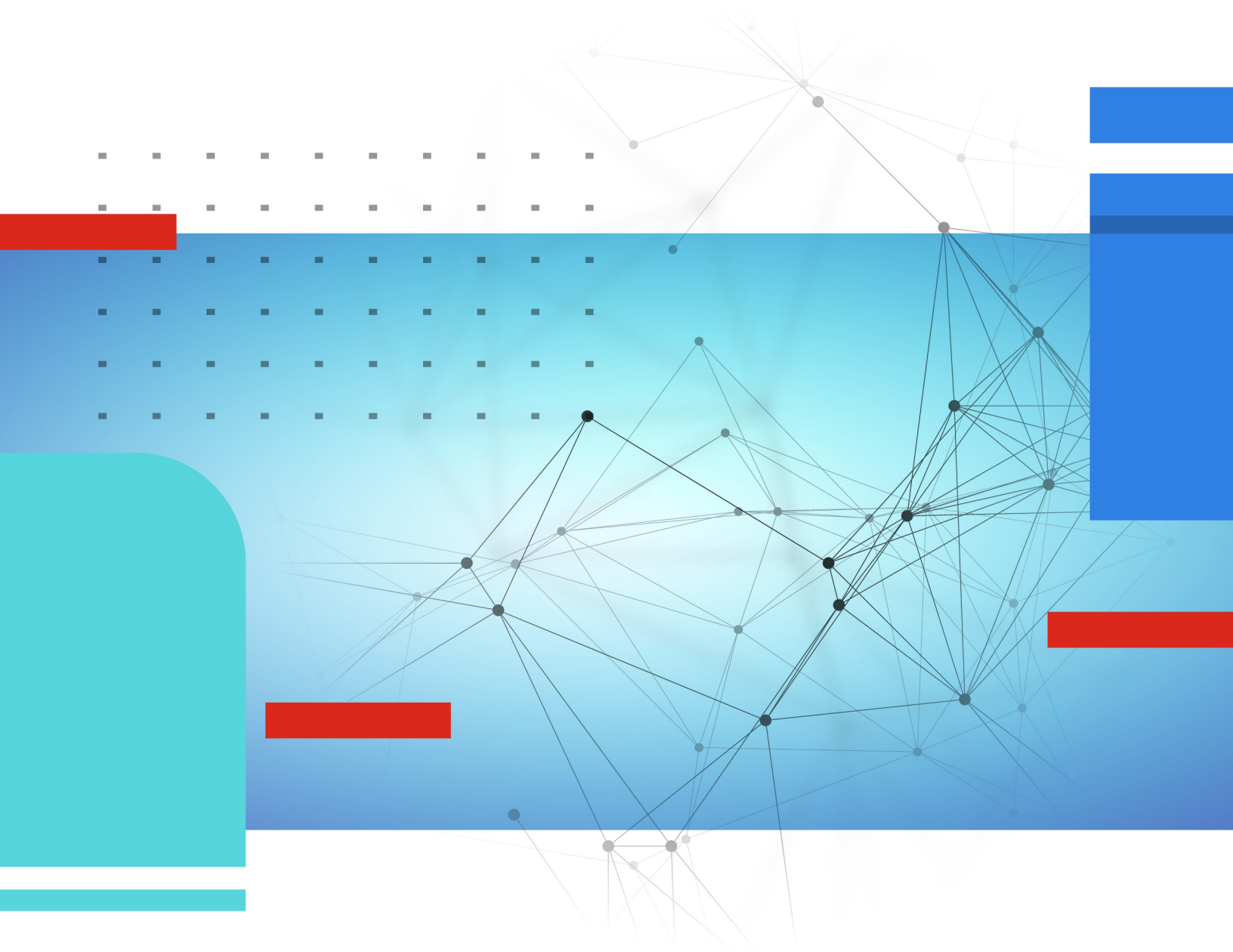




CLI Reference

FortiWeb 7.6.5





CLI Reference

FortiWeb 7.6.5

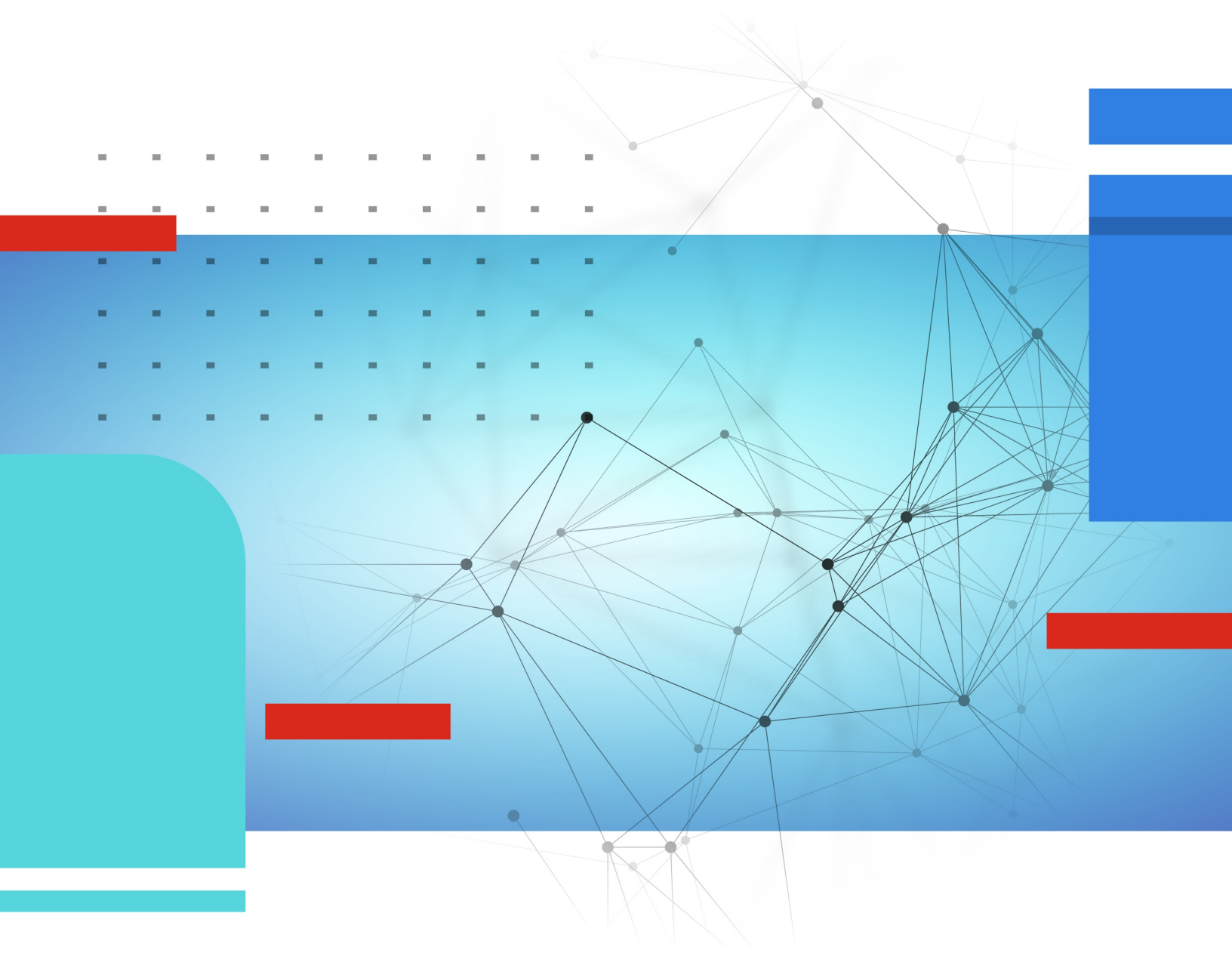


TABLE OF CONTENTS

Introduction	30
Scope	30
Conventions	31
IP addresses	31
Cautions, notes, & tips	31
Typographic conventions	32
Command syntax	32
Using the CLI	33
Connecting to the CLI	33
Connecting to the CLI using a local console	33
Enabling access to the CLI through the network (SSH or Telnet or CLI Console widget)	34
Connecting to the CLI using SSH	36
Connecting to the CLI using Telnet	37
Command syntax	39
Terminology	39
Indentation	40
Notation	40
Subcommands	42
Table commands	43
Field commands	45
Permissions	46
Access profile permissions	46
Tips & tricks	48
Help	48
Shortcuts & key commands	48
Command abbreviation	49
Special characters	49
Language support & regular expressions	50
Screen paging	51
Baud rate	52
Editing the configuration file in a text editor	52
Pipeline 'grep' command	53
Administrative domains (ADOMs)	55
Differences between administrator accounts when ADOMs are enabled	55
Defining ADOMs	57
Assigning administrators to an ADOM	58
config	60
log alertMail	60
Syntax	60
Example	61
Related topics	61
log attack-log	61
Syntax	61
Example	63

Related topics	63
log custom-sensitive-rule	64
Syntax	64
Example	65
Related topics	66
log disk	66
Syntax	66
Example	67
Related topics	67
log email-policy	68
Syntax	68
Example	70
Related topics	71
log event-log	71
Syntax	71
Example	72
Related topics	72
log forti-analyzer	72
Syntax	73
Example	74
Related topics	74
log fortianalyzer-policy	74
Syntax	75
Example	75
Related topics	76
log ftp-policy	76
Syntax	76
Related topics	77
log reports	77
Syntax	78
Example	85
Related topics	86
log sensitive	86
Syntax	86
Example	87
Related topics	87
log siem-message-policy	87
Syntax	88
Example	88
Related topics	88
log siem-policy	89
Syntax	89
Example	90
Related topics	90
log syslogd	91
Syntax	91
Example	92
log syslog-policy	93

Syntax	93
Example	94
Related topics	94
log traffic-log	95
Syntax	95
Example	96
Related topics	96
log trigger-policy	96
Syntax	97
Example	98
Related topics	98
router policy	98
Syntax	98
Related topics	99
router setting	100
Syntax	101
Example	101
Related topics	101
router static	101
Syntax	102
Example	103
Related topics	103
server-policy acceleration	103
Syntax	104
Related topics	105
server-policy allow-hosts	106
Syntax	107
Example	108
Related topics	109
server-policy allow-list	109
Syntax	109
Example	112
Related topics	112
server-policy health	112
Syntax	113
Example	117
Related topics	117
server-policy HTTP-content-routing-policy	118
Syntax	118
Example	124
Related topics	124
server-policy ip-group	124
Syntax	125
server-policy pattern custom-data-type	125
Syntax	125
Example	126
server-policy pattern custom-global-white-list-group	126

Syntax	126
Example	129
Related topics	129
server-policy pattern threat-score-profile	129
Syntax	129
Related Topics	132
server-policy pattern threat-weight	132
Syntax	132
Related Topics	146
server-policy persistence-policy	146
Syntax	147
Example	150
Related topics	150
server-policy policy	150
Syntax	152
Example	181
Related topics	182
server-policy server-pool	182
Syntax	183
Example	207
Related topics	207
server-policy service custom	207
Syntax	208
Example	208
Related topics	208
server-policy service predefined	208
Syntax	209
Example	209
Related topics	209
server-policy setting	210
Syntax	210
Related topics	214
server policy traffic-mirror	214
Syntax	214
Example	215
Related topics	215
server-policy vserver	215
Syntax	216
Example	217
Related topics	217
server-policy ztna-profile	217
Syntax	218
Related topics	218
server-policy ztna-rule	219
Syntax	219
Related topics	220
system accprofile	220
Syntax	221

Example	223
Related topics	223
system admin	223
Syntax	224
Example	228
Related topics	228
system admin-certificate ca	228
Syntax	229
Example	229
system admin-certificate intermediate-ca	229
Syntax	229
Example	230
Related topics	230
system admin-certificate intermediate-ca-group	230
Syntax	231
Related topics	231
system admin-certificate local	231
Syntax	232
Example	233
system advanced	233
Syntax	233
Related topics	236
system antivirus	236
Syntax	236
system automation-email	237
Syntax	238
Related topics	238
system automation-script	238
Syntax	238
Related topics	239
system automation-trigger	239
Syntax	239
Related topics	240
system automation-stitch	240
Syntax	240
Related topics	241
system autoupdate override	241
Syntax	242
Related topics	242
system autoupdate schedule	242
Syntax	243
Example	243
Related topics	243
system autoupdate tunneling	244
Syntax	244
Example	244
Related topics	245

system backup	245
Syntax	245
Related topics	247
system captcha	247
Syntax	247
system central-management	248
Syntax	248
Example	249
system certificate ca	249
Syntax	249
Example	250
Related topics	250
system certificate ca-group	251
Syntax	251
Example	252
Related topics	252
system certificate crt	252
Syntax	252
Related topics	253
system certificate crt-group	253
Syntax	253
Related topics	254
system certificate intermediate-certificate	254
Syntax	254
Example	255
Related topics	255
system certificate intermediate-certificate-group	255
Syntax	256
Related topics	256
system certificate letsencrypt	256
Syntax	256
Related topics	258
system certificate local	258
Syntax	259
Example	260
Related topics	261
system certificate multi-local	261
Syntax	261
Related topics	262
system certificate ocsp-stapling	262
Syntax	262
Related topics	263
system certificate server-certificate-verify	263
Syntax	263
Related topics	264
system certificate sni	264
Syntax	264

Related topics	266
system certificate xml-client-certificate	266
Syntax	266
Related topics	267
system certificate tsl-ca	267
Syntax	267
Related topics	267
system certificate urlcert	268
Syntax	268
Related topics	268
system certificate verify	269
Syntax	269
Related topics	270
system certificate xml-client-certificate-group	270
Syntax	270
Related topics	271
system conf-sync	271
Syntax	271
Related topics	273
system console	273
Syntax	273
Example	274
Related topics	274
system cpumem-monitor	274
system csf	276
Syntax	276
Related topics	277
system decoding enhancement	277
Syntax	277
Example	278
Related Topic(s)	279
system dns	279
Syntax	279
Example	280
Related topics	280
system encryption-method	280
system endpoint-control	281
Syntax	281
Related topics	282
system eventhub	282
Syntax	283
Related topics	284
system external-resource	284
Syntax	284
Related topics	286
system fail-open	286
Syntax	287

Related topics	287
system fds proxy	287
Syntax	287
Example	288
system feature-visibility	288
Syntax	289
Related Topics	290
system fips-cc	291
Syntax	291
system firewall address	293
Syntax	293
Related topics	294
system firewall service	294
Syntax	294
Related topics	295
system firewall firewall-policy	295
Syntax	295
Example	297
Related topics	297
system firewall fwmark-policy	297
Syntax	297
Example	298
system firewall admin-policy	299
Syntax	299
Related topics	300
system firewall dn timer policy	300
Syntax	300
Related Topic	302
system firewall snat-policy	302
Syntax	302
Related Topic	303
system fortigate-integration	304
Syntax	304
Related topics	305
system fortisandbox	305
Syntax	305
Example	306
Related topics	307
system global	307
Syntax	307
Example	318
Related topics	318
system ha	319
Syntax	319
Example	332
Related topics	332
system ha-aa-server-policy-hlck	332

Syntax	333
Example	335
system ha-mgmt-router-static	335
Syntax	336
system ha-mgmt-router-policy	336
Syntax	336
system ha-node	337
Syntax	337
Example	338
system icapserver	338
Syntax	338
Example	339
Related topics	339
system ha-traffic-distribution	339
Syntax	340
Example	340
system hsm info	340
Syntax	341
Related topics	342
system hsm partition	342
Syntax	342
Related topics	342
system icapserver	343
Syntax	343
Example	344
Related topics	344
system interface	344
Syntax	345
Example	350
Example	350
Related topics	350
system ip-detection	351
Syntax	351
Related topics	351
system manager-mode	351
Syntax	351
system nethsm	353
system network-option	355
Syntax	355
Example	360
Related topics	360
system ntp	360
Syntax	360
Example	361
system object-tagging	362
Syntax	362
system password-policy	362

Syntax	362
Example	364
system raid	364
Syntax	365
Example	365
Related topics	365
system recaptcha-api	365
Syntax	366
system replacemsg-image	366
Syntax	366
system saml	367
Syntax	367
Related topics	368
system sdn-connector	368
Syntax	368
Related topics	372
system settings	372
Syntax	373
Related topics	375
system snmp community	375
Syntax	375
Example	379
Related topics	379
system snmp sysinfo	379
Syntax	379
Example1234	380
Related topics	381
system snmp user	381
Syntax	381
Example	385
Related topics	385
system sso-admin	385
Syntax	385
Related topics	386
system tcpdump	386
Syntax	386
Related topics	387
system vip	387
Syntax	387
system v-zone	388
Syntax	389
Example	390
Related topics	390
system wccp	390
Syntax	391
Example	393
Related topics	393

system certificate xml-server-certificate	393
Syntax	393
Related topics	394
user admin-usergrp	394
Syntax	394
Example	395
Related topics	396
user kerberos-user	396
Syntax	396
Related topics	397
user ldap-user	397
Syntax	397
Example	400
Related topics	400
user local-user	401
Syntax	401
Example	401
Related topics	402
user ntlm-user	402
Syntax	402
Example	402
Related topics	403
user oauth-user request	403
Syntax	403
Related topics	404
user oauth-user server	404
Syntax	404
Related topics	406
user pki-user	406
Syntax	406
Example	407
user radius-user	407
Syntax	407
Related topics	409
user recaptcha-user	409
Syntax	409
user saml-user	410
Syntax	410
Example	411
Related topic	412
user tacacs+ user	412
Related topics	413
user user-group	413
Syntax	413
Example	414
Related topics	415
wad file-filter	415
Syntax	415

Example	416
Related topics	416
wad website	416
Syntax	417
Example	420
Related topics	420
waf advanced-bot-protection	420
Syntax	421
Related topics	423
waf allow-method-exceptions	423
Syntax	423
Example	425
Related topics	425
waf allow-method-policy	426
Syntax	426
Example	427
Related topics	428
waf api-learning-policy	428
Syntax	428
waf api-learning-rule	430
waf api-policy	431
Syntax	431
Related topics	432
waf api-rules	432
Syntax	432
Related topics	436
waf api-users	437
Syntax	437
Related topics	439
waf api-user-group	439
Syntax	439
Related topics	439
waf application-layer-dos-prevention	440
Syntax	440
Example	441
Related topics	441
waf base-signature-disable	442
Syntax	442
Example	442
Related topics	442
waf biometrics-based-detection	442
Syntax	443
Related topics	446
waf bot-detection-policy	446
Syntax	446
waf bot-mitigation-exception	455
Syntax	455

Related topics	459
waf bot-mitigation-policy	459
Syntax	459
Related topics	460
waf cookie-security	460
Syntax	460
Related topics	464
waf csrf-protection	464
Syntax	464
Example	467
waf custom-access policy	468
Syntax	468
Example	469
Related topics	469
waf custom-access rule	469
Syntax	469
Example	484
Related topics	485
waf custom-protection-group	485
Syntax	485
Example	486
Related topics	486
waf custom-protection-rule	486
Syntax	487
Example	491
Related topics	491
waf dlp exception	492
waf exclude-url	493
Syntax	493
Example	494
Related topics	495
waf file-compress-rule	495
Syntax	495
Example	497
Related topics	497
waf file-upload-restriction-policy	497
Syntax	497
Related topics	501
waf file-upload-restriction-rule	501
Syntax	501
Example	505
Related topics	505
waf ftp-command-restriction-rule	505
Syntax	506
Related Topic	507
waf ftp-file-security	508
Syntax	508
Related Topic	510

waf ftp-protection-profile	510
Syntax	510
Related Topics	511
waf geo-block-list	511
Syntax	512
Example	513
Related topics	514
waf geo-ip-except	514
Syntax	514
Example	515
Related topics	515
waf graphql-validation rule	515
Syntax	515
Related topics	519
waf grpc-security rule	519
Syntax	519
Related topics	521
waf grpc-security policy	521
Syntax	521
Related topics	522
waf hidden-fields-protection	522
Syntax	522
Related topics	523
waf hidden-fields-rule	523
Syntax	523
Example	526
Related topics	527
waf HTTP-authen HTTP-authen-policy	527
Syntax	527
Example	528
Related topics	529
waf HTTP-authen HTTP-authen-rule	529
Syntax	530
Example	531
Related topics	532
waf HTTP-connection-flood-check-rule	532
Syntax	532
Related topics	533
waf HTTP-constraints-exceptions	534
Syntax	534
Example	539
Related topics	540
waf HTTP-header-security	540
Syntax	540
Example	543
waf HTTP-protocol-parameter-restriction	543
Syntax	544
Example	547

