin cli console Thu Jun 21 14:50:09 2012

1 admin cli ssh(172.20.120.225) Thu Jun 21 15:19:09 2012
```

Related topics

- `config system admin`
- `config system global`

system performance

Displays the FortiWeb appliance's CPU usage, memory usage, average system load, and up time.

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.

System load is the average of percentages relative to the maximum possible capability of this FortiWeb appliance's hardware. It includes:

- average system load
- number of HTTP daemon/proxy processes or children
- memory usage
- disk swap usage

Syntax

```
get system performance
```

Example

```
FortiWeb # get system performance
CPU states: 4% used, 96% idle
Memory states: 18% used
System Load: 1
Up: 28 days, 11 hours, 38 minutes
```

Related topics

- get system status
- diagnose hardware cpu
- diagnose hardware mem
- diagnose hardware raid list
- diagnose system kill
- diagnose system top
- diagnose policy
- execute reboot

system status

Use this command to display system status information including:

- FortiWeb firmware version, build number and date
- FortiWeb appliance serial number and boot loader (“Bios”) version
- log hard disk availability
- host name
- operation mode, such as reverse proxy or transparent inspection
- current HA status for all appliances in the HA cluster (if HA is enabled)

Syntax

```
get system status
```

Example

```
get system status
International Version:FortiWeb-1000C 5.01,build0039,130726
Serial-Number:FV-1KC3R11700094
Bios version:04000002
Log hard disk:Available
Hostname:FortiWeb
Operation Mode:Reverse Proxy
Current HA mode=active-passive, Status=main
HA member :
Serial-Number Priority HA-Role
FV-1KC3R11700136 5 standby
FV-1KC3R11700094 1 main
```

Related topics

- `get system performance`
- `diagnose system ha status`
- `config system global`

waf signature-rules

Use this command to list the IDs, names, and descriptions of signature rules.

You specify signatures in the `config waf signature` command using the signature ID only. This command allows you to view the names and descriptions of the IDs.

Syntax

```
get waf signature rules
```

Example

```
get waf signature rules
```

This example output is the first four entries that the CLI displays when FortiWeb is configured with the default signatures only.

```
rule id : 110000009
main class id : 110000000
main class name : Bad Robot
sub class id : 000000000
sub class name : Bad Robot
rule description : This signature prevents Google Skipfish scanner from exploiting a
    vulnerability to include an arbitrary remote file with malicious PHP code and
    executing it in the context of the webserver process.
This attack can be achieved in HTTP request arguments.


rule id : 110000010
main class id : 110000000
main class name : Bad Robot
sub class id : 000000000
sub class name : Bad Robot
rule description : This signature checks whether the request came from Google Skipfish Web
    scanner .
The signature check region: user-agent field in http request header.


rule id : 110000011
main class id : 110000000
main class name : Bad Robot
sub class id : 000000000
sub class name : Bad Robot
```

```
rule description : This signature checks whether the request contains a string of a
    content scraper, which could be a part of virus.
The signature check region: user-agent field in http request header.


rule id : 110000012
main class id : 110000000
main class name : Bad Robot
sub class id : 000000000
sub class name : Bad Robot
rule description : This signature checks whether the request came from Acunetix Web
    Vulnerability Scanner .
The signature check region: http request url.
```

Related topics

- config waf signature

show

The `show` command displays parts of your FortiWeb appliance's configuration in the form of commands that are required to achieve that configuration from the firmware's default state.

The `show` commands require at least read (r) permission to applicable administrator profile groups.

Although not explicitly shown in this section, for all config commands, there are related get and `show` commands which display that part of the configuration. `get` and `show` commands use the same syntax as their related `config` command, unless otherwise mentioned. For syntax examples and descriptions of each configuration object, field, and option, see config on page 89.

Unlike `get`, `show` does **not** display settings that are assumed to remain in their default state.

For example, you might show the current DNS settings:

```
FortiWeb# show system dns
config system dns
   set primary 172.16.1.10
   set domain "example.com"
end
```

Notice that the command does **not** display the setting for the secondary DNS server. This indicates that it has not been configured, or has reverted to its default value.

Like `get`, depending on whether or not you have specified an object, `show` may display one of two different outputs, either the configuration:

- that you have just entered but not yet saved, or
- as it currently exists on the flash disk, respectively.

For example, immediately after configuring the secondary DNS server setting but **before** saving it, `show` displays two different outputs (differences highlighted in bold):

```
FortiWeb# config system dns
FortiWeb (dns)# set secondary 192.168.1.10
FortiWeb (dns)# show
config system dns
   set primary 172.16.1.10
   set secondary 192.168.1.10
   set domain "example.com"
end
FortiWeb (end)# show system dns
config system dns
   set primary 172.16.1.10
   set domain "example.com"
end
```

The first output from `show` indicates the value that you have configured but not yet saved; the second output from `show` indicates the value that was last saved to disk.

Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.