Related topics	547
waf HTTP-request-flood-prevention-rule	547
Syntax	547
Example	550
Related topics	550
waf input-rule	551
Syntax	551
Example	555
Related topics	556
waf ip-intelligence	556
Syntax	556
Example	558
Related topics	559
waf ip-intelligence-exception	559
Syntax	559
Example	560
Related topics	560
waf ip-intelligence-ignore-x-forwarded-for	560
Syntax	560
Related topics	560
waf ip-list	561
Syntax	561
Example	564
Related topics	564
waf json-schema	565
Syntax	565
Related topics	565
waf json-schema group	565
Syntax	566
Related topics	566
waf json-validation rule	566
Syntax	566
Example	570
Related topics	570
waf known-bots	571
Syntax	571
Related Topics	582
waf layer4-access-limit-rule	582
Syntax	583
Example	585
Related topics	586
waf layer4-connection-flood-check-rule	586
Syntax	586
Example	588
Related topics	588
waf link-cloaking link-cloaking-rule	588
waf link-cloaking link-cloaking-policy	589

waf machine-learning url-replacer-rule/policy	590
Syntax	590
Related Topic	593
waf machine-learning-policy	593
Syntax	593
Related Topics	599
waf mitb-policy	600
Syntax	600
Related topics	600
waf mitb-rule	600
Syntax	600
Related topics	602
waf mobile-api-protection	602
Syntax	602
waf openapi-file	605
Syntax	605
Related topics	605
waf openapi-validation-policy	605
Syntax	605
Related topics	606
waf padding-oracle	606
Syntax	607
Example	609
Related topics	610
waf parameter-validation-rule	610
Syntax	610
Example	611
Related topics	611
waf signature	612
Syntax	613
Example	620
Related topics	621
waf signature_update_policy	621
Syntax	621
Example	621
Related topics	621
waf site-publish-helper authentication-server-pool	622
Syntax	622
Example	623
Related topics	623
waf site-publish-helper form-based-delegation	623
Syntax	623
waf site-publish-helper policy	624
Syntax	624
Example	626
Related topics	626
waf site-publish-helper rule	626
Syntax	627

Example	637
Related topics	638
waf site-publish-helper saml-spool	639
Syntax	639
Related topics	639
waf staged_signature_list	640
Syntax	640
Example	640
Related topics	640
waf syntax-based-attack-detection	640
Syntax	641
Related topics	658
waf threshold-based-detection	658
Syntax	658
Related Topics	664
waf url-access url-access-policy	664
Syntax	665
Example	665
Related topics	665
waf url-encryption	666
Syntax	666
Related topics	668
waf url-access-parameter	668
Syntax	669
waf url-access url-access-rule	669
Syntax	670
Example	674
Related topics	674
waf url-rewrite url-rewrite-policy	675
Syntax	675
Related topics	675
waf url-rewrite url-rewrite-rule	676
Syntax	677
Related topics	684
waf user-tracking policy	684
Syntax	684
waf user-tracking rule	685
Syntax	685
Example	690
Related topics	691
waf waiting-room policy	691
Syntax	691
waf web-cache-rule/policy	693
Syntax	693
waf web-protection-profile inline-protection	696
Syntax	697
Related topics	705

waf web-protection-profile offline-protection	706
Syntax	706
Related topics	712
waf webshell-detection-policy	712
Syntax	712
Related topics	715
waf websocket-security rule	715
Syntax	716
Related topics	717
waf websocket-security policy	717
Syntax	717
Related topics	718
waf ws security	718
Syntax	718
Related topics	720
waf x-forwarded-for	721
Syntax	721
Example	724
waf xml-dtd	725
Syntax	725
Related topics	725
waf xml-exempted-urls	726
Syntax	726
Related topics	726
waf xml-schema	727
Syntax	727
Related topics	727
waf xml-validation	727
Syntax	727
Example	734
Related topics	734
waf xml-wsdl	735
Syntax	735
Related topics	735
waf xsw-detection rule	735
Syntax	735
Related topics	736
wvs limit	737
Syntax	737
Example	737
Related topics	738
wvs policy	738
Syntax	738
Example	739
Related topics	739
wvs profile	740
Syntax	740
Related topics	743

wvs schedule	743
Syntax	744
Example	745
Related topics	745
wvs template	745
Syntax	745
Example	746
Related topics	746
diagnose	747
debug	747
Syntax	748
Related topics	748
debug application	748
Syntax	749
Related topics	749
debug asan	749
Syntax	749
debug cli	750
Syntax	750
Related topics	751
debug cmdb	751
Syntax	751
Related topics	752
debug comlog	752
Syntax	752
debug console timestamp	752
Syntax	753
Related topics	753
debug coredumplog	753
Syntax	753
Related Topic	753
debug crashlog	754
Syntax	754
Example	754
debug daemonlog	754
Syntax	755
Related Topic	755
debug dnsproxy list	755
Syntax	755
Example	755
Related topics	755
debug emerglog	755
Syntax	756
debug flow filter	756
Syntax	756
Related topics	758
debug flow filter module-bypass-info	758

Syntax	758
debug flow reset	759
Syntax	759
Related topics	759
debug flow trace	759
Syntax	759
Example	759
Related topics	762
debug ha	762
Syntax	762
debug info	763
Syntax	763
Example	763
Related topics	764
debug init	764
Syntax	764
debug jemalloc-heap	764
Syntax	764
diagnose debug jemalloc proxyd	765
debug netstatlog	766
Syntax	767
Related Topic	767
debug nowaf	767
Syntax	767
Related topics	768
debug pkcs11providerlog	768
debug proxy log	768
Syntax	768
Related Topic	769
debug primuslog	769
debug reset	769
Syntax	769
Related topics	770
debug shell-access history show	770
Syntax	770
debug trace report	770
Syntax	770
Related topics	771
debug trace tcpdump	771
Syntax	771
Related topics	771
debug upload	772
Syntax	772
Example	772
Related topics	772
ha synchronize health-check	772
Syntax	773

hardware bypass info	773
Syntax	773
hardware check	773
Syntax	773
Example	774
hardware cpld info	774
Syntax	774
hardware cpu	774
Syntax	774
Example	775
Related topics	775
hardware fail-open	775
hardware harddisk	775
Syntax	776
Example	776
Related topics	776
hardware interrupts	776
Syntax	777
Example	777
Related topics	777
hardware logdisk info	777
Syntax	778
Example	778
Related topics	778
hardware mem	778
Syntax	778
Example	778
Related topics	779
hardware nic	779
Syntax	780
Example	780
Related topics	781
hardware raid list	782
Syntax	782
Example	782
Related topics	782
hardware raid-card info	782
Syntax	782
index	783
Syntax	783
Example	783
Related topics	783
log	784
Syntax	784
Example	784
Related topics	784
network arp	785
Syntax	785

Example	785
Related topics	786
network ip	786
Syntax	786
Example	786
Example	787
Related topics	787
network route	787
Syntax	787
Example	788
Example	788
Related topics	788
network rtcache	789
Syntax	789
Example	789
Example	789
Related topics	790
network sniffer	790
Syntax	790
Example	792
Example	792
Example	793
network tcp list	795
Syntax	795
Example	795
Related topics	796
network udp list	796
Syntax	796
Example	796
Related topics	797
policy	797
Syntax	797
Example	798
Related topics	798
system endpoint-control	799
Syntax	799
system flash	799
Syntax	799
Example	800
Related topics	800
system ha backup-config	800
Syntax	800
Example	800
	800
system ha confd_status	800
Syntax	801
Example	801
system ha dev-info	801

Syntax	802
Example	802
system ha export-eventlog	803
Syntax	803
Example	803
	803
system ha file-log	803
Syntax	803
system ha file-stat	804
Syntax	804
Example	804
Related topics	804
system ha interface-macinfo	805
Syntax	805
Example	805
Related topics	805
system ha mac	806
Syntax	806
Example	806
Related topics	806
system ha md5fixed	806
system ha md5sum-gen	807
system ha nodes	807
Syntax	807
Example	807
system ha sessions_stat	807
Syntax	807
Example	807
system ha status	808
Syntax	808
Example	808
Related topics	809
system ha sync-config	809
Syntax	809
system ha sync-stat	809
Syntax	809
Example	810
Related topics	810
system ha traffic-distribution	810
Syntax	810
Example	811
system jeprof	811
Syntax	811
system kill	812
Syntax	812
Related topics	813
system mount	813

Syntax	813
Example	813
Related topics	813
system top	813
Syntax	814
Example	814
Related topics	815
system update info	815
Syntax	815
Example	815
system waf-signature pcre-high-cpu-cost	818
Related topics	819
test application	819
execute	820
backup cert-config	820
Syntax	820
Example	820
Related topics	820
backup cli-config	821
Syntax	821
Example	822
Related topics	822
backup full-config	822
Syntax	822
Example	823
Related topics	823
backup full-config-with-ML-data	823
Syntax	823
Example	824
Related topics	824
backup web-protection-profile	824
Syntax	824
Example	825
Related topics	825
batch	825
Syntax	825
create-raid level	826
Syntax	826
Related topics	827
create-raid rebuild	827
Syntax	827
Example	828
Related topics	828
date	828
Syntax	828
Example	828
Related topics	829

db rebuild	829
Syntax	829
Related topics	829
dnscache-cleanup	829
Syntax	829
erase-disk	829
Syntax	830
factoryreset	830
Syntax	830
Related topics	830
fctems	831
Syntax	831
Related topics	831
fdnserver delete	831
Syntax	831
Related topics	831
fdnserver show	832
Syntax	832
Example	832
Related topics	832
formatlogdisk	832
Syntax	832
Related topics	832
forticloud-sandbox	833
ha disconnect	833
Syntax	834
Example	834
Related topics	834
ha manage	835
Syntax	835
Example	835
Related topics	835
ha md5sum	836
Syntax	836
Example	836
Related topics	836
ha synchronize	836
Syntax	836
Example	837
Related topics	837
icap-cache-clear	837
Syntax	838
Example	838
ping	838
Syntax	838
Example	838
Example	839
Related topics	839

ping6	839
Syntax	840
Example	840
Related topics	840
ping-options	841
Syntax	841
Example	842
Related topics	842
ping6-options	842
Syntax	842
Example	843
Related topics	844
private-encryption-key	844
reboot	845
Syntax	845
Example	845
Related topics	846
redis rebuild	846
Syntax	846
Related topics	846
remove vmlicense	846
Syntax	846
Example	846
Related Topics	847
restore cert-config	847
Syntax	847
Example	847
Related topics	848
restore config	848
Syntax	848
Example	848
Related topics	849
restore image	849
Syntax	849
Example	849
Related topics	850
restore secondary-image	850
Syntax	850
Example	850
Related topics	851
restore vmlicense	851
Syntax	851
Example	852
sandbox-cache-clear	852
Syntax	852
Example	852
session-cleanup	852
Syntax	853

shutdown	853
Syntax	853
Example	853
Related topics	853
telnet	854
Syntax	854
Example	854
Related topics	854
telnettest	854
Syntax	855
Example	855
Related topics	855
time	856
Syntax	856
Example	856
Related topics	856
traceroute	857
Syntax	857
Example	857
Example	857
Example	858
Related topics	858
ttp_src_ip_whitelist	859
update-now	860
Syntax	860
get	861
system fortisandbox-statistics	862
Syntax	862
Example	863
Related topics	863
system performance	863
Syntax	863
Example	863
Related topics	864
system status	864
Syntax	864
Example	864
Related topics	865
waf predefined-global-allow-list	865
Syntax	865
waf signature-rules	865
Syntax	865
Example	865
Related topics	866
show	867

Introduction

This document describes how to use the command line interface (CLI) of FortiWeb. It assumes that you have already successfully deployed FortiWeb and completed basic setup by following the instructions in the *FortiWeb Administration Guide*: <http://docs.fortinet.com/fortiweb/admin-guides>.

Scope

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 or first-time setup. For that information, see the *FortiWeb Administration Guide*: <http://docs.fortinet.com/fortiweb/admin-guides>.

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

<https://tools.ietf.org/html/rfc1918>

RFC 5737: IPv4 Address Blocks Reserved for Documentation

<https://tools.ietf.org/html/rfc5737>

RFC 3849: IPv6 Address Prefix Reserved for Documentation

<https://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 192.0.2.108, 198.51.100.155, or 203.0.113.79.

Cautions, notes, & tips

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



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



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



Present 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	<pre>config system dns set primary <address_ipv4> end</pre>
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	Enter a name for the remote VPN peer or client, such as <code>Central_Office_1</code> .
Navigation	Go to VPN > IPSEC > Auto Key (IKE) .
Publication	For details, see the <i>FortiWeb Administration Guide</i> : https://docs.fortinet.com/document/fortiweb .

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 40](#).

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. 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 FortiWeb, or if you are new to the CLI, this section can help you to become familiar with using it.

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 a 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, including when you're:

- Installing FortiWeb for the first time and it's 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. For details, see the *FortiWeb Administration Guide*:
<http://docs.fortinet.com/fortiweb/admin-guides>
- Restoring the firmware and FortiWeb 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 must enable SSH, 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 (<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>)



The following instructions describe connecting to the CLI using PuTTY; steps may vary with other terminal emulators.

To connect to the CLI using a local console connection

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.

On your management computer, start PuTTY.

In the **Category** tree on the left, go to **Connection > Serial** and configure these settings:

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

In the **Category** tree on the left, go to **Session** (not the sub-node, **Logging**).

From **Connection type**, select **Serial**.

Click **Open**.

Press the Enter key to initiate a connection.

Enter a valid administrator account name (such as `admin`) then press Enter.

Enter the password for that administrator account and press Enter. By default, 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, and configure 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 34](#).

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*:
<http://docs.fortinet.com/fortiweb/admin-guides>

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. For details, see [router static on page 101](#).

You can do this using either:

- A local console connection (see the following procedure)
- The web UI (see the *FortiWeb Administration Guide*; <http://docs.fortinet.com/fortiweb/admin-guides>)

Requirements

- A computer with an available serial communications (COM) port and RJ-45 port
- Terminal emulation software such as PuTTY (<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>)
- 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

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

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.

Note the number of the physical network port.

Using a local console connection, connect and log into the CLI. For details, see [Connecting to the CLI using a local console on page 33](#).

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.

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.

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 [router static on page 101](#).

To connect to the CLI through the network interface, see [Connecting to the CLI using SSH on page 36](#) or [Connecting to the CLI using Telnet on page 37](#).

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 34](#))
- an SSH client such as PuTTY (<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>)



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

To connect to the CLI using SSH

On your management computer, start PuTTY.

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

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

In **Port**, enter 22.

For **Connection type**, select **SSH**.

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.

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.

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

Alternatively, you can log in using an SSH key. For details, see [system admin on page 223](#).

Enter 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 34](#))
- Terminal emulation software such as PuTTY (<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>)



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

To connect to the CLI using Telnet

On your management computer, start PuTTY.

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

In **Port**, enter `23`.

For **Connection type**, select **Telnet**.

Click **Open**.

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

Type the password for this administrator account and press Enter.

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



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.

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
```

This document uses the following conventions to describe valid command syntax.

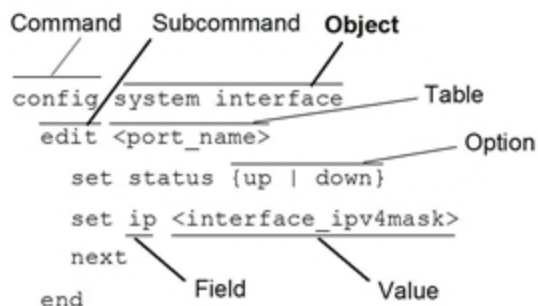
Terminology

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
```

This document uses the below 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 FortiWeb 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. For details, see [Shortcuts & key commands on page 48](#).

Valid command lines must be unambiguous if abbreviated. For details, see [Command abbreviation on page 49](#).

Optional words or other command line permutations are indicated by syntax notation. For details, see [Notation on page 40](#).

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. For details, see [Indentation on page 40](#).

Not all top-level commands have subcommands. Available subcommands vary by their containing scope. For details, see [Subcommands on page 42](#).

- **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. For details, see [Notation on page 40](#).
- **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. For details, see [Notation on page 40](#).
- **Option**—A kind of value that must be one or more words from a fixed set of options. For details, see [Notation on page 40](#).

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 details about available subcommands, see [Subcommands on page 42](#).

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

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 [].

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.

Non-mutually exclusive options. For example:

```
{HTTP HTTPS ping snmp ssh telnet}
```

Options delimited by spaces

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.

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 `192.0.2.99`.
- **<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 `192.0.2.99 255.255.255.0`.
- **<xxx_ipv4/mask>** — A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as `192.0.2.99/24`.
- **<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. For details, see [Special characters on page 49](#).
- **<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 45](#))
- Commands that affect tables (see [Table commands on page 43](#))



Subcommand scope is indicated in this [FortinetVariables.Document title3] by indentation. For details, see [Indentation on page 40](#).

Syntax examples for each top-level command in this [FortinetVariables.Document title3] 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 <code>config system admin</code>, you could delete an administrator account named <code>newadmin</code> by typing <code>delete newadmin</code> and pressing Enter. This deletes <code>newadmin</code> and all its fields, such as <code>newadmin's first-name</code> and <code>email-address</code>. <code>delete</code> is only available within objects containing tables.
edit <table_name>	Create or edit a table in the current object. For example, in <code>config system admin</code>: • Edit the settings for the default <code>admin</code> administrator account by

	typing <code>edit admin</code>. • Add a new administrator account with the name <code>newadmin</code> and edit <code>newadmin</code>'s settings by entering <code>edit newadmin</code>. <code>edit</code> is an interactive subcommand: further subcommands are available from within <code>edit</code>. <code>edit</code> changes the prompt to reflect the table you are currently editing. <code>edit</code> is only available within objects containing tables.
end	Save the changes to the current object and exit the <code>config</code> command. This returns you to the top-level command prompt.
get	List the configuration of the current object or table. • In objects, <code>get</code> lists the table names (if present), or fields and their values. • In a table, <code>get</code> lists the fields and their values. For more information on <code>get</code> commands, see get on page 861.
purge	Remove all tables in the current object. For example, in <code>config user local-user</code>, you could type <code>get</code> to see the list of all local user names, then type <code>purge</code> and then <code>y</code> to confirm that you want to delete all users. <code>purge</code> 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 backup cli-config on page 821. Caution: Do not purge <code>system interface</code> or <code>system admin</code> 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 <code>show</code> commands, see show on page 867.

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 <code>edit</code> and/or <code>config</code> commands without saving the fields.
end	Save the changes made to the current table or object fields, and exit the <code>config</code> command. To exit without saving, use <code>abort</code> instead.
get	List the configuration of the current object or table. • In objects, <code>get</code> lists the table names (if present), or fields and their values. • In a table, <code>get</code> lists the fields and their values.
next	Save the changes you have made in the current table's fields, and exit the <code>edit</code> command to the object prompt. To save and exit completely to the root prompt, use <code>end</code> instead. <code>next</code> is useful when you want to create or edit several tables in the same object, without leaving and re-entering the <code>config</code> command each time. <code>next</code> 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 <code>config system admin</code>, after entering <code>edit admin</code>, you could enter <code>set password newpass</code> to change the password of the <code>admin</code> administrator to <code>newpass</code>. Note: When using <code>set</code> to change a field containing a space-delimited list, enter the whole new list. For example, <code>set <field> <new-value></code> will replace the list with the <code><new-value></code> rather than appending <code><new-value></code> 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 <code>config system admin</code>, after entering <code>edit admin</code>, entering <code>unset password</code> resets the password of the <code>admin</code> 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)
- Both **Read** and **Write** (view access, and change and execute access)
- No access

to each area of the FortiWeb software. For details about configuring the access profile for an administrator account to use, see [system accprofile on page 220](#).

Access profile permissions

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
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	Network ...	Web UI
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 ...	CLI

	<pre> execute date ... execute ha ... execute ping ... execute ping-option ... execute traceroute ... execute time ... </pre>	
Server Policy Configuration	Policy > Server Policy ... Server Objects ... Application Delivery ...	Web UI
traroutegrp	<pre> config server-policy ... except custom-application ... config waf file-compress-rule config waf HTTP-authen ... config waf url-rewrite ... diagnose policy ... </pre>	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
wafgrp	<pre> config system dos-prevention config waf except: • config waf file-compress-rule • config waf HTTP-authen ... • config waf url-rewrite ... • config waf web-custom-robot • config waf web-robot • config waf x-forwarded-for </pre>	CLI
Machine Learning Configuration	Web Protection > ML Based Anomaly Detection Bot Mitigation > ML Based Bot Detection API Protection > ML Based API Protection	Web UI
mlgrp	<pre> config waf api-learning-rule config waf api-learning-policy config waf bot-detection-policy config waf machine-learning-policy </pre>	CLI
Web Vulnerability Scan Configuration	Web Vulnerability Scan ...	Web UI
wvsgrp	config wvs ...	CLI
* For each <code>config</code> command, there is an equivalent <code>get/show</code> command, unless otherwise noted. <code>config</code> access requires write permission. <code>get/show</code> 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 `admin` administrator account.

Tips & tricks

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

This section includes:

- [Help on page 48](#)
- [Shortcuts & key commands on page 48](#)
- [Command abbreviation on page 49](#)
- [Special characters on page 49](#)
- [Language support & regular expressions on page 50](#)
- [Screen paging on page 51](#)
- [Baud rate on page 52](#)
- [Editing the configuration file in a text editor on page 52](#)
- [Pipeline 'grep' command on page 53](#)

Help

To display brief help during command entry, enter the question mark (?) key:

- At the command prompt to display a list of the commands available and a description of each.
- After a command keyword to display a list of the objects available with that command and a description of each.
- After entering a word or part of a word 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.	Tab

Action	Keys
Press the key multiple times to cycle through available matches.	
Recall the previous command. Command memory is limited to the current session.	Up arrow, or Ctrl + P
Recall the next command.	Down arrow, or Ctrl + N
Move the cursor left or right within the command line.	Left or Right arrow
Move the cursor to the beginning of the command line.	Ctrl + A
Move the cursor to the end of the command line.	Ctrl + E
Move the cursor backwards one word.	Ctrl + B
Move the cursor forwards one word.	Ctrl + F
Delete the current character.	Ctrl + D
Abort current interactive commands, such as when entering multiple lines. If you are not currently within an interactive command such as <code>config</code> or <code>edit</code> , 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
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

The CLI currently supports the following languages:

- 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.

FortiWeb stores inputs 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 if the symbol is entered using the wrong encoding.

For best results, you should use:

- UTF-8 encoding.
- 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.
- Regular expressions that match HTTP requests.
- 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:

- **CLI access via the web UI**—Configure your web browser to interpret the page as UTF-8 encoded. The console will then display non-ASCII characters in commands in their character code equivalent.
 - **CLI access via a Telnet or SSH client**—Configure the client to send and receive characters using UTF-8 encoding. Depending on the client, you may have to enter non-ASCII characters in commands in their character code equivalent.
-

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.
- Enter `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 details, see [system console on page 273](#).

Baud rate

You can change the default baud rate of the local console connection. For details, see [system console on page 273](#).

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
- 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 (<http://www.barebones.com/products/textwrangler>) and Notepad++ (<http://notepad-plus-plus.org>).



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

Use [backup cli-config on page 821](#) or [backup full-config on page 822](#) to download the configuration file to a TFTP server, such as your management computer.

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.

Use [restore config on page 848](#) 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.

Pipeline 'grep' command

FortiWeb supports 'grep' in `get` and `show` to search for desired information and present the results in a format you want.

The 'grep' command format is as follows:

```
get <xxx> [ [path] <object> ] | grep [options] <search string>
```

```
show [ [path] <object> ] | grep [options] <search string>
```

For example:

```

login as: admin
admin@10.200.30.101's password:
FortiWeb # get system status
International Version: FortiWeb-1000E 6.0.2,build0047(Interim),181030
Serial-Number: FV-1KE4417900014
Bios version: 00010002
Log hard disk: Available
Hostname: FortiWeb
Operation Mode: Reverse Proxy
FIPS-CC mode: disabled
Current HA mode: standalone
Database Status: Available

FortiWeb # get system status | grep version
Bios version: 00010002

FortiWeb # get system status | grep version -v
International Version: FortiWeb-1000E 6.0.2,build0047(Interim),181030
Serial-Number: FV-1KE4417900014
Log hard disk: Available
Hostname: FortiWeb
Operation Mode: Reverse Proxy
FIPS-CC mode: disabled
Current HA mode: standalone
Database Status: Available

FortiWeb # get system status | grep version -c
1

FortiWeb # get system status | grep version -n
3:Bios version: 00010002

FortiWeb # get system status | grep version
Bios version: 00010002

FortiWeb # get system status | grep version -n
3:Bios version: 00010002

FortiWeb # get system status | grep version -i
International Version: FortiWeb-1000E 6.0.2,build0047(Interim),181030
Bios version: 00010002

```

The following options are supported:

-n	Add 'line_no:' prefix.
-o	Show only the matching part of the line.
-v	Select non-matching lines.
-i	Ignore the case.
-w	Match whole words only.

-x	Match whole lines only.
-F	PATTERN is a literal (not regexp).
-E	PATTERN is an extended regexp.

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 you're 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

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

If ADOMs are enabled and you log in as `admin`, a superset of the typical CLI commands appear, allowing unrestricted access and ADOM configuration.

`config global` contains settings used by the FortiWeb itself and settings shared by ADOMs, such as RAID and administrator accounts. It does not include ADOM-specific settings or data, such as logs and reports. When configuring other administrator accounts, an additional option appears allowing you to restrict other administrators to an ADOM.

If ADOMs are enabled and you log in as any other administrator, you enter the ADOM assigned to your account. A subset of the typical menus or CLI commands appear, allowing access only to only logs, reports, policies, servers, and LDAP queries specific to your ADOM. You cannot access global configuration settings or enter other ADOMs.

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

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

To enable ADOMs

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 details about how to back up the configuration, see [backup full-config on page 822](#).

Enter the following commands:

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

FortiWeb terminates your administrative session.

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.

Continue by defining ADOMs. For details, see [Defining ADOMs on page 57](#).

To disable ADOMs

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 details about how to back up the configuration, see [backup full-config on page 822](#).

Enter the following commands:

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

FortiWeb terminates your administrative session.

Continue by reconfiguring the appliance. For details, see the *FortiWeb Administration Guide*:

<http://docs.fortinet.com/fortiweb/admin-guides>

See also

- [Permissions on page 46](#)
- [Defining ADOMs on page 57](#)
- [Assigning administrators to an ADOM on page 58](#)
- [system admin on page 223](#)
- [system accprofile on page 220](#)

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
- [ping on page 838](#) 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

Log in with the `admin` account.

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. For details, see the *FortiWeb Administration Guide*:

<http://docs.fortinet.com/fortiweb/admin-guides>

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

Either:

- Assign another administrator account to configure the ADOM (continue with [Assigning administrators to an ADOM on page 58](#)), 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 on page 58](#)
- [Administrative domains \(ADOMs\) on page 55](#)
- [Permissions on page 46](#)
- [system admin on page 223](#)
- [system accprofile on page 220](#)

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

If you have not yet created any administrator access profiles, create at least one. For details, see [system accprofile on page 220](#).

In the administrator account's [access-profile "<access-profile_name>" on page 224](#) 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.)

In the administrator account's [domains "<adom_name>" on page 225](#) 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 on page 46](#)
- [system admin on page 223](#)
- [system accprofile on page 220](#)
- [Defining ADOMs on page 57](#)

config

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



Although not usually explicitly shown in each `config` command's "Syntax" section, for all `config` commands, there are related [get on page 861](#) and [show on page 867](#) 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 alertMail

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 details about the severity levels of log messages associated with an email policy, see [log email-policy on page 68](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config log alertMail
    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 log email-policy on page 68 .	disable
email-policy "<policy_name>"	Enter the name of a previously configured email policy. The maximum length is 63 characters. To display a list of the existing email policies, type: <code>set email-policy ?</code>	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 alertMail
  set status enable
  set email-policy "emailpolicy1"
end
```

Related topics

- [log email-policy on page 68](#)

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 [log disk on page 66](#) 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. For details, see [network sniffer on page 790](#).

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*:

<http://docs.fortinet.com/fortiweb/admin-guides>

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 [log sensitive on page 86](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config log attack-log
  set status {enable | disable}
  set HTTP-parse-error-output {enable | disable}
```

```

set packet-log {account-lockout-detection | anti-virus-detection | cookie-security |
credential-db-detection | csrf-detection | custom-access | custom-protection-
rule | fsa-detection | hidden-fields-failed | HTTP-protocol-constraints |
illegal-file-type | illegal-file-size | cors-protection | json-protection | ip-
intelligence | padding-oracle | parameter-rule-failed | signature-detection |
trojan-detection | user-tracking-detection | xml-protection | machine-learning
| openapi-validation | websocket-security | mobile-api-protection | malicious-
bots | known-good-bots | syntax-based-detection}
set no-ssl-error {enable | disable}
set HTTP2-parse-error-output {enable | disable} on page 63
set adjust-packet {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 log disk on page 66 command.	enable
HTTP-parse-error-output {enable disable}	Enable while debugging only, to log errors of the HTTP protocol parser.	disable
packet-log {account-lockout-detection anti-virus-detection cookie-security credential-db-detection csrf-detection custom-access custom-protection-rule fsa-detection hidden-fields-failed HTTP-protocol-constraints illegal-file-type illegal-file-size cors-protection json-protection ip-intelligence padding-oracle parameter-rule-failed signature-detection trojan-detection user-tracking-detection xml-protection machine-learning openapi-validation websocket-security mobile-api-protection malicious-bots known-good-bots syntax-based-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, enter <code>unset packet-log</code>.	No default
no-ssl-error {enable disable}	Enable to stop FortiWeb from logging SSL errors.	disable

Variable	Description	Default
	This setting is useful when you use high-level security settings, which generate a high volume of these types of errors. This option is also available in <code>config server-policy policy</code> which applies only to the specific server policy. Please note that if there is a discrepancy between the values set individually for server policies and the global value in <code>config log attack-log</code>, the global value takes precedence.	
HTTP2-parse-error-output {enable disable}	Enable while debugging only, to log errors of the HTTP/2 protocol parser.	enable
adjust-packet {enable disable}	When the attack packet log exceeds 4 KB, it will be truncated, removing the excess portion. To ensure that the matched attack pattern is consistently preserved, enable this option so that the truncation retains the relevant portion.	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

- [log sensitive on page 86](#)
- [log custom-sensitive-rule on page 64](#)
- [log event-log on page 71](#)
- [log traffic-log on page 95](#)
- [log on page 784](#)

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 [log sensitive on page 86](#).

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 [log attack-log on page 61](#) and [log sensitive on page 86](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For details, see [Permissions on page 46](#).

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-mas-rule | general-mask-rule}
next
end
```

Variable	Description	Default
"<custom-sensitive-rule_name>"	Enter the name of a new or existing rule. The maximum length is 63 characters. To display the list of existing rules, enter: <code>edit ?</code>	No default.
expression "<sensitive-type_pattern>"	Enter 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: <code>age\[1-13]</code> Expressions must not start with an asterisk (*). The maximum length is 255 characters.	No default.

Variable	Description	Default
type {field-mas-rule general-mask-rule}	Select either <code>general-mask-rule</code> (a regular expression that will match any substring in the packet payload) or <code>field-mask-rule</code> (a regular expression that will match only the value of a specific form input). If you select <code>general-mask-rule</code> , configure expression "<sensitive-type_pattern>" on page 64 . If you select <code>field-mask-rule</code> , configure field-name "<parameter-name_pattern>" on page 65 and field-value "<parameter-value_pattern>" on page 65 .	<code>general-mask-rule</code>
field-name "<parameter-name_pattern>"	Enter 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 <code>general-mask-rule</code> instead. The maximum length is 255 characters.	No default.
field-value "<parameter-value_pattern>"	Enter 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>" on page 65 , enter <code>age</code> , and for field-value "<parameter-value_pattern>" on page 65 , enter <code>[1-13]</code> . 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 <code>username</code> but not any of the parameters that follow it, you could enter the field value: <code>. * ? (? = \ &)</code> This would result in: <code>username****&age=13&origurl=%2Flogin</code>	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

- [log sensitive on page 86](#)
- [log attack-log on page 61](#)
- [log traffic-log on page 95](#)

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. For details, see [log attack-log on page 61](#), [log event-log on page 71](#), and [log traffic-log on page 95](#) for details.

Each log file can have at most 51,200 logs, and each log size is limited to 4k; thus, each log file size is limited to 200M.

You can use SNMP traps to notify you when disk space usage exceeds 80%. For details, see [system snmp community on page 375](#).

You can generate reports based on log messages that you save to the local hard disk. For details, see [log reports on page 77](#).

Syntax

```
config log disk
  set diskfull overwrite
  set severity {alert | critical | debug | emergency | error | information |
    notification | warning}
  set status {enable | disable}
  set log-used-disk <log-used-disk_int>
  set logtype {elog | tlog | alog}
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 log attack-log on page 61 , log event-log on page 71 , and log traffic-log on page 95 . Also configure diskfull overwrite on page 67 and severity {alert critical debug emergency error information notification warning} on page 67 .	enable
diskfull overwrite	Select <code>overwrite</code> to delete the oldest log file in order to free disk space, and then store the new log message. This field is available only if status {enable disable} on page 67 is <code>enable</code> .	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
log-used-disk <log-used-disk_int>	This field is unique for Docker platform. Enter the log disk size. The valid range is 10–500 G.	10 G
logtype {elog tlog alog}	Select the log types to be saved on local hard disk.	elog tlog alog

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.

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

Related topics

- [log attack-log on page 61](#)
- [log event-log on page 71](#)
- [log traffic-log on page 95](#)
- [system snmp community on page 375](#)
- [log reports on page 77](#)
- [formatlogdisk on page 832](#)

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 details, see [Permissions on page 46](#).

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}
    set send-email-based-on-interval-time {enable | disable} on page 70
    set company-logo "<company-logo_str>"
    set company-name "<company-name_str>"
    set
next
end
```

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

Variable	Description	Default
	characters.	
mailto2 "<recipient_email>"	Enter 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>"	Enter 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>"}	Enter the IP address or fully qualified domain name (FQDN) of the SMTP server, such as <code>mail.example.com</code> , 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. The valid range is 1–65,535.	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} on page 69 , enter 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} on page 69 .	No default.
smtp-password "<password_str>"	If you enable smtp-auth {enable disable} on page 69 , enter the password that corresponds with the user name. This field is available only if you enable smtp-auth {enable disable} on page 69 .	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. The valid range is 1–2,147,483,647.	1
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	NONE

Variable	Description	Default
server using SSL/TLS.		
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
send-email-based-on-interval-time {enable disable}	Enable/disable sending emails by interval time.	No default.
company-logo "<company-logo_str>"	Set the company logo in the email policy by entering a Base64 string (base64 encoding) of the image. Only JPG format is supported. Size limit is 36 KB. You are strongly recommended to upload a company logo through the FortiWeb GUI.	No default.
company-name "<company-name_str>"	Set the company name in the email policy. The maximum length is 63 characters.	No default.
logtype {elog tlog alog}	Select the log types to be transferred to the SMTP Server. Please note if a particular log type is not saved on local hard disk, it cannot be transferred to the SMTP server, as the logs must be transferred from local storage to remote servers.	elog tlog alog

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 "fortiWebPassworD2"
    set severity notification
    set interval 10
next
```

```
end
```

Related topics

- [log alertMail on page 60](#)
- [log trigger-policy on page 96](#)
- [system dns on page 279](#)
- [router static on page 101](#)

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.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config log event-log
  set status {enable | disable}
  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, see log disk on page 66 .	enable
cpu-high <percentage_int>	Enter a threshold level as a percentage beyond which CPU usage triggers an event log entry. The valid range is 60–99.	60
mem-high <percentage_int>	Enter a threshold level as a percentage beyond which memory usage triggers an event log entry. The valid range is 60–99.	60

Variable	Description	Default
logdisk-high <percentage_int>	Enter a threshold level as a percentage beyond which log disk usage triggers an event log entry. The valid range is 60–99.	60
trigger-policy "<trigger-policy_name>"	Enter the name of the trigger to apply when the CPU, memory, log disk usage, or number of sessions meets or exceeds the threshold (see log trigger-policy on page 96). The maximum length is 63 characters. To display the list of existing trigger policies, enter: 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 event-log
    set status enable
end
```

Related topics

- [log disk on page 66](#)
- [log attack-log on page 61](#)
- [log traffic-log on page 95](#)
- [log on page 784](#)

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 [log fortianalyzer-policy on page 74](#).

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.

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.



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.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config log forti-analyzer
  set fortianalyzer-policy "<policy_name>"
  set status {enable | disable}
  set severity {alert | critical | debug | emergency | error | information |
    notification | warning}
  set traffic_packet {enable | disable}
  set logtype {elog | tlog | alog}
  set traffic_packet_size <integer> on page 74
end
```

Variable	Description	Default
fortianalyzer-policy "<policy_name>"	Enter the name of an existing FortiAnalyzer policy to use when storing log information remotely. The maximum length is 63 characters. To view a list of the existing FortiAnalyzer policies, enter : <code>set fortianalyzer-policy ?</code>	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
traffic_packet {enable disable}	Enable to append traffic packet log to the traffic logs sent to FortiAnalyzer. The packet information may be helpful for troubleshooting. To use this feature, you must already have enabled packet-log in <code>config log traffic-log</code> . Please note that enabling this might consume system resources, thus decreasing the performance of sending logs to FortiAnalyzer.	disable
logtype {elog tlog alog}	Select the log types to be stored on FortiAnalyzer.	elog tlog alog

Variable	Description	Default
	Please note if a particular log type is not saved on local hard disk, it cannot be saved on an external log server, as the logs must be transferred from local storage to remote servers.	
traffic_packet_size <integer>	The maximum size of the traffic packet payload sent to log servers was 1024 bytes before version 7.4.3. This was extended to 4096 bytes in version 7.4.3. Starting from version 7.6.0, you can set this maximum size yourself with this command. The default value is 1024, and the valid range is 1-4096. Please note that larger packet logs cost more time for FortiWeb to encrypt and compress if the log server requires, increasing the likelihood of the logd queue reaching 80% capacity, which may result in some traffic logs being dropped.	1024,

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

- [log fortianalyzer-policy on page 74](#)

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 details, see [Permissions on page 46](#).

Syntax

```

config log fortianalyzer-policy
edit "<policy_name>"
    config fortianalyzer-server-list
        edit <entry_index>
            set ip-address "<forti-analyzer_ipv4>"
            set is-fazcloud {enable|disable}
        end
    next
end

```

Variable	Description	Default
"<policy_name>"	Enter the name of the new or existing FortiAnalyzer policy. The maximum length is 63 characters. To display a list of the existing policies, enter: edit ?	No default.
<entry_index>	Enter the index number of the individual entry in the table.	No default.
ip-address "<forti-analyzer_ipv4>"	Enter the IP address of the remote FortiAnalyzer appliance.	No default.
is-fazcloud {enable disable}	Enable or disable using FortiAnalyzer Cloud. When FAZ Cloud is enabled in the FortiAnalyzer Policy, FortiWeb resolves the default FortiAnalyzer Cloud domain (fortianalyzer.forticloud.com) and initiates an OFTP connection for secure log transmission. Upon a successful connection, FortiWeb dynamically updates FortiAnalyzer Cloud domain name resolution by performing periodic DNS checks, ensuring consistent connectivity and reliability. Note: Each FortiAnalyzer Policy can have only one FortiAnalyzer server with FAZ Cloud enabled. Additional FortiAnalyzer servers can be included in the policy, but they must have FAZ Cloud disabled.	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 "192.0.2.133"
        end
    next
end

```

```
end
config log forti-analyzer
  set fortianalyzer-policy "fa-policy1"
  set status enable
  set severity error
end
```

Related topics

- [log forti-analyzer on page 72](#)

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 details, see [Permissions on page 46](#).

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>"	Enter the name of a new or existing FTP/TFTP policy. The maximum length is 63 characters. To display the list of existing policies, enter: <code>edit ?</code>	No default.
<code>type {ftp tftp}</code>	Specify whether the server is FTP or TFTP.	<code>ftp</code>
<code>server "<ftp-server_ipv4>"</code>	Enter the IP address of the FTP or TFTP server.	No default.
<code>ftp_auth {enable disable}</code>	Specify whether the server requires a user name and password for authentication, rather than allowing anonymous connections. Available only if <code>type {ftp tftp}</code> on page 76 is <code>ftp</code> .	<code>disable</code>

Variable	Description	Default
ftp_user "<ftp-user_str>"	Enter the user name that FortiWeb uses to authenticate with the server. Available only if ftp_auth {enable disable} on page 76 is enable.	No default.
ftp_passwd "<ftp_pswd>"	Enter the password for the specified username. Available only if ftp_auth {enable disable} on page 76 is enable.	No default.
ftp-dir "<ftp-dir_str>"	Enter the location on the server where FortiWeb stores reports.	No default.

Related topics

- [log reports on page 77](#)

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> on page 85](#) is **x**.
- [scope_top2 <topY_int> on page 85](#) 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 [log attack-log on page 61](#) and [log disk on page 66](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For details, see [Permissions on page 46](#).



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 custom_header "<header_str>"
    set custom_header_logo "<filename_hex_str>"
    set custom_title_logo "<filename_hex_str>"
    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 | thiyar | 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-srccountry attacks-signature-id attacks-type-signature-id
        attacks-fortisandbox attacks-HTTPhost attacks-username attacks-HTTPprefer
        attacks-HTTPversion attack-summary attack-details}
    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 ev-day-login ev-week-login ev-
        user-login}
    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
        net-HTTPprefer net-HTTPversion}
```

```

set report_pci_activity {pci-attacks-date-type pci-attacks-month-type pci-attacks-
    day-type pci-attacks-hour-type}
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>"	Enter 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, enter: edit ?	No default.
custom_company "<org_str>"	Enter 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 details about enabling the summary, see scope_include_summary {yes no} on page 84.	No default.
custom_footer_options {custom report-title}	Select either: - report-title—Use "<report_name>" on page 79 as the footer text. - custom—Provide different footer text.	report-title
custom_footer "<footer_str>"	Enter 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 {custom report-title} on page 79 is custom.	No default.
custom_header "<header_str>"	Enter 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_str>"	Enter 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.

Variable	Description	Default
custom_title_logo "<filename_hex_str>"	Enter 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} on page 80 .	disable
email_attachment_name "<filename_str>"	Enter 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} on page 80 .	No default.
email_body "<message_str>"	Enter 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} on page 80 .	No default.
email_subject "<subject_str>"	Enter 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} on page 80 .	No default.
filter_string "<log-filter_str>"	Enter 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 85 .	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. Enter <code>disable</code> 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 <code>output_email</code> , enter the name of the email policy that contains settings for sending the report by email. The maximum length is 63 characters.	No default.

Variable	Description	Default
	For details about email policies, see log email-policy on page 68 .	
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. For details, see log ftp-policy on page 76 .	No 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 <code>hh:mm</code> and the date format is <code>yyyy/mm/dd</code>, where: • <code>hh</code> is the hour according to a 24-hour clock • <code>mm</code> is the minute • <code>yyyy</code> is the year • <code>mm</code> is the month • <code>dd</code> is the day This setting appears only when you select a 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 thiyear today yesterday} on page 82 of other.	No default.
period_last_n <n_int>	Enter the number that defines n if the 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 thiyear today yesterday} on page 82 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 <code>hh:mm</code> and the date format is <code>yyyy/mm/dd</code>, where: • <code>hh</code> is the hour according to a 24-hour clock • <code>mm</code> is the minute • <code>yyyy</code> is the year • <code>mm</code> is the month • <code>dd</code> is the day	No default.

Variable	Description	Default
	This setting appears only when you select a 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 thiyear today yesterday } on page 82 of other .	
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 thiyear 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> on page 81. If you select other, you must also define the start and end of the report's time range by entering period_start "<time_str>" "<date_str>" on page 81 and period_end "<time_str>" "<date_str>" on page 81. The span of time will be included in the summary, if enabled. For information on enabling the summary, see scope_include_summary {yes no} on page 84.	last-7-days
report_desc "<comment_str>"	Enter 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} on page 84.	No default.
report_title "<title_str>"	Enter 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} on page 84.	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-srccountry attacks-signature-id attacks-type-signature-id attacks-fortisandbox attacks-HTTPhost attacks-username attacks-HTTPprefer attacks-HTTPversion attack-summary attack-details}	Enter 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 <code>attacks-policy</code> . To include “Top Attacked HTTP Methods by Type,” enter a list of charts that includes <code>attacks-method-type</code> .	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 ev-day-login ev-week-login ev-user-logint}	Enter 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 <code>ev-stat</code> .	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 net-HTTPprefer net-HTTPversion}	Enter 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 <code>net-day-src</code>.	No default.
report_pci_activity {pci-attacks-date-type pci-attacks-month-type pci-attacks-day-type pci-attacks-hour-type}	Enter 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 <code>schedule_type</code> is <code>daily</code>, <code>dates</code> or <code>days</code>, specify the <code>schedule_time</code>, <code>schedule_days</code>, or <code>schedule_dates</code> when the report will be generated. If <code>schedule_type</code> is <code>none</code>, the report will be generated only when you manually initiate it.	none
schedule_days {sun mon tue wed thu fri sat}	If <code>schedule_type {daily dates days none}</code> on page 84 is <code>days</code> , select the day of the week when the report should be generated.	No default.
schedule_dates "<dates_str>"	If <code>schedule_type {daily dates days none}</code> on page 84 is <code>dates</code> , 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 <code>schedule_type {daily dates days none}</code> on page 84 is not <code>none</code>, select the time of day when the report should be run. The time format is <code>hh:mm</code>, where: <code>hh</code> is the hour according to a 24-hour clock <code>mm</code> is the minute	00:00
scope_include_summary {yes no}	Enter <code>yes</code> to include a summary section at the beginning of the report. The summary includes: <code><report_name></code> on page 79 <code>custom_company <org_str></code> on page 79 <code>report_desc <comment_str></code> on page 82	yes

Variable	Description	Default
	- 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 <code>period_type</code> {<code>last-14-days</code> <code>last-2-weeks</code> <code>last-30-days</code> <code>last-7-days</code> <code>lastmonth</code> <code>last-n-days</code> <code>last-n-hours</code> <code>last-n-weeks</code> <code>last-quarter</code> <code>last-week</code> <code>other</code> <code>this-month</code> <code>this-quarter</code> <code>this-week</code> <code>thiyear</code> <code>today</code> <code>yesterday</code>} on page 82	
<code>scope_include_table_of_content</code> {yes no}	Enter <code>yes</code> 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
<code>scope_top1</code> <topX_int>	Enter <code>x</code> 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 <code>x</code> 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
<code>scope_top2</code> <topY_int>	Enter <code>y</code> 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 <code>x</code> entries. Some report types have two levels of ranking: the top <code>y</code> sub-entries for each top <code>x</code> 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 192.0.2.20. 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 "eport_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==\'192.0.2.20\')
    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

- [log attack-log on page 61](#)
- [log disk on page 66](#)
- [log email-policy on page 68](#)
- [log ftp-policy on page 76](#)

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 [log custom-sensitive-rule on page 64](#).

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 [log attack-log on page 61](#) and [log traffic-log on page 95](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For details, see [Permissions on page 46](#).

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. For details, see log custom-sensitive-rule on page 64 .	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

- [log custom-sensitive-rule on page 64](#)
- [log attack-log on page 61](#)
- [log traffic-log on page 95](#)

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 [log siem-policy on page 89](#).

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.

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.



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.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config log siem-message-policy
  set siem-policy "<policy_name>"
  set severity {alert | critical | debug | emergency | error | information |
    notification | warning}
  set status {enable | disable}
  set logtype {elog | tlog | alog}
end
```

Variable	Description	Default
siem-policy "<policy_name>"	Enter the name of an existing SIEM policy to use when storing log information remotely. The maximum length is 63 characters. To view a list of the existing SIEM policies, enter: 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 {alert critical debug emergency error information notification warning} on page 88.	disable
logtype {elog tlog alog}	Select the log types to be stored on SIEM servers. Please note if a particular log type is not saved on local hard disk, it cannot be saved on an external log server, as the logs must be transferred from local storage to remote servers.	elog tlog alog

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

- [log siem-policy on page 89](#)

log siem-policy

Use this command to configure a connection to one or more ArcSight SIEM (security information and event management) servers, IBM QRadar servers or Azure Security Center (if your FortiWeb-VM is deployed on Microsoft Azure). The policy is used by the `log syslogd` configuration to define the specific ArcSight server, QRadar server or Azure Event Hub on which log messages are stored. For details, see [log syslogd on page 91](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For details, see [Permissions on page 46](#).

Syntax

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

Variable	Description	Default
"<policy_name>"	Enter the name of a new or existing SIEM policy. The maximum length is 63 characters. To display the list of existing policies, enter: <code>edit ?</code>	No default.
<entry_index>	Enter the index number of the individual entry in the table.	No default.
type <arcsight-cef qradar-leef azure-cef>	Enter to store log messages to a SIEM (Security Information and Event Management) server. According to the specified SIEM policy, FortiWeb will carry out one of the following actions: <code>arcsight-cef</code>—Store log messages remotely to an ArcSight server <code>qradar-leef</code>—Store log messages remotely to a QRadar server <code>azure-cef</code>—Send log messages to Azure Event Hub (only available for FortiWeb-VM installed on Azure) FortiWeb sends log entries in CEF (Common Event Format) format. There is a 256 byte limit for URLs.	<code>arcsight-cef</code>

Variable	Description	Default
	If this option is enabled, but no trigger action is selected for a specific type of violation, FortiWeb records every occurrence of that violation to the resource specified by SIEM Policy. The Azure CEF policy type requires you to complete Azure event hub settings using the system eventhub on page 282 CLI command. Note: Before you enable this option, verify that log frequency is not too great. If logs are very frequent, enabling this option can decrease performance and cause the FortiWeb appliance to send many log messages to the resource. Note: You cannot view logs stored remotely from the FortiWeb web UI.	
port <port_int>	Enter the port where the ArcSight or QRadar server listens for log output.	514
server "<siem_ipv4>"	Enter the IP address of the ArcSight or QRadar server.	No default.

Example

This example creates `SIEM_Policy1`. FortiWeb contacts the ArcSight server using its IP address, `192.0.2.10`. 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 "192.0.2.10"
      end
    next
  end
```

Related topics

- [log siem-policy on page 89](#)
- [system dns on page 279](#)
- [router static on page 101](#)

log syslogd

Use this command to configure the FortiWeb appliance to send log messages to a Syslog server defined by [log syslog-policy on page 93](#).



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 details, see [Permissions on page 46](#).

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>"
  set logtype {elog | tlog | alog}
  config custom-field
    edit 1
      set name <name1>
      set value <value1>
    next
    edit 2
      set name <name2>
      set value <value2>
    next
  end
```

Variable	Description	Default
<code>status {enable disable}</code>	Enable to send log messages to the Syslog server defined by log syslog-policy on page 93. Also configure: <code>facility {alert audit auth authpriv clock cron daemon ftp kernel local0 local1 local2 local3 local4 local5 local6 local7 mail ntp user}</code> on page 92 <code>policy "<syslogd-policy_name>"</code> on page 92 <code>severity {alert critical debug emergency error information notification warning}</code> on page 92	<code>disable</code>

Variable	Description	Default
facility {alert audit auth authpriv clock cron daemon ftp kernel local0 local1 local2 local3 local4 local5 local6 local7 mail ntp user}	Enter 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, enter the name of a Syslog policy which describes the Syslog server to which the log message will be sent. The maximum length is 63 characters. For details about Syslog policies, see log syslog-policy on page 93 .	No default.
name	Set this option to add customized identifiers in syslog records, for example, add the hostname in syslogs so that you can easily track the logs for specific hosts. Enter a name for the identifier.	No default.
value	Enter the value of the identifier. It can be a fixed value or a variable. In the HA deployment, the configuration is synchronized among the HA group members but meanwhile each member should have its own hostname recorded in the syslog. In this case, you can use the variable such as <code>set value \$hostname</code> to refer to the hostname defined in <code>config system global</code> . Only the hostname variable is supported.	No default.
logtype {elog tlog alog}	Select the log types to be stored on Syslog servers. Please note if a particular log type is not saved on local hard disk, it cannot be saved on an external log server, as the logs must be transferred from local storage to remote servers.	elog tlog alog

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 details, see [log syslogd on page 91](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For details, see [Permissions on page 46](#).

Syntax

```

config log syslog-policy
  edit "<policy_name>"
    config syslog-server-list
      edit <entry_index>
        set port <port_int>
        set proto {tcp | tls | udp}
        set packet {enable | disable}
        set format {cef | csv | default | json}
        set server "<syslog_ipv4/ipv6>"
        set cus-fields <cus-fields_name>
      end
    end
  next
end

```

Variable	Description	Default
"<policy_name>"	Enter the name of a new or existing Syslog policy. The maximum length is 63 characters. The name of the report profile will be included in the report header. To display the list of existing policies, enter: 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.
port <port_int>	Enter the port number on which the Syslog server listens. The valid range is 1–65,535.	514
proto {tcp tls udp}	Select the protocol to transfer the logs between FortiWeb and the syslog server.	udp

Variable	Description	Default
format {cef csv default json}	Select the format of the system log. Note that CEF is for Syslog server, not for SIEM. If your receiver is a SIEM server such as Azure Sentinel, please refer to Configuring SIEM policies in FortiWeb Administration Guide.	default
server "<syslog_ipv4/ipv6>"	Enter the IPv4 or IPv6 address of the Syslog server.	No default.
packet {enable disable}	Enable packet to include packet payloads in the JSON format logs. Packet payloads supplement the log message by providing the actual request headers and body. This option is available only when the Format is JSON and the Protocol is TCP or TLS . Please note that using JSON format or enabling packet payloads may have negative impact on system performance.	disable
cus-fields <cus-fields_name>	Select one of the identifiers you have defined in <code>config log syslogd</code> under <code>config custom-field</code> . It will be attached to the syslog records.	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

- [log syslogd on page 91](#)
- [system dns on page 279](#)
- [router static on page 101](#)

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 [log disk on page 66](#) 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*:

<http://docs.fortinet.com/fortiweb/admin-guides>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config log traffic-log
  set packet-log {enable | disable}
  set status {enable | disable}
  set message-event {enable | disable} on page 95
  set low-priority {enable | disable} on page 95
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 log disk on page 66 .	disable
packet-log {enable disable}	Enable to keep packet payloads stored with their associated traffic log message. For details about obscuring sensitive information in packet payloads, see log sensitive on page 86 .	disable
message-event {enable disable}		disable
low-priority {enable disable}	Enable to set the attack log with a higher priority than the traffic log. This way, if the <code>logd</code> queue is more than 80% full, FortiWeb will stop generating traffic logs to prioritize the processing of attack logs until the <code>logd</code> queue drops below 80%. The following event log will be displayed to notify you of the <code>logd</code> status change:	disable

Variable	Description	Default
	- When the logd queue exceeds 80% and FortiWeb stops generating traffic logs, you will see the following event log: <pre>Log ID=11000516, Log Level=Debug, MSG=Alog to server queue will be full, pause tlog for a while, Action=pause</pre> - When the server queue drops below 80% and FortiWeb resumes generating traffic logs, you will see the following event log: <pre>Log ID=11000514, Log Level=Debug, MSG=Alog to server queue is ok, resume tlog for a while, Action=resume</pre>	

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

- [log attack-log on page 61](#)
- [log event-log on page 71](#)
- [log disk on page 66](#)
- [log sensitive on page 86](#)
- [log on page 784](#)

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 details, see [log email-policy on page 68](#), [log syslog-policy on page 93](#), and [log fortianalyzer-policy on page 74](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `loggrp` area. For details, see [Permissions on page 46](#).

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>"	Enter the name of a new or existing trigger policy. The maximum length is 63 characters.	No default.
email-policy "<email-policy_name>"	Enter the name of the email policy to be used with the trigger policy. The maximum length is 63 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 details, see log email-policy on page 68 .	No default.
syslog-policy "<syslog-policy_name>"	Enter the name of the Syslog policy to be used with the trigger policy. The maximum length is 63 characters. If the conditions associated with the trigger policy occur, the Syslog policy determines which Syslog server the messages are sent to. For details, see log syslog-policy on page 93 .	No default.
analyzer-policy "<fortianalyzer-policy_name>"	Enter the name of an existing FortiAnalyzer policy to be used with the trigger policy. The maximum length is 63 characters. For details, see log fortianalyzer-policy on page 74 .	No default.
siem-policy "<siem-policy_name>"	Enter the name of an existing SIEM policy to be used with the trigger policy. The maximum length is 63 characters. For details, see log siem-policy on page 89 .	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

- [log email-policy on page 68](#)
- [log syslog-policy on page 93](#)
- [log fortianalyzer-policy on page 74](#)
- [log siem-policy on page 89](#)
- [waf HTTP-protocol-parameter-restriction on page 543](#)
- [waf signature on page 612](#)

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.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `netgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config router policy
  edit <policy_index>
    set iif "<incoming_interface_name>"
    set src "<source_ip>"
    set dst "<destination_ip>"
    set fwmark <fwmark_int> on page 99
    set set action {forward-traffic | stop-policy-routing} on page 99
    set oif "<outgoing_interface_name>"
    set gateway "<router_ip>"
    set priority <priority_int>
  next
end
```

Variable	Description	Default
<policy_index>	Enter the index number of the policy route. The valid range is 0–65,535.	No default.
"<incoming_interface_name>"	Enter the name of the interface, such as <code>port1</code> , 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
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
fwmark <fwmark_int>	Enter the Fwmark value specified in Firewall Fwmark Policy . If you don't need to match traffic against the Fwmark value, enter value 0. The valid range is 0-255.	
set action {forward-traffic stop-policy-routing}	forward-traffic: FortiWeb filters traffic against the specified conditions and forwards the traffic to this policy route. stop-policy-routing: FortiWeb filters traffic against the specified conditions and forwards the traffic according to the matched static route.	
"<outgoing_interface_name>"	Enter the name of the interface, such as <code>port2</code> , 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. A gateway address is not required for the particular routing policies used as static routes in an one-arm topology. Leave this blank for a one-arm network topology.	0.0.0.0
priority <priority_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

- [router static on page 101](#)
- [router setting on page 100](#)

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 details, see [Permissions on page 46](#).

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
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

- [router static on page 101](#)
- [router policy on page 98](#)
- [router all on page 1](#)

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 details, see [Permissions on page 46](#).

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>	Enter 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 0–65,535.	No default.
device "<interface_name>"	Enter the name of the network interface device, such as <code>port1</code> , through which traffic subject to this route will be outbound. The maximum length is 63 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 <code>0.0.0.0 0.0.0.0</code> or <code>::/0</code> .	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 192.0.2.1, through the network interface named `port1`.

```
config router static
  edit 0
    set dst "0.0.0.0 0.0.0.0"
    set gateway "192.0.2.1"
    set device port1
  next
end
```

Related topics

- [router setting on page 100](#)
- [router policy on page 98](#)
- [system interface on page 344](#)
- [log syslog-policy on page 93](#)
- [server-policy policy on page 150](#)
- [system admin on page 223](#)
- [system dns on page 279](#)
- [system snmp community on page 375](#)
- [wad website on page 416](#)
- [traceroute on page 857](#)
- [network arp on page 785](#)
- [network ip on page 786](#)
- [network route on page 787](#)
- ["router all" on page 1](#)

server-policy acceleration

Acceleration provides a technology solution to speed up web application response and optimize web pages and resources in real time.

An Acceleration policy specifies the option(s) for optimizing the delivery of web applications. To take full advantage of the benefits that Acceleration offers, you must first create your own Acceleration policy, and then select the policy in **Policy > Server Policy**.

You can also specify certain URLs to be skipped for web application delivery optimization, and add the exception items to the acceleration policy.

FortiWeb offers options for optimizing the delivery of the following web content:

- HTML
- JavaScript
- CSS



If Acceleration is not enabled, go to [system feature-visibility](#) to enable it first.

Syntax

```
config server-policy acceleration exception
edit "<exception_name>"
config list
edit "<exception-item_id>"
set host-status {enable | disable}
set host <host_int>
set url-type {plain | regular}
set url-pattern <url-pattern_str>
next
end
next
end

config server-policy acceleration policy
edit "<policy_name>"
set exception <exception_str>
set html-minify {enable | disable}
set html-combine-heads {enable | disable}
set html-css2head {enable | disable}
set js-minify {enable | disable}
set css-minify {enable | disable}
next
end
```

Variable	Description	Default
"<exception_name>"	Enter a name for the exception rule.	No default.
"<exception-item_id>"	Enter an ID for the acceleration exception item.	No default
host-status {enable disable}	Enable to require that the Host: field of the HTTP request match a protected host names entry in order to match the Acceleration exceptions rule. Also configure host <host_int> .	disable
host <host_int>	Select which protected host names entry (either a web host name or IP address) that the Host: field of the HTTP request must be in to match the Acceleration exceptions rule.	No default.
url-type {plain regular}	Select whether url-pattern <url-pattern_str> will contain a literal URL (plain), or a regular expression designed to match multiple URLs (regular).	plain

Variable	Description	Default
url-pattern <url-pattern_str>	Depending on your selection in url-type {plain regular}, enter either: - The literal URL, such as <code>/index.php</code>, that the HTTP request must contain in order to match the acceleration rule. The URL must begin with a slash (/). - A regular expression, such as <code>^/*\.php</code>, matching all and only the URLs to which the acceleration 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 <code>/index.cfm</code>. Note: Regular expressions beginning with an exclamation point (!) are not supported. For information on language and regular expression matching, see the <i>FortiWeb Administration Guide</i>: https://docs.fortinet.com/document/fortiweb	No default.
"<policy_name>"	Enter a name for the acceleration policy.	No default.
exception <exception_str>	Select the acceleration exception rule created.	No default.
html-minify {enable disable}	Enable to minify js in the script and delete the extra white space and comments to reduce bandwidth utilization.	disable
html-combine-heads {enable disable}	Enable to combine multiple heads in HTML page to one.	disable
html-css2head {enable disable}	Enable to move CSS elements above script tags. Note: This ensures that the CSS styles are parsed in the head of the HTML page before any body elements are introduced. In so doing, it can effectively reduce the number of times web browsers have to re-flow HTML documents.	disable
js-minify {enable disable}	Enable to minify js in the script and delete the extra white space and comments to reduce bandwidth utilization.	disable
css-minify {enable disable}	Enable to minify js in the script and delete the extra white space and comments to reduce bandwidth utilization.	disable

Related topics

- [server-policy policy on page 150](#)

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
- 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 details, see [Permissions on page 46](#).

Syntax

```

config server-policy allow-hosts
  edit "<protected-hosts_name>"
    set default-action {allow | deny | deny_no_log}
  config host-list
    edit <protected-host_index>
      set action {allow | deny | deny_no_log}
      set host {"<host_ipv4>" | "<host_fqdn>" | "<host_ipv6>"}
      set ignore-port {enable|disable}
      set include-subdomains {enable|disable}
      set override-headers {enable|disable}
    next
  end
next
end

```

Variable	Description	Default
"<protected-hosts_name>"	Enter the name of a new or existing group of protected hosts. The maximum length is 63 characters. To display the list of existing groups, enter: edit ?	No default.
default-action {allow deny deny_no_log}	Select whether to accept or deny HTTP requests whose <code>Host</code> : field does not match any of the host definitions that you will add to this protected hosts group.	allow
<protected-host_index>	Enter the index number of a protected host within its group. Each host-list can contain up to 64 IP addresses and/or fully qualified domain names (FQDNs). The valid range is 1–9,223,372,036,854,775,807.	No default.
action {allow deny deny_no_log}	Select whether to accept or deny HTTP requests whose <code>Host</code> : field matches the host definition in <code>host {"<host_ipv4>" "<host_fqdn>" "<host_ipv6>"}</code> on page 107.	allow
host {"<host_ipv4>" "<host_fqdn>" "<host_ipv6>"}	Enter the IP address or FQDN of a virtual or real web host, as it appears in the <code>Host</code> : field of HTTP headers, such as <code>www.example.com</code> . 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 192.0.2.1/24 forwards traffic to the physical server 192.0.2.155, for protected hosts, you would enter: 192.0.2.1, the address of the virtual server - www.example.com, the domain name that resolves to	No default.

Variable	Description	Default
the virtual server		
ignore-port {enable disable}	Enable <code>ignore-port</code> so that FortiWeb will ignore the port numbers after the host name, and consider them as a match. For example, if you configure the host name as <code>example.com</code>, and enable Ignore Port, then the host name with any port numbers (e.g. <code>example.com:443</code>, <code>example.com:80</code>) will be considered a match. However, please be aware that if the port number falls outside the range of 0 to 65535 or contains a string instead of a numerical value, the system will identify it as abnormal. In such cases, the system will consider it abnormal and take the Alert and Deny action. If you don't enable Ignore Port but you want to match specific port numbers such as <code>example.com:443</code> and <code>example.com:80</code>, then you need to add two host name items respectively for <code>example.com:443</code> and <code>example.com:80</code>.	disable
include-subdomains {enable disable}	Enable <code>include-subdomains</code> so that the sub domains of the host (for example <code>abc.myhost.com</code>) will be protected.	disable
override-headers {enable disable}	Enable <code>override-headers</code> so that host headers can still be identified even if they are overridden with the following headers: • X-Forwarded-Host • X-Host • X-Forwarded-Server • X-HTTP-Host-Override • Forwarded	disable

Example

This example configures a protected hosts group named `example_com_hosts` that contains a website'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

- [server-policy policy on page 150](#)
- [waf allow-method-exceptions on page 423](#)
- [server-policy custom-application application-policy on page 1](#)
- [waf input-rule on page 551](#)
- [waf signature on page 612](#)
- [waf hidden-fields-rule on page 523](#)

server-policy allow-list

Use this command to configure objects that will be exempt from scans, and it can be applied at the server policy level. For the traffic that arrives at this server policy, it will be screened only according to the server policy based allow list instead of the global one.

This command applies only at server-policy level. If you want to define a allow list that applies globally to all server policies, use `config server-policy pattern custom-global-white-list-group` instead of this one.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config server-policy allow-list
edit <entry_index>
    config allow-list-items
    edit <entry_index>
        set type {Cookie | Parameter | URL | Header_Field | Lets_Encrypt}
        set status {enable | disable}
        set domain "<cookie_str>"
        set name "<name_str>"
        set path "<url_str>"
        set wildcard {enable | disable}
        set request-type {plain | regular}
        set domain-type {plain | regular}
        set name-type {plain | regular}
        set request-file-status {enable | disable}
        set domain-status {enable | disable}
        set request-file "<url_str>"
        set header-type {plain | regular}
        set value-status {enable | disable}
        set value-type {plain | regular}
        set value <header_value_string>
    next
end
```

Variable	Description	Default
<entry_index>	Enter the index number of the individual rule in the table. The valid range is 1–9,223,372,036,854,775,807.	No default.
status {enable disable}	Enable to exempt this object from all scans.	enable
type {Cookie Parameter URL Header_Field Lets_Encrypt}	Indicate the type of the object. Depending on your selection, the remaining settings vary. Note: If <code>Type</code> is <code>lets_encrypt</code> , you don't need to specify the Let's Encrypt request-type and request URL as they are fixed. If you are using Let's Encrypt to generate a certificate, it is recommended to enable this allow list, otherwise it may result in certificate retrieval failures if requests from Let's Encrypt are blocked. For more information about Let's Encrypt certificate, see Let's Encrypt certificates .	URL
path "<url_str>"	Enter the path as it appears in the cookie, such as / or /blog/folder. This setting is available if <code>type {Cookie Parameter URL Header_Field Lets_Encrypt}</code> on page 110 is set to <code>Cookie</code> .	No default.
wildcard {enable disable}	The wildcard option is available if the type is Cookie . Enable wildcard matching for the cookie name. When enabled, the asterisk (*) character can match zero or more characters. Up to two asterisks are allowed per name , and matching is case-sensitive . Wildcards can appear at the beginning , middle , or end of the name. Examples: <code>_ga*</code> matches <code>_ga</code>, <code>_ga123</code> <code>*_gid</code> matches <code>_gid</code>, <code>abc_gid</code> <code>aaa*bbb</code> matches <code>aaabbb</code>, <code>aaa123bbb</code> <code>*aaa*bbb</code> matches <code>xyzaaa123bbb</code>	disable
request-type {plain regular}	Indicate whether the <code>request-file "<url_str>"</code> on page 111 field contains a literal URL (<code>plain</code>), or a regular expression designed to match multiple URLs (<code>regular</code>). This setting is available if <code>type {Cookie Parameter URL Header_Field Lets_Encrypt}</code> on page 110 is set to <code>URL</code> .	plain
domain-type {plain regular}	Indicate whether the <code>domain "<cookie_str>"</code> field will contain a literal domain/IP address (Simple String), or a regular expression designed to match multiple domains/IP addresses (Regular Expression).	plain
domain "<cookie_str>"	Enter the partial or complete domain name or IP address as it appears in the cookie, such as: <code>www.example.com</code>	No default.

Variable	Description	Default
	.google.com 192.0.2.50 If clients sometimes access the host via IP address instead of DNS, create allow list objects for both. This setting is available if type {Cookie Parameter URL Header_Field Lets_Encrypt} on page 110 is set to Cookie. Caution: Do not allowlist untrusted subdomains that use vulnerable cookies. It could compromise the security of that domain and its network.	
name-type {plain regular}	Indicate whether the name "<name_str>" field will contain a literal parameter name (Simple String), or a regular expression designed to match all parameter names (Regular Expression).	plain
name "<name_str>"	Depending on your selection in type {Cookie Parameter URL Header_Field Lets_Encrypt} on page 110, either: - Enter the name of the cookie as it appears in the HTTP request, such as NID. - Enter the name of the parameter as it appears in the HTTP URL or body, such as rememberme. This setting is available if type {Cookie Parameter URL Header_Field Lets_Encrypt} on page 110 is set to Cookie, Parameter, or Header_Field.	No default.
request-file-status {enable disable}	Enable to apply this rule only to HTTP requests for specific URLs. Configure request-file "<url_str>" if it is enabled.	disable
domain-status {enable disable}	Enable to apply this rule only to HTTP requests for specific domains. If enabled, also configure domain "<cookie_str>".	disable
request-file "<url_str>"	Depending on your selection in the request-type {plain regular} on page 110 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.	

Variable	Description	Default
	This setting is available if type {Cookie Parameter URL Header_Field Lets_Encrypt} on page 110 is set to <code>URL</code> .	
<code>header-type {plain regular}</code>	Indicate whether the type field will contain a literal name (<code>plain</code>), or a regular expression designed to match multiple names (<code>regular</code>).	<code>plain</code>
<code>value-status {enable disable}</code>	Enable to also check the value of the HTTP header. Only the HTTP headers which match both the name and the value will be allowlisted.	<code>disable</code>
<code>value-type {plain regular}</code>	Indicate whether the header name will contain a literal name (<code>plain</code>), or a regular expression designed to match multiple names (<code>regular</code>).	<code>plain</code>
<code>value <header_value_string></code>	The value of the HTTP header. Depending on your selection in the <code>value-type</code> field, enter either a literal value or a regular expression.	No default.

Example

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

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

Related topics

- [waf web-protection-profile inline-protection on page 696](#)

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 [timeout <seconds_int> on page 115](#) 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 [server-policy server-pool on page 182](#).

To apply server health checks, select them in a server pool configuration. For details, see [server-policy server-pool on page 182](#).

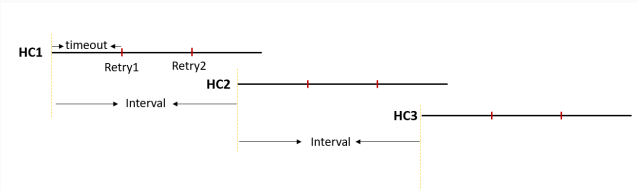
To use this command, your administrator account's access control profile requires either `w` or `rw` permission to the `traroutegrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config server-policy health
edit "<health-check_name>"
  set trigger-policy "<trigger-policy_name>"
  set relationship {and |or}
  set group-id <int>
  set role {master | slave | standalone}
  configure health-list
    edit <entry_index>
      set type {icmp | tcp | HTTP | tcp-ssl | tcp-half-open}
      set timeout <seconds_int>
      set timeout <seconds_int>
      set timeout <seconds_int>
      set url-path "<request_str>"
      set method {get | head | post}
      set match-type {response-code | match-content | all}
      set response-code {response-code_int}
      set match-content "<match-content_str>"
    next
  next
end
```

Variable	Description	Default
"<health-check_name>"	Enter the name of the server health check. The maximum length is 63 characters. To display the list of existing server health checks, enter: edit ?	No default.
trigger-policy "<trigger-policy_name>"	Enter the name of the trigger to apply when the health check detects a failed server (see log trigger-policy on page 96). The maximum length is 63 characters. To display the list of existing trigger policies, enter: set trigger ?	No default.
relationship {and or}	and—FortiWeb considers the server to be responsive when it passes all the tests in the list.	and

Variable	Description	Default
	<code>or</code>—FortiWeb considers the server to be responsive when it passes at least one of the tests in the list.	
<code>group-id <int></code>	<code>group-id</code> is used together with <code>role {master slave}</code>. FortiWeb performs health check on the server pool which has referenced a "master" health check, then synchronize the result to all the server pools which have referenced the "slave" health check of the same <code>group-id</code>. This can avoid unnecessary health checks in certain cases such as when different server pools sharing the same IP address. This option is not available if the role is standalone.	No default.
<code>role {master slave standalone}</code>	If you want the health check result to be shared across multiple server pools, then specify whether this health check is a master or a slave. This is used together with the above command <code>group-id <int></code>. If the health check result is not to be shared, then choose <code>standalone</code>.	standalone
<code><entry_index></code>	Enter the index number of the individual rule in the table. The valid range is 1–16.	No default.
<code>type {icmp tcp HTTP tcp-ssl tcp-half-open}</code>	Select either: <code>icmp</code>—Send ICMP type 8 (<code>ECHO_REQUEST</code>) and listen for either ICMP type 0 (<code>ECHO_RESPONSE</code>) indicating responsiveness, or timeout indicating that the host is not responsive. <code>tcp</code>—Send TCP <code>SYN</code> and listen for either TCP <code>SYN ACK</code> indicating responsiveness, or timeout indicating that the host is not responsive. <code>HTTP</code>—Send an HTTP request and listen for the code specified by <code>response-code</code>, the page content specified by <code>match-content</code>, 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. <code>tcp-ssl</code>—Send a TCP SSL 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 <code>HTTP</code> or <code>HTTPS</code>. Apply to server pool members only if the SSL setting for the member is enabled.	ping

Variable	Description	Default
	tcp-half-open—Send TCP <code>SYN</code> and listen for either TCP <code>SYN ACK</code> indicating responsiveness, or timeout indicating that the host is not responsive. If the response is <code>SYN ACK</code>, send TCP <code>RST</code> to terminate the connection. This type of health check requires fewer resources from the pool member than <code>tcp</code>.	
timeout <seconds_int> retry-times <retries_int> interval <seconds_int>	timeout <seconds_int>: The maximum duration (in seconds) FortiWeb will wait for a response from a back-end server during a health check. If the server does not respond within this time frame, the health check is considered failed. The valid range is 1–30 . retry-times <retries_int>: The number of consecutive retries FortiWeb will perform—each with the configured timeout—if no response is received from the server. The server is marked down only after all retries fail. The valid range is 1 - 10. interval <seconds_int>: The frequency (in seconds) at which FortiWeb performs health checks on the back-end server. The valid range is from 1 - 300. The diagram illustrates how FortiWeb's health check mechanism uses <code>timeout</code>, <code>retry-times</code>, and <code>interval</code>. In this example: - Each health check (HC) begins and, if no response is received, performs up to two retries (<code>retry-times = 2</code>), with each retry waiting up to the configured <code>timeout</code> duration. - Health checks can run concurrently—starting a new health check does not cancel or override an existing one that is still active. As shown in the diagram, HC2 begins while the second retry of HC1 is still in progress. 	timeout : 3 retry-times: 3 interval:10
Best Practice Strategy		

Variable	Description	Default
	We recommend setting the interval so that the next health check begins when the last retry of the current health check is underway, as shown in the diagram above. - Example If: - timeout = 3 seconds - retry-times = 2 Then, the recommended interval is between 6 and 9 seconds. This ensures: - Minimal overlap between health check cycles. - Efficient use of CPU and memory by reducing unnecessary concurrency. - Faster failover or recovery detection without redundant checks. Special Notice for Public Cloud Deployments If FortiWeb and your back-end resources are hosted on public cloud platforms, be aware that network latency is typically higher compared to on-premises environments. As a result, the default timeout value of 3 seconds may be too short for receiving a response from the server. We recommend configuring a longer <code>timeout</code> and <code>interval</code> based on the observed network conditions in your environment to ensure reliable health check results.	
url-path "<request_str>"	Enter the URL, such as <code>/index.html</code>, 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 <code>match-content</code>, FortiWeb considers it to be responsive. Available when <code>type {icmp tcp HTTP tcp-ssl tcp-half-open}</code> on page 114 is HTTP or HTTPS.	No default.
method {get head post}	Specify whether the health check uses the HEAD, GET, or POST method. Available when <code>type {icmp tcp HTTP tcp-ssl tcp-half-open}</code> on page 114 is HTTP or HTTPS.	get
match-type {response-code match-content all}	<code>response-code</code>—If the web server successfully returns the URL specified by <code>url-path</code> and the code specified by <code>response-code</code>, FortiWeb considers the server to be responsive. <code>match-content</code>—If the web server successfully returns the URL specified by <code>url-path</code> and its content matches the <code>match-content</code> value,	match-content

Variable	Description	Default
	FortiWeb considers the server to be responsive. <code>all</code>—If the web server successfully returns the URL specified by <code>url-path</code> and its content matches the <code>match-content</code> value, and the code specified by <code>response-code</code>, FortiWeb considers the server to be responsive. Available when type {icmp tcp HTTP tcp-ssl tcp-half-open} on page 114 is HTTP or HTTPS.	
<code>response-code {response-code_int}</code>	Enter the response code that you require the server to return to confirm that it is available, if <code>match-type</code> is <code>response-code</code> or <code>all</code>. Available when type {icmp tcp HTTP tcp-ssl tcp-half-open} on page 114 is HTTP or HTTPS.	200
<code>match-content "<match-content_str>"</code>	Enter a regular expression that matches the content that must be present in the HTTP reply to indicate proper server connectivity, if <code>match-type</code> is <code>match-content</code> or <code>all</code>. Available when type {icmp tcp HTTP tcp-ssl tcp-half-open} on page 114 is HTTP or HTTPS.	No default.

Example

This example configures a server health check that periodically requests the main page of the website, `/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

- [server-policy server-pool on page 182](#)
- [server-policy policy on page 150](#)
- [log trigger-policy on page 96](#)

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
- Geo IP

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:

- 192.0.2.1—Hosts the website and blog
- 192.0.2.2 and 192.0.2.3—Host movie clips and multimedia
- 192.0.2.4 and 192.0.2.5—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 details about rewriting, see [waf url-rewrite url-rewrite-policy on page 675](#).

To apply your HTTP-based routes, select them when you configure the server policy. For details, see [server-policy policy on page 150](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config server-policy HTTP-content-routing-policy
edit "<routing-policy_name>"
    set server-pool "<server-pool_name>"
    set HTTP-content-routing-id <HTTP-content-routing-id_str>
    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 | HTTPS-sni | geo-ip | ztna-ems-tags}
            set match-condition {match-begin | match-end | match-sub | match-domain |
                match-dir | match-reg | ip-range | ip-range6 | equal | ip-list}
            set x509-subject-name {E | CN | OU | O | L | ST | C}
            set match-expression "<match-expression_str>"
```

```

set
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 reverse {enable | disable}
set concatenate {and | or}
set country-list <country-list_str>
set ip-list <ip-list_str>
next
end
next
end

```

Variable	Description	Default
"<routing-policy_name>"	Enter the name of the HTTP content routing policy. The maximum length is 63 characters. To display the list of existing policies, enter: edit ?	No default.
server-pool "<server-pool_name>"	Enter the name of the server pool to which FortiWeb forwards traffic when the traffic matches rules in this policy. For details, see server-policy server-pool on page 182 .	No default.
<entry_index>	Enter the index number of the individual rule in the table. The valid range is 1–9,999,999,999,999,999.	No default.
HTTP-content-routing-id <HTTP-content-routing-id_str>	Enter a HTTP content routing policy sequence number.	No default.
match-object {HTTP-host HTTP-request url-parameter HTTP-referer HTTP-cookie HTTP-header source-ip x509-certificate-Subject x509-certificate-Extension HTTPS-sni geo-ip ztna-ems-tags}	Enter 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 • HTTPS-sni— Select this option so that FortiWeb will	No default.

Variable	Description	Default
	forward requests based on the SNI in the SSL handshake. • <code>geo-ip</code>— Select this option so that FortiWeb matches against the IP addresses from specified countries. • <code>ztna-ems-tags</code>— Select this option so that FortiWeb matches against the ZTNA tags.	
<code>match-condition {match-begin match-end match-sub match-domain match-dir match-reg ip-range ip-range6 equal ip-list}</code>	Enter the type of value to match. Values can be a literal value that appears in the object or a regular expression. The value of <code>match-object</code> (<code>HTTP-host</code> <code>HTTP-request</code> <code>url-parameter</code> <code>HTTP-referer</code> <code>HTTP-cookie</code> <code>HTTP-header</code> <code>source-ip</code> <code>x509-certificate-Subject</code> <code>x509-certificate-Extension</code> <code>HTTPS-sni</code> <code>geo-ip</code> <code>ztna-ems-tags</code>) on page 119 determines which content types you can specify. If <code>match-object</code> is <code>HTTP-host</code>, <code>HTTP-request</code>, <code>HTTP-referer</code>, or <code>x509-certificate-Extension</code>: • <code>match-begin</code>—The object to match begins with the specified string. • <code>match-end</code>—The object to match ends with the specified string. • <code>match-sub</code>—The object to match contains the specified string. • <code>match-domain</code>—The host to match contains the specified string between the periods in a domain name. • <code>ip-list</code>—The IPs to match. If <code>match-object</code> is <code>HTTP-host</code> only: • <code>match-domain</code>—The object to match contains the specified string between the periods in a domain name. For example, if <code>match-expression</code> is <code>abc</code>, the condition matches the following hostnames: <pre> dname1.abc.com dname1.dname2.abc.com </pre> However, the same Match Simple String value does not match the following hostnames: <pre> abc.com dname.abc </pre> If <code>match-object</code> is <code>HTTP-request</code>: • <code>match-dir</code>—The object to match contains the specified string between delimiting characters (slash) in a domain name.	No default.

Variable	Description	Default
	For example, if <code>match-expression</code> is <code>abc</code>, the condition matches the following hostnames: <pre>test.com/abc/ test.com/dir1/abc/</pre> However, the same <code>match-string</code> value does not match the following hostnames: <pre>test.com/abc test.abc.com</pre> If <code>match-object</code> is <code>source-ip</code>: <code>ip-range</code>—The source IP to match is an IPv4 IP address or within a range of IPv4 IP addresses. <code>ip-range6</code>—The source IP to match is an IPv6 IP address or within a range of IPv6 IP addresses. If <code>match-object</code> is <code>HTTP-host</code>, <code>HTTP-request</code>, <code>HTTP-referer</code>, <code>source-ip</code>, or <code>x509-certificate-Extension</code>: <code>match-reg</code>—The object to match has a value that matches the specified regular expression.	
<code>ztna-ems-tag <tag_name></code>	If <code>match-object</code> is <code>ztna-ems-tags</code> , enter the tag names.	No default.
<code>ztna-ems-tag-combine {and or}</code>	Available only if <code>match-object</code> is <code>ztna-ems-tags</code>. and means the request only matches if it has all tags specified; or means the request matches if it has any of the tags specified. Note: For ZTNA tags, when Reverse is on, it means all the request will be matched except the ones that meet the or or and condition. For example, if <code>Tag_A</code> and <code>Tag_B</code> are specified, and the Reverse is on, the matching logic will be: - When ztna-ems-tag-combine is or, all the request will be matched except the ones having any of the <code>Tag_A</code> and <code>Tag_B</code> tags. - When ztna-ems-tag-combine is and, all the requests will be matched except the ones having both <code>Tag_A</code> and <code>Tag_B</code> tags.	and
<code>x509-subject-name {E CN OU O L ST C}</code>	Enter the attribute type to match. Available when <code>match-object</code> {<code>HTTP-host</code> <code>HTTP-request</code> <code>url-parameter</code> <code>HTTP-referer</code> <code>HTTP-cookie</code> <code>HTTP-header</code>	No default.

Variable	Description	Default
	 source-ip x509-certificate-Subject x509-certificate-Extension HTTPS-sni geo-ip ztna-ems-tags on page 119 is <code>x509-certificate-Subject</code> .	
<code>match-expression "<match-expression_str>"</code>	Enter a value to match in the object element specified by match-object {HTTP-host HTTP-request url-parameter HTTP-referer HTTP-cookie HTTP-header source-ip x509-certificate-Subject x509-certificate-Extension HTTPS-sni geo-ip ztna-ems-tags} on page 119 and <code>match-condition</code>. Examples: - A literal URL, such as <code>/index.php</code>, that a matching HTTP request contains. - An expression, such as <code>^/*.php</code>, that matches a URL. Tip: When you enter a regular expression using the web UI, you can validate its syntax.	No default.
<code>value-match-condition {match-begin match-end match-sub match-reg equal}</code>	Enter the type of value to match. The value refers to the <code>x509-subject-name</code> and can be a literal value that appears in the object or a regular expression. <code>match-begin</code>—The name to match begins with the specified string. <code>match-end</code>—The name to match ends with the specified string. <code>match-sub</code>—The name to match contains the specified string. <code>equal</code>—The name to match is the specified string. <code>match-reg</code>—The name to match matches the specified regular expression.	No default.
<code>name "<name_str>"</code>	Enter 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 only if match-object {HTTP-host HTTP-request url-parameter HTTP-referer HTTP-cookie HTTP-header source-ip x509-certificate-Subject x509-certificate-Extension HTTPS-sni geo-ip ztna-ems-tags} on page 119 is <code>url-parameter</code>, <code>HTTP-cookie</code>, or <code>HTTP-header</code>.	No default.
<code>name-match-condition {match-begin match-end match-sub match-reg equal}</code>	Enter the type of value to match. The value is specified by <code>name</code> and can be a literal value that appears in the object or a regular expression. <code>match-begin</code>—The name to match begins with the specified string. <code>match-end</code>—The name to match ends with the specified string.	No default.

Variable	Description	Default
	<code>match-sub</code>—The name to match contains the specified string. <code>equal</code>—The name to match is the specified string. <code>match-reg</code>—The name to match matches the specified regular expression.	
value "<value_str>"	Enter the object value to match. The value can be a literal value or a regular expression. Available if match-object {HTTP-host HTTP-request url-parameter HTTP-referer HTTP-cookie HTTP-header source-ip x509-certificate-Subject x509-certificate-Extension HTTPS-sni geo-ip ztna-ems-tags} on page 119 is url-parameter, HTTP-cookie, or HTTP-header.	No default.
value-match-condition {match-begin match-end match-sub match-reg equal}	Enter the type of value to match. The value is specified by value and can be a literal value or a regular expression. <code>match-begin</code>—The value to match begins with the specified string. <code>match-end</code>—The value to match ends with the specified string. <code>match-sub</code>—The value to match contains the specified string. <code>equal</code>—The value to match is the specified string. <code>match-reg</code>—The value to match matches the specified regular expression.	No default.
start-ip "<start_ip>"	Enter the first IP address in a range of IP addresses. Available if match-condition {match-begin match-end match-sub match-domain match-dir match-reg ip-range ip-range6 equal ip-list} on page 120 is ip-range or ip-range6.	No default.
end-ip "<end_ip>"	Enter the last IP address in a range of IP addresses. Available if match-object {HTTP-host HTTP-request url-parameter HTTP-referer HTTP-cookie HTTP-header source-ip x509-certificate-Subject x509-certificate-Extension HTTPS-sni geo-ip ztna-ems-tags} on page 119 is source-ip	No default.
reverse {enable disable}	When enabled, FortiWeb will route requests to the server pool that do not match the specified values for the Match Object.	disable
country-list <country-list_str>	Select countries where the IP addresses originate.	No default.
concatenate {and or}	Select either: <code>and</code>—A matching request matches this entry in addition to other entries in the HTTP content routing	and

Variable	Description	Default
	list. or—A matching request matches this entry or other entries in the list.	
ip-list <ip-list_str>	Enter multiple IPs or IP range.	No default.

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

- [server-policy server-pool on page 182](#)
- [server-policy policy on page 150](#)
- [waf url-rewrite url-rewrite-policy on page 675](#)

server-policy ip-group

Use this command to group IP addresses or IP ranges, so that you can later reference them in **IP Protection > IP List** (`config waf ip-list`).

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

Syntax

```
config server-policy ip-group
  edit <index>
    config members
      edit <index>
        set ip <IP_addresses_or_ranges>
      next
    end
  next
end
```

Variable	Description	Default
<IP_addresses_or_ranges>	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). Multiple addresses or ranges should be separated with comma ",". - A range or addresses (e.g. 1.2.3.4,2001::1,1.2.3.4-1.2.3.40,2001::1-2001::100).	No default.

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 details, see [Permissions on page 46](#).

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>"	Enter the name of the custom data type. The maximum length is 63 characters.	No default.

Variable	Description	Default
	To display the list of existing types, enter: edit ?	
expression "<regex_pattern>"	Enter 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
```

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

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

This command applies to all the server-policies. If you want to define an allow list that applies specifically to a certain server policy, use `config server-policy allow-list` instead of this one.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For details, see [Permissions on page 46](#).

Syntax

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

```

set request-file "<url_str>"
set header-type {plain | regular}
set value-status {enable | disable}
set value-type {plain | regular}
set value <header_value_string>
next
end

```

Variable	Description	Default
<entry_index>	Enter the index number of the individual rule in the table. The valid range is 1–9,223,372,036,854,775,807.	No default.
status {enable disable}	Enable to exempt this object from all scans.	enable
type {Cookie Parameter URL Header_Field }	Indicate the type of the object. Depending on your selection, the remaining settings vary.	URL
path "<url_str>"	Enter the path as it appears in the cookie, such as / or /blog/folder. This setting is available if type {Cookie Parameter URL Header_Field } on page 127 is set to <code>Cookie</code> .	No default.
wildcard {enable disable}	The wildcard option is available if the type is Cookie . Enable wildcard matching for the cookie name. When enabled, the asterisk (*) character can match zero or more characters. Up to two asterisks are allowed per name , and matching is case-sensitive . Wildcards can appear at the beginning , middle , or end of the name. Examples: • <code>_ga*</code> matches <code>_ga</code>, <code>_ga123</code> • <code>*_gid</code> matches <code>_gid</code>, <code>abc_gid</code> • <code>aaa*bbb</code> matches <code>aaabbbb</code>, <code>aaa123bbb</code> • <code>*aaa*bbb</code> matches <code>xyzaaa123bbb</code>	disable
request-type {plain regular}	Indicate whether the request-file "<url_str>" on page 128 field contains a literal URL (<code>plain</code>), or a regular expression designed to match multiple URLs (<code>regular</code>). This setting is available if type {Cookie Parameter URL Header_Field } on page 127 is set to <code>URL</code> .	plain
domain-type {plain regular}	Indicate whether the <code>domain "<cookie_str>"</code> field will contain a literal domain/IP address (Simple String), or a regular expression designed to match multiple domains/IP addresses (Regular Expression).	plain
domain "<cookie_str>"	Enter the partial or complete domain name or IP address as it appears in the cookie, such as: <code>www.example.com</code> <code>.google.com</code> <code>192.0.2.50</code>	No default.

Variable	Description	Default
	If clients sometimes access the host via IP address instead of DNS, create allow list objects for both. This setting is available if type {Cookie Parameter URL Header_Field } on page 127 is set to <code>Cookie</code>. Caution: Do not allowlist untrusted subdomains that use vulnerable cookies. It could compromise the security of that domain and its network.	
name-type {plain regular}	Indicate whether the name " <code><name_str></code> " field will contain a literal parameter name (Simple String), or a regular expression designed to match all parameter names (Regular Expression).	plain
name " <code><name_str></code> "	Depending on your selection in type {Cookie Parameter URL Header_Field } on page 127, either: - Enter the name of the cookie as it appears in the HTTP request, such as <code>NID</code>. - Enter the name of the parameter as it appears in the HTTP URL or body, such as <code>rememberme</code>. This setting is available if type {Cookie Parameter URL Header_Field } on page 127 is set to <code>Cookie</code>, <code>Parameter</code>, or <code>Header_Field</code>.	No default.
request-file-status {enable disable}	Enable to apply this rule only to HTTP requests for specific URLs. Configure <code>request-file "<code><url_str></code>"</code> if it is enabled.	disable
domain-status {enable disable}	Enable to apply this rule only to HTTP requests for specific domains. If enabled, also configure <code>domain "<code><cookie_str></code>"</code>.	disable
request-file " <code><url_str></code> "	Depending on your selection in the request-type {plain regular} on page 127 field, enter either: - The literal URL, such as <code>/robots.txt</code>, that the HTTP request must contain in order to match the rule. The URL must begin with a backslash (<code>/</code>). - A regular expression, such as <code>^/*.html</code>, matching all and only the URLs to which the rule should apply. The pattern does not require a slash (<code>/</code>); however, it must at match URLs that begin with a backslash, such as <code>/index.html</code>. Do not include the domain name, such as <code>www.example.com</code>. This setting is available if type {Cookie Parameter URL Header_Field } on page 127 is set to <code>URL</code>.	

Variable	Description	Default
header-type {plain regular}	Indicate whether the type field will contain a literal name (plain), or a regular expression designed to match multiple names (regular).	plain
value-status {enable disable}	Enable to also check the value of the HTTP header. Only the HTTP headers which match both the name and the value will be allowlisted.	disable
value-type {plain regular}	Indicate whether the header name will contain a literal name (plain), or a regular expression designed to match multiple names (regular).	plain
value <header_value_string>	The value of the HTTP header. Depending on your selection in the <code>value-type</code> field, enter either a literal value or a regular expression.	No default.

Example

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

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

Related topics

- [waf web-protection-profile inline-protection on page 696](#)

server-policy pattern threat-score-profile

The settings in `config server-policy pattern threat-weight` apply to all the web protection profiles in a ADOM. However, if you want to differentiate the Threat Score settings in different web protection profiles, you can use `server-policy pattern threat-score-profile` to create multiple Threat Score profiles and apply them to different web protection profiles.

For details about Threat Weight, see the *FortiWeb Administration Guide*:

<http://docs.fortinet.com/fortiweb/admin-guides>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config server-policy pattern threat-score-profile
```

```

edit <name>
  set low-level-score-end <level_int>
  set medium-level-score-end <level_int>
  set statistics-period {one-day | three-days | one-week}
  set malicious-action {none | alert | alert_deny | block-period | client-id-block-
    period}
  set malicious-block-period <minutes_int>
  set suspicious-action {none | alert | alert_deny | block-period | client-id-block-
    period}
  set suspicious-block-period <minutes_int>
  set signature-only-threat-score {enable | disable}
  set signature-score-threshold <int>
  set signature-action {alert | alert_deny | block-period | client-id-block-period}
  set signature-block-period <int>
  set always-record-signature-alog {enable | disable}

end

```

Variable	Description	Default
low-level-score-end <level_int>	Set the low level threat score for different risk levels of a client based on the threat weight sum of all the security violations launched by the client at the time of the last access.	100
medium-level-score-end <level_int>	Set the high threat score for different risk levels of a client based on the threat weight sum of all the security violations launched by the client at the time of the last access.	200
statistics-period {one-day three-days one-week}	Select the amount of time in days that FortiWeb will store the threat score data for an active client. For example, when the statistics period is 3 days, and the total threat score in this period is 150. Then 150 will be taken as the score to compare with those set for trusted/suspicious/malicious clients.	three-days
malicious-action {none alert alert_deny block-period client-id-block-period}	• block-period: Block a malicious client based on source IP. • client-id-block-period: Block a malicious client based on the FortiWeb generated client ID. This is useful when the source IP of a certain client keeps changing. • alert: Accept the connection and generate an alert email and/or log message. • alert_deny : Block the request (or reset the connection) and generate an alert and/or log message.	none
malicious-block-period <minutes_int>	When selecting block-period or client-id-block-period , you need to enter the number of minutes that you want to block subsequent requests from the IP or client. Valid range is 1-1440 minutes.	10

Variable	Description	Default
suspicious-action {none alert alert_deny block-period client-id-block-period}	• block-period: Block a suspicious client based on source IP. • client-id-block-period: Block a suspicious client based on the FortiWeb generated client ID. This is useful when the source IP of a certain client keeps changing. • alert: Accept the connection and generate an alert email and/or log message. • alert_deny : Block the request (or reset the connection) and generate an alert and/or log message.	none
suspicious-block-period <minutes_int>	When selecting block-period or client-id-block-period , you need to enter the number of minutes that you want to block subsequent requests from the IP or client. Valid range is 1-1440 minutes.	10
signature-only-threat-score {enable disable}	Enable signature-only-threat-score to limit Threat Score threshold calculation to signature violations only. When enabled, a single signature violation from the client will not trigger the system to take actions according to the settings on the Signature page. The system will calculate threat scores and take action only when the signature-only-threat-score threshold is reached. An exception is for the Erase action, when means the system will take immediate action if the client violates a signature for which the action is Erase .	disable
signature-score-threshold <int>	Enter a threshold value for the signature violations. Available only when signature-only-threat-score is enabled.	200
signature-action {alert alert_deny block-period client-id-block-period}	• block-period: Block a client based on source IP. • client-id-block-period: Block a client based on the FortiWeb generated client ID. This is useful when the source IP of a certain client keeps changing. • alert: Accept the connection and generate an alert email and/or log message. • alert_deny : Block the request (or reset the connection) and generate an alert and/or log message. Available only when signature-only-threat-score is enabled.	alert_deny
signature-block-period <int>	When selecting block-period or client-id-block-period , you need to enter the number of minutes that you want to block subsequent requests from the IP or client. Available only when signature-only-threat-score is enabled.	10

Variable	Description	Default
always-record-signature- alog {enable disable}	When disabled, the Signature module itself will no longer record logs. Signature log will be generated only when the signature-only-threat-score exceeds the threshold. When enabled, every time a signature rule is triggered, the signature attack log will be generated. Available only when signature-only-threat-score is enabled.	disable

Related Topics

- [waf web-protection-profile inline-protection on page 696](#)

server-policy pattern threat-weight

Use this command to configure the global threat weight of security violations. When a security violation is detected, the threat weight of the security violation is used to calculate the threat score of a client that launched the event.

For details about Threat Weight, see the *FortiWeb Administration Guide*:

<http://docs.fortinet.com/fortiweb/admin-guides>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config server-policy pattern threat-weight
    set allow-hosts-level {low | critical | informational | moderate | substantial | severe}
    set allow-hosts-op {enable | disable}
    set allow-method-level {low | critical | informational | moderate | substantial | severe}
    set allow-method-op {enable | disable}
    set api-management-level {low | critical | informational | moderate | substantial |
        severe}
    set api-management-op {enable | disable}
    set biometrics-based-detection -level {low | critical | informational | moderate |
        substantial | severe}
    set biometrics-based-detection-op {enable | disable}
    set bot-deception-level {low | critical | informational | moderate | substantial |
        severe}
    set bot-deception-op {enable | disable}
    set client-management-expire <time_int>
    set concurrent-users-peraccount- exceeds-limit-level {low | critical | informational |
        moderate | substantial | severe}
    set concurrent-users-peraccount- exceeds-limit-op {enable | disable}
    set cookie-signature-checkfailed- level {low | critical | informational | moderate |
        substantial | severe}
    set cookie-signature-checkfailed- op {enable | disable}
```

```
set cors-protection-level {low | critical | informational | moderate | substantial |
    severe}
set cors-protection-op {enable | disable}
set credential-stuffing-defenselevel {low | critical | informational | moderate |
    substantial | severe}
set credential-stuffing-defenseop {enable | disable}
set csrf-protection-level {low | critical | informational | moderate | substantial |
    severe}
set csrf-protection-op {enable | disable}
set custom-policy-op {enable | disable}
set custom-signature-op {enable | disable}
set fail-to-validate-json-schemalevel {low | critical | informational | moderate |
    substantial | severe}
set fail-to-validate-json-schemaop {enable | disable}
set fail-to-validate-xml-schemalevel {low | critical | informational | moderate |
    substantial | severe}
set fail-to-validate-xml-schemaop {enable | disable}
set forbid-xml-entities-level {low | critical | informational | moderate | substantial |
    severe}
set forbid-xml-entities-op {enable | disable}
set format-xml-allowed-inwebsocket- level {low | critical | informational | moderate |
    substantial | severe}
set format-not-allowed-inwebsocket- op {enable | disable}
set geo-ip-level {low | critical | informational | moderate | substantial | severe}
set geo-ip-op {enable | disable}
set grpc-rate-limit-level {low | critical | informational | moderate | substantial |
    severe}
set grpc-rate-limit-op {enable | disable}
set grpc-parse-level {low | critical | informational | moderate | substantial | severe}
set grpc-parse-op {enable | disable}
set grpc-size-limit-level {low | critical | informational | moderate | substantial |
    severe}
set grpc-size-limit-op {enable | disable}
set hidden-field-protection-level {low | critical | informational | moderate |
    substantial | severe}
set hidden-field-protection-op {enable | disable}
set http-access-limit-level {low | critical | informational | moderate | substantial |
    severe}
set http-access-limit-op {enable | disable}
set http-flood-prevention-level {low | critical | informational | moderate | substantial
    | severe}
set http-flood-prevention-op {enable | disable}
set http-protocol-constraints-op {enable | disable}
set illegal-file-size-level {low | critical | informational | moderate | substantial |
    severe}
set illegal-file-size-op {enable | disable}
set illegal-file-type-level {low | critical | informational | moderate | substantial |
    severe}
set illegal-file-type-op {enable | disable}
set ip-list-level {low | critical | informational | moderate | substantial | severe}
set ip-list-op {enable | disable}
set ip-replay-violation-level {low | critical | informational | moderate | substantial |
    severe}
set ip-replay-violation-op {enable | disable}
set ip-reputation-level {low | critical | informational | moderate | substantial |
    severe}
set ip-reputation-op {enable | disable}
```

```
set json-element-lengthexceeded- level {low | critical | informational | moderate |
    substantial | severe}
set json-element-lengthexceeded- op {enable | disable}
set known-bots-op {enable | disable}
set low-level <level_int>
set low-level-score-end <level_int>
set malicious-action {alert | alert_deny | block-period | client-id-block-period}
set malicious-block-period <minutes_int>
set malicious-file-detected-byfortisandbox- level {low | critical | informational |
    moderate | substantial | severe}
set malicious-file-detected-byfortisandbox- op {enable | disable}
set malicious-ips-level {low | critical | informational | moderate | substantial |
    severe}
set malicious-ips-op {enable | disable}
set man-in-browser-protectionlevel {low | critical | informational | moderate |
    substantial | severe}
set man-in-browser-protectionop {enable | disable}
set medium-level-score-end <level_int>
set ml-bot-detection-level {low | critical | informational | moderate | substantial |
    severe}
set ml-bot-detection-op {enable | disable}
set ml-anomaly-detection-level {low | critical | informational | moderate | substantial |
    severe}
set ml-anomaly-detection-op {enable | disable}
set ml-api-level {low | critical | informational | moderate | substantial | severe}
set ml-api-op {enable | disable}
set mobile-api-protection-level {low | critical | informational | moderate | substantial
    | severe}
set mobile-api-protection-op {enable | disable}
set openapi-validation-level {low | critical | informational | moderate | substantial |
    severe}
set openapi-validation-op {enable | disable}
set origin-not-allowed-level {low | critical | informational | moderate | substantial |
    severe}
set origin-not-allowed-op {enable | disable}
set padding-oracle-protectionlevel {low | critical | informational | moderate |
    substantial | severe}
set padding-oracle-protection-op {enable | disable}
set parameter-validation-level {low | critical | informational | moderate | substantial |
    severe}
set parameter-validation-op {enable | disable}
set quarantined-ip-level {low | critical | informational | moderate | substantial |
    severe}
set quarantined-ip-op {enable | disable}
set session-fixation-protectionlevel {low | critical | informational | moderate |
    substantial | severe}
set session-fixation-protectionop {enable | disable}
set session-idle-timeout-level {low | critical | informational | moderate | substantial |
    severe}
set session-idle-timeout-op {enable | disable}
set signature-op {enable | disable}
set size-exceeds-limit-level {low | critical | informational | moderate | substantial |
    severe}
set size-exceeds-limit-op {enable | disable}
set sql-xss-sbd-op {enable | disable}
set statistics-period {one-day | three-days | one-week}
set suspicious-action {alert | alert_deny | block-period | client-id-block-period}
set suspicious-block-period <minutes_int>
```

```

set tcp-flood-prevention-level {low | critical | informational | moderate | substantial |
    severe}
set tcp-flood-prevention-op {enable | disable}
set threshold-based-detectionlevel {low | critical | informational | moderate |
    substantial | severe}
set threshold-based-detection-op {enable | disable}
set threat-score-profile {enable | disable}
set trojan-detected-level {low | critical | informational | moderate | substantial |
    severe}
set trojan-detected-op {enable | disable}
set url-access-level {low | critical | informational | moderate | substantial | severe}
set url-access-op {enable | disable}
set url-encryption-level {low | critical | informational | moderate | substantial |
    severe}
set url-encryption-op {enable | disable}
set virus-detected-level {low | critical | informational | moderate | substantial |
    severe}
set virus-detected-op {enable | disable}
set websocket-extensions-notallowed-level {low | critical | informational | moderate |
    substantial | severe}
set websocket-extensions-notallowed-op {enable | disable}
set websocket-traffic-notallowed-level {low | critical | informational | moderate |
    substantial | severe}
set websocket-traffic-notallowed-op {enable | disable}
set wsd1-validation-failed-level {low | critical | informational | moderate | substantial
    | severe}
set wsd1-validation-failed-op {enable | disable}
set wsi-check-failed-level {low | critical | informational | moderate | substantial |
    severe}
set wsi-check-failed-op {enable | disable}
set xml-element-lengthexceeded-level {low | critical | informational | moderate |
    substantial | severe}
set xml-element-lengthexceeded-op {enable | disable}
set ztna-level {low | critical | informational | moderate | substantial | severe}
set ztna-op {enable | disable}

```

end

Variable	Description	Default
allow-hosts-level {low critical informational moderate substantial severe}	Set the threat weight for Protected Hostname violations.	moderate
allow-hosts-op {enable disable}	Enable to configure the threat weight for Protected Hostname violations.	disable
allow-method-level {low critical informational moderate substantial severe}	Set the threat weight for HTTP request method violations.	moderate
allow-method-op {enable disable}	Enable to configure the threat weight for HTTP request method violations.	enable

Variable	Description	Default
set api-management-level {low critical informational moderate substantial severe}	Set the threat weight for API Gateway policy violations.	moderate
api-management-op {enable disable}	Enable to configure the threat weight for API Gateway policy violations.	enable
biometrics-based-detection-level {low critical informational moderate substantial severe}	Set the threat weight for biometrics based detection rule violations.	substantial
biometrics-based-detection-op {enable disable}	Enable to configure the threat weight for biometrics based detection rule violations.	disable
bot-deception-level {low critical informational moderate substantial severe}	Set the threat weight for bot deception policy violations.	substantial
bot-deception-op {enable disable}	Enable to configure the threat weight for bot deception policy violations.	disable
client-management-expire <time_int>	Set the amount of time that FortiWeb will store the tracked client information. Once the information has been stored for longer than the set amount of time, FortiWeb will remove that information.	15 days
concurrent-users-per-account-exceeds-limit-level {low critical informational moderate substantial severe}	Set the threat weight for violations that the number of concurrent users per account exceeds the limit.	moderate
concurrent-users-per-account-exceeds-limit-op {enable disable}	Enable to configure the threat weight for violations that the number of concurrent users per account exceeds the limit.	enable
cookie-signature-check-failed-level {low critical informational moderate substantial severe}	When the security mode is None or Signed, enable to configure the threat weight for cookie tampering protection rule violations.	substantial
cookie-signature-check-failed-op {enable disable}	Enable to configure the threat weight for cookie tampering protection rule violations.	enable

Variable	Description	Default
cors-protection-level {low critical informational moderate substantial severe}	Set the threat weight for CORS protection rule violations.	moderate
cors-protection-op {enable disable}	Enable to configure the threat weight for CORS protection rule violations.	enable
credential-stuffing-defense-level {low critical informational moderate substantial severe}	Set the threat weight for Credential Stuffing attacks.	severe
credential-stuffing-defense-op {enable disable}	Enable to configure the threat weight for Credential Stuffing attacks.	enable
csrf-protection-level {low critical informational moderate substantial severe}	Set the threat weight for CSRF protection rule violations.	substantial
csrf-protection-op {enable disable}	Enable to configure the threat weight for CSRF protection rule violations.	enable
custom-policy-op {enable disable}	Enable to configure the threat weight for custom policy violations.	enable
custom-signature-op {enable disable}	Enable to configure the threat weight for custom signature policy violations.	disable
fail-to-validate-json-schema-level {low critical informational moderate substantial severe}	Set the threat weight for JSON protection rule violations.	substantial
fail-to-validate-json-schema-op {enable disable}	Enable to configure the threat weight for violation of failing to validate JSON schema file.	enable
fail-to-validate-xml-schema-level {low critical informational moderate substantial severe}	Set the threat weight for violation of failing to validate JSON schema file.	moderate
fail-to-validate-xml-schema-op {enable disable}	Enable to configure the threat weight for violation of failing to validate XML schema file.	enable

Variable	Description	Default
forbid-xml-entities-level {low critical informational moderate substantial severe}	Set the threat weight for violation of failing to validate XML schema file.	substantial
forbid-xml-entities-op {enable disable}	Enable to configure the threat weight for forbidden XML entities violations.	enable
format-not-allowed-in-websocket-level {low critical informational moderate substantial severe}	When the WebSocket connection is established, data is transmitted in the form of frame. Set the threat weight for violation that frame formats are not allowed.	moderate
format-not-allowed-in-websocket-op {enable disable}	Enable to configure the threat weight for violation that frame formats are not allowed.	enable
geo-ip-level {low critical informational moderate substantial severe}	Set the threat weight for requests from blocked countries or regions based on the associated source IP address.	critical
geo-ip-op {enable disable}	Enable to configure the threat weight for Geo IP block policy violations.	enable
grpc-rate-limit-level {low critical informational moderate substantial severe}	Set the threat weight for gRPC rate limit violations.	moderate
grpc-rate-limit-op {enable disable}	Enable to configure the threat weight for gRPC rate limit violations.	enable
grpc-parse-level {low critical informational moderate substantial severe}	Set the threat weight for gRPC format violations.	substantial
grpc-parse-op {enable disable}	Enable to configure the threat weight for gRPC format violations.	enable
grpc-size-limit-level {low critical informational moderate substantial severe}	Set the threat weight for gRPC size limit violations.	moderate
grpc-size-limit-op {enable disable}	Enable to configure the threat weight for gRPC size limit violations.	enable

Variable	Description	Default
hidden-field-protection-level {low critical informational moderate substantial severe}	Set the threat weight for attempts to tamper with hidden field rules.	substantial
hidden-field-protection-op {enable disable}	Enable to configure the threat weight for hidden field protection rule violations.	enable
http-access-limit-level {low critical informational moderate substantial severe}	Set the threat weight for violation that the number of HTTP requests per second, per source IP address exceeds the limit.	moderate
http-access-limit-op {enable disable}	Enable to configure the threat weight for violation that the number of HTTP requests per second, per source IP address exceeds the limit.	enable
http-flood-prevention-level {low critical informational moderate substantial severe}	Set the threat weight for violation that the number of HTTP requests per second, per session, per URL exceeds the limit.	moderate
HTTP-flood-prevention-op {enable disable}	Enable to configure the threat weight for violation that the number of HTTP requests per second, per session, per URL exceeds the limit.	enable
HTTP-protocol-constraints-op {enable disable}	Enable to configure the threat weight for HTTP protocol constraints. Once enabled, the threat weight for each HTTP protocol constraint may be set using waf HTTP-protocol-parameter-restriction on page 543 .	enable
illegal-file-size-level {low critical informational moderate substantial severe}	Set the threat weight for the file size detection and restriction violation.	moderate
illegal-file-size-op {enable disable}	Enable to configure the threat weight for the file size detection and restriction violation.	enable
illegal-file-type-level {low critical informational moderate substantial severe}	Set the threat weight for the file type detection and restriction violation.	substantial
illegal-file-type-op {enable disable}	Enable to configure the threat weight for the file type detection and restriction violation.	enable

Variable	Description	Default
ip-list-level {low critical informational moderate substantial severe}	Set the threat weight for requests from blocklisted IP addresses.	critical
ip-list-op {enable disable}	Enable to configure the threat weight for requests from blocklisted IP addresses.	enable
ip-replay-violation-level {low critical informational moderate substantial severe}	When the security mode is Encrypted, select whether FortiWeb uses the IP address of a request to determine the owner of the cookie. Set the threat weight for IP replay violations.	substantial
ip-replay-violation-op {enable disable}	Enable to configure the threat weight for IP replay violations.	enable
ip-reputation-level {low critical informational moderate substantial severe}	Set the threat weight for requests from IP addresses with a poor reputation.	critical
ip-reputation-op {enable disable}	Enable to configure the threat weight for requests from IP addresses with a poor reputation.	enable
json-element-length-exceeded-level {low critical informational moderate substantial severe}	Set the threat weight for the violation that the JSON element length exceeds.	moderate
json-element-length-exceeded-op {enable disable}	Enable to configure the threat weight for the violation that the JSON element length exceeds.	enable
known-bots-op {enable disable}	Enable to configure the threat weight for the known bots attacks.	disable
low-level <level_int>	Set the risk level value for Low level.	10
low-level-score-end <level_int>	Set the low level threat score for different risk levels of a client based on the threat weight sum of all the security violations launched by the client at the time of the last access.	100
malicious-action {alert alert_deny block-period client-id-block-period}	block-period: Block a malicious client based on source IP. client-id-block-period: Block a malicious client based on the FortiWeb generated client ID. This is useful when the source IP of a certain client keeps changing.	none

Variable	Description	Default
	• alert: Accept the connection and generate an alert email and/or log message. • alert_deny : Block the request (or reset the connection) and generate an alert and/or log message.	
malicious-block-period	When selecting block-period or client-id-block-period , you need to enter the number of minutes that you want to block subsequent requests from the IP or client. Valid range is 1-1440 minutes.	10
malicious-file-detected-by-fortisandbox-level {low critical informational moderate substantial severe}	Set the threat weight for the violation of malicious file detection by FortiSandbox.	severe
malicious-file-detected-by-fortisandbox-op {enable disable}	Enable to configure the threat weight for the violation of malicious file detection by FortiSandbox.	enable
malicious-ips-level {low critical informational moderate substantial severe}	Set the threat weight for the violation that the number of TCP connections per HTTP session exceeds the limit.	moderate
malicious-ips-op {enable disable}	Enable to configure the threat weight the violation that the number of TCP connections per HTTP session exceeds the limit.	enable
man-in-browser-protection-level {low critical informational moderate substantial severe}	Set the threat weight for MiTB attacks.	substantial
man-in-browser-protection-op {enable disable}	Enable to configure the threat weight for MiTB attacks.	enable
medium-level-score-end <level_int>	Set the high threat score for different risk levels of a client based on the threat weight sum of all the security violations launched by the client at the time of the last access.	200
ml-bot-detection-level {low critical informational moderate substantial severe}	Set the threat weight for ML Based Bot Detection rule violations.	moderate

Variable	Description	Default
ml-bot-detection-op {enable disable}	Enable to configure the threat weight for ML Based Bot Detection rule violations.	disable
ml-anomaly-detection-level {low critical informational moderate substantial severe}	Set the threat weight for ML Anomaly Detection rule violations.	substantial
ml-anomaly-detection-op {enable disable}	Enable to configure the threat weight for ML Anomaly Detection rule violations.	disable
ml-api-level {low critical informational moderate substantial severe}	Set the threat weight for ML API Detection rule violations.	substantial
ml-api-op {enable disable}	Enable to configure the threat weight for ML API Detection rule violations.	disable
mobile-api-protection-level {low critical informational moderate substantial severe}	Set the threat weight for mobile API protection rule violations.	substantial
mobile-api-protection-op {enable disable}	Enable to configure the threat weight for mobile API protection rule violations.	enable
openapi-validation-level {low critical informational moderate substantial severe}	Set the threat weight for OpenAPI validation rule violations.	moderate
openapi-validation-op {enable disable}	Enable to configure the threat weight for OpenAPI validation rule violations.	enable
origin-not-allowed-level {low critical informational moderate substantial severe}	Set the threat weight for the violation of origin not allowed.	low
origin-not-allowed-op {enable disable}	Enable to configure the threat weight for the violation of origin not allowed.	enable
padding-oracle-protection-level {low critical informational moderate substantial severe}	Set the threat weight for padding oracle attacks.	severe
padding-oracle-protection-op {enable disable}	Enable to configure the threat weight for padding oracle attacks.	enable

Variable	Description	Default
parameter-validation-level {low critical informational moderate substantial severe}	Set the threat weight for parameter validation violation.	moderate
parameter-validation-op {enable disable}	Enable to configure threat weight for parameter validation violation.	enable
quarantined-ip-level {low critical informational moderate substantial severe}	Set the threat weight for FortiGate Quarantined IPs.	critical
quarantined-ip-op {enable disable}	Enable to configure the threat weight for FortiGate Quarantined IPs.	disable
session-fixation-protection-level {low critical informational moderate substantial severe}	Set the threat weight for session fixation protection rule violation.	moderate
session-fixation-protection-op {enable disable}	Enable to configure the threat weight for session fixation protection rule violation.	enable
session-idle-timeout-level {low critical informational moderate substantial severe}	Set the threat weight for the violation of session idle timeout.	moderate
session-idle-timeout-op {enable disable}	Enable to configure the threat weight for the violation of session idle timeout.	enable
signature-op {enable disable}	Enable to set the threat weight for each signature rule.	enable
size-exceeds-limit-level {low critical informational moderate substantial severe}	Set the threat weight for the violation when the maximum acceptable frame header and body size in bytes exceeds the limit.	moderate
size-exceeds-limit-op {enable disable}	Enable to configure the threat weight for the violation when the maximum acceptable frame header and body size in bytes exceeds the limit.	enable
sql-xss-sbd-op {enable disable}	Enable to configure the threat weight for the SQL/XSS syntax based detection rule violation.	enable
statistics-period {one-day three-days one-week}	Select the amount of time in days that FortiWeb will store the threat score data for an active client.	three-days

Variable	Description	Default
	For example, when the statistics period is 3 days, and the total threat score in this period is 150. Then 150 will be taken as the score to compare with those set for thrusted/suspicious/malicious clients.	
suspicious-action {alert alert_deny block-period client-id-block-period}	• block-period: Block a suspicious client based on source IP. • client-id-block-period: Block a suspicious client based on the FortiWeb generated client ID. This is useful when the source IP of a certain client keeps changing. • alert: Accept the connection and generate an alert email and/or log message. • alert_deny : Block the request (or reset the connection) and generate an alert and/or log message.	none
suspicious-block-period	When selecting block-period or client-id-block-period , you need to enter the number of minutes that you want to block subsequent requests from the IP or client. Valid range is 1-1440 minutes.	10
tcp-flood-prevention-level {low critical informational moderate substantial severe}	Set the threat weight for the violation when the number of fully-formed TCP connections per source IP address exceeds the limit.	moderate
tcp-flood-prevention-op {enable disable}	Enable to configure the threat weight for the violation when the number of fully-formed TCP connections per source IP address exceeds the limit.	enable
threshold-based-detection-level {low critical informational moderate substantial severe}	Set the threat weight for the threshold based detection rule violation.	substantial
threshold-based-detection-op {enable disable}	Enable to configure the threat weight for the threshold based detection rule violation.	disable
threat-score-profile {enable disable}	If you want to differentiate the Threat Score settings in different web protection profiles, you can enable threat-score-profile . After enabling it, use <code>config server-policy pattern threat-score-profile</code> to create multiple	disable

Variable	Description	Default
	Threat Score profiles and apply them to different web protection profiles.	
trojan-detected-level {low critical informational moderate substantial severe}	Set the threat weight for the Trojan detection rule violation.	enable
trojan-detected-op {enable disable}	Enable to configure the threat weight for the Trojan detection rule violation.	severe
url-access-level {low critical informational moderate substantial severe}	Set the threat weight for the URL access rule violation.	substantial
url-access-op {enable disable}	Enable to configure the threat weight for the URL access rule violation.	enable
url-encryption-level {low critical informational moderate substantial severe}	Set the threat weight for URL Encryption rule violations.	substantial
url-encryption-op {enable disable}	Enable to configure the threat weight for URL Encryption rule violations.	disable
virus-detected-level {low critical informational moderate substantial severe}	Set the threat weight for the virus detection rule violation.	critical
virus-detected-op {enable disable}	Enable to configure the threat weight for the virus detection rule violation.	enable
websocket-extensions-not-allowed-level {low critical informational moderate substantial severe}	Set the threat weight for the violation of extension header in WebSocket handshake packet.	substantial
websocket-extensions-not-allowed-op {enable disable}	Enable to configure the threat weight for the violation of extension header in WebSocket handshake packet.	enable
websocket-traffic-not-allowed-level {low critical informational moderate substantial severe}	Set the threat weight for the WebSocket traffic blocking violation.	substantial

Variable	Description	Default
websocket-traffic-not-allowed-op {enable disable}	Enable to configure the threat weight for the WebSocket traffic blocking violation.	enable
wSDL-validation-failed-level {low critical informational moderate substantial severe}	Set the threat weight for the WSDL file validation rule violation.	substantial
wSDL-validation-failed-op {enable disable}	Enable to set the threat weight for the WSDL file validation rule violation.	enable
wsi-check-failed-level {low critical informational moderate substantial severe}	Set the threat weight for the WS-security rule violation.	moderate
wsi-check-failed-op {enable disable}	Enable to set the threat weight for the WS-security rule violation.	enable
xml-element-length-exceeded-level {low critical informational moderate substantial severe}	Set the threat weight for the violation that the XML element length exceeds.	moderate
xml-element-length-exceeded-op {enable disable}	Enable to configure the threat weight for the violation that the XML element length exceeds.	enable
ztna-level {low critical informational moderate substantial severe}	Set the threat weight for ZTNA rule violations.	substantial
ztna-op {enable disable}	Enable to configure the threat weight for ZTNA rule violations.	disable

Related Topics

- [waf web-protection-profile inline-protection on page 696](#)

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 [server-policy server-pool on page 182](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For details, see [Permissions on page 46](#).

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>"
    set secure-cookie {enable | disable}
  next
end
```

Variable	Description	Default
"<persistence-policy_name>"	Enter the name of the persistence policy. The maximum length is 63 characters. To display the list of existing persistence policies, enter: edit ?	No 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 }	<code>source-ip</code>—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 "<v4mask>" on page 149 and ipv6-mask-length "<v6mask>" on page 149. <code>persistent-cookie</code>—If an initial request contains a cookie whose name matches the cookie-name "<cookie-name_str>" on page 149 value, FortiWeb forwards subsequent requests that contain the same cookie value to the same pool member as the initial request. <code>asp-sessionid</code>—If a cookie in the initial	<code>source-ip</code>

Variable	Description	Default
	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. • <code>php-sessionid</code>—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. • <code>jsp-sessionid</code>—FortiWeb forwards subsequent requests with the same JSP session ID as the initial request to the same pool member. FortiWeb preserves the original cookie name. • <code>insert-cookie</code>—FortiWeb inserts a cookie with the name specified by <code>cookie-name</code> "<code><cookie-name_str></code>" on page 149 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 <code>cookie-path</code> "<code><cookie-path_str></code>" on page 150 and <code>cookie-domain</code> "<code><cookie-domain_str></code>" on page 150. • <code>HTTP-header</code>—Forwards subsequent requests with the same value for an HTTP header as the initial request to the same pool member. Also configure <code>HTTP-header</code>.	
	• <code>url-parameter</code>—Forwards subsequent requests with the same value for a URL parameter as the initial request to the same pool member. Also configure <code>url-parameter</code>. • <code>rewrite-cookie</code>—If the HTTP response has a <code>Set-Cookie:</code> value that matches the value specified by <code>cookie-name</code> "<code><cookie-name_str></code>" on page 149, 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. • <code>embedded-cookie</code>—If the HTTP response contains a cookie with the name specified by <code>cookie-name</code> "<code><cookie-name_str></code>" on page	

Variable	Description	Default
	149, 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. <code>ssl-session-id</code>—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 <code>sessioncookie-enforce</code> setting to maintain persistence for transactions within a session. For details, see server-policy policy on page 150.	
cookie-name "<cookie-name_str>"	Enter a value to match or the name of the cookie that FortiWeb inserts. Available only when the persistence type uses a cookie.	No default.
timeout "<timeout_int>"	Enter 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>"	Enter the IPv4 subnet used for session persistence. For example, if IPv4 Netmask is 255.255.255.255, FortiWeb can forward requests from IP addresses 192.0.2.1 and 192.0.2.2 to different server pool members. If IPv4 Netmask is 255.255.255.0, FortiWeb forwards requests from IP addresses 192.0.2.1 and 192.0.2.2 to the same pool member.	255.255.255.255
ipv6-mask-length "<v6mask>"	Enter the IPv6 network prefix used for session persistence.	128
HTTP-header "<HTTP-header_str>"	Enter the name of the HTTP header that the persistence feature uses to route requests.	No default.

Variable	Description	Default
url-parameter "<url-parameter_str>"	Enter the name of the URL parameter that the persistence feature uses to route requests.	No default.
cookie-path "<cookie-path_str>"	Enter a path attribute for the cookie that FortiWeb inserts, if type { source-ip persistent-cookie asp-sessionid php-sessionid jsp-sessionid insert-cookie HTTP-header url-parameter rewrite-cookie embedded-cookie ssl-session-id } on page 147 is insert-cookie.	No default.
cookie-domain "<cookie-domain_str>"	Enter a domain attribute for the cookie that FortiWeb inserts, if type { source-ip persistent-cookie asp-sessionid php-sessionid jsp-sessionid insert-cookie HTTP-header url-parameter rewrite-cookie embedded-cookie ssl-session-id } on page 147 is insert-cookie.	No default.
secure-cookie {enable disable}	Configure the secure cookie to force browsers to return the cookie only for HTTPS traffic.	disable

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

- [server-policy server-pool on page 182](#)

server-policy policy

Use this command to configure HTTP, FTP, and AD FS server policies.

FortiWeb applies only one server policy to each connection.

HTTP policy behavior varies by the operation mode. FTP and AD FS server policies are available only in Reverse Proxy mode. For details, see *FortiWeb Administration Guide*:

<http://docs.fortinet.com/fortiweb/admin-guides>



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

To determine which type of server policy to create, configure [protocol {HTTP | FTP | ADFSPIP} on page 164](#).

Before you configure an HTTP server policy, you can configure several policies and profiles:

- Configure a virtual server and server pool. For details, see [server-policy vserver on page 215](#) and [server-policy server-pool on page 182](#).
- To route traffic based on headers in the HTTP layer, configure one or more HTTP content routing policies. For details, see [server-policy HTTP-content-routing-policy on page 118](#).
- To restrict traffic based upon which hosts you want to protect, configure a group of protected host names. For details, see [server-policy allow-hosts on page 106](#).
- 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. For details, see [user ldap-user on page 397](#), [user local-user on page 401](#), [user ntlm-user on page 402](#), [user user-group on page 413](#), [waf HTTP-authen HTTP-authen-rule on page 529](#), and [waf HTTP-authen HTTP-authen-policy on page 527](#).
- To apply a web protection profile to a server policy, you must first configure them. For details, see [waf web-protection-profile inline-protection on page 696](#) (Reverse Proxy mode or either of the transparent modes), or [waf web-protection-profile offline-protection on page 706](#) (Offline Protection mode).
- 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. For details, see [system certificate local on page 258](#), [system certificate sni on page 264](#), and [system certificate urlcert on page 268](#).
- 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 [system certificate verify on page 269](#).

You can also use SNMP traps to notify you of policy status changes, or when a policy enforces your network usage policy. For details, see [system snmp community on page 375](#).

Before you configure an FTP server policy, you need to:

- Configure an FTP command restriction rule. For details, see [waf ftp-command-restriction-rule on page 505](#).
- Configure an FTP file check rule. For details, see [waf ftp-file-security on page 508](#).
- Enable IP reputation intelligence. For details, see [waf ip-intelligence-ignore-x-forwarded-for on page 560](#).
- Create a geo IP rule. For details, see [waf geo-block-list on page 511](#).
- Create an IP list. For details, see [waf ip-list on page 561](#).
- Configure an FTP security inline profile. For details, see [waf ftp-protection-profile](#).

Before you configure an AD FS server policy, you need to:

- Configure a virtual server and server pool. For details, see [server-policy vserver on page 215](#) and [server-policy server-pool on page 182](#).
- Import a certificate file and a CA file. For details, see [system certificate local on page 258](#) and [system certificate ca on page 249](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For details, see [Permissions on page 46](#).

Syntax

```

config server-policy policy
edit "<policy_name>"
    set allow-hosts "<hosts_name>"
    set block-port <port_int>
    set case-sensitive {enable | disable}
    set certificate "<certificate_name>"
    set chunk-encoding {enable | disable}
    set client-certificate-forwarding {enable | disable}
    set server-policy policy
    set client-certificate-forwarding-sub-header "<header_str>"
    set client-real-ip {enable | disable}
    set client-real-ip-random-port {enable | disable}
    set real-ip-addr <real-ip-addr_str>
    set client-timeout <seconds_int>
    set comment "<comment_str>"
    set data-capture-port <port_int>
    set deployment-mode {server-pool | HTTP-content-routing | offline-protection |
        transparent-servers | wccp-servers}
    set ftp-protection-profile <profile_name>
    set half-open-threshold <packets_int>
    set hpkp-header "<hpkp_name>"
    set hsts-header {enable | disable}
    set hsts-max-age <timeout_int>
    set HTTP2 {enable | disable}
    set http2-window-size <int>
    set HTTP-header-timeout <seconds_int>
    set http-parse-max-size <integer>
    set HTTP-pipeline {enable | disable}
    set HTTP-to-HTTPS {enable | disable}
    set redirect-naked-domain {enable | disable}
    set HTTPS-service "<service_name>"
    set implicit_ssl {enable | disable}
    set intermediate-certificate-group "<CA-group_name>"
    set internal-cookie-HTTPonly {enable | disable}
    set internal-cookie-secure {enable | disable}
    set internal-cookie-samesite {enable | disable}
    set internal-cookie-samesite-value {strict | lax | none}
    set monitor-mode {enable | disable}
    set noparse {enable | disable}
    set prefer-current-session {enable | disable}
    set protocol {HTTP | FTP | ADFSPIP}
    set server-pool "<server-pool_name>"
    set service "<service_name>"
    set proxy-protocol {enable | disable}
    set use-proxy-protocol-addr {enable | disable} on page 162
    set replacemsg <replacemsg_name>
    set sessioncookie-enforce {enable | disable}
    set sni {enable | disable}
    set sni-certificate "<sni_name>"
    set sni-strict {enable | disable}
    set certificate-type {enable | disable}
    set lets-certificate <name>
    set ssl {enable | disable}
    set ssl-cipher {medium | high | custom}
    set ssl-client-verify "<verifier_name>"

```



```

set ssl-custom-cipher {<cipher_1> <cipher2> <cipher3> ...}
set tls13-custom-cipher {<cipher_1> <cipher2> <cipher3> ...}
set rfc7919-comply {enable | disable}
set supported-groups {X25519 | prime256v1 | secp384r1 | secp521r1 |
    brainpoolP256r1 | brainpoolP384r1 | brainpoolP512r1 | ffdhe2048 | ffdhe3072 |
    ffdhe4096 | ffdhe6144 | ffdhe8192}
set ssl-noreg {enable | disable}
set ssl-quiet-shutdown {enable | disable}
set ssl-session-timeout <ssl-session-timeout_int>
set status {enable | disable}
set syncookie {enable | disable}
set tcp-recv-timeout <seconds_int>
set tls-v10 {enable | disable}
set tls-v11 {enable | disable}
set tls-v12 {enable | disable}
set tls-v13 {enable | disable}
set urlcert {enable | disable}
set urlcert-group "<urlcert-group_name>"
set urlcert-hlen <len_int>
set vserver "<vserver_name>"
set v-zone "<bridge_name>"
set server-policy policy
set traffic-mirror {enable | disable}
set traffic-mirror-type {client-side | server-side | both-side}
set traffic-mirror-profile <traffic-mirror-profile_str>
set adfs-certificate-ssl-client-verify <adfs-certificate-ssl-client-verify_str>
set adfs-certificate-service <adfs-certificate-service_str>
set multi-certificate {enable | disable}
set certificate-group <certificate-group_str>
set acceleration-policy <acceleration-policy_str>
set web-cache {enable | disable}
set retry-on {enable | disable}
set retry-on-cache-size <retry-on-cache-size_int>
set retry-on-connect-failure {enable | disable}
set retry-times-on-connect-failure <retry-times-on-connect-failure_int>
set retry-on-HTTP-layer {enable | disable}
set retry-times-on-HTTP-layer <retry-times-on-HTTP-layer_int>
set retry-on-HTTP-response-codes {404 | 408 | 500 | 501 | 502 | 503 | 504}
set replacemsg-on-connect-failure {disable | enable}
set tcp-conn-timeout <integer>
set ztna-profile <string>
set reply-100-continue {enable | disable}
set forward-expect-100-continue {enable | disable}
set transaction-based-persistence {enable | disable}
set no-ssl-error-log {enable | disable}
set server-latency-alert <integer>
config HTTP-content-routing-list
    edit <entry_index>
        set content-routing-policy-name "<content-routing_name>"
        set is-default {yes | no}
        set profile-inherit {enable | disable}
        set server-policy policy
    next
end
next
end

```

Variable	Description	Default
"<policy_name>"	Enter the name of the policy. The maximum length is 63 characters. To display the list of existing policies, enter: <pre>edit ?</pre>	No default.
allow-hosts "<hosts_name>"	Enter the name of a protected hosts group to allow or reject connections based upon whether the <code>Host :</code> field in the HTTP header is empty or does or does not match the protected hosts group. The maximum length is 63 characters. To display the list of existing groups, enter: <pre>edit ?</pre> If you do not select a protected hosts group, FortiWeb accepts or blocks requests based upon other criteria in the policy or protection profile, but regardless of the <code>Host :</code> field in the HTTP header. Note: Unlike HTTP 1.1, HTTP 1.0 does not require the <code>Host :</code> field. The FortiWeb appliance does not block HTTP 1.0 requests because they do not have this field, regardless of whether or not you have selected a protected hosts group.	No default.
block-port <port_int>	Enter the number of the physical network interface port that FortiWeb uses to send TCP <code>RST</code> (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 <code>RST</code> from <code>port1</code>, enter: <pre>set block-port port1</pre> Available only when the operating mode is Offline Protection.	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 block list rules, and allow list rules.	No default.

Variable	Description	Default
	For example, when enabled, an HTTP request involving <code>http://www.Example.com/</code> would not match protection profile features that specify <code>http://www.example.com</code> (difference highlighted in bold).	
certificate "<certificate_name>"	Enter the name of the certificate that FortiWeb uses to encrypt or decrypt SSL-secured connections. The maximum length is 63 characters. To display the list of existing certificates, enter: <pre>edit ?</pre> If sni {enable disable} on page 166 is <code>enable</code>, FortiWeb uses a Server Name Indication (SNI) configuration instead of or in addition to this server certificate. For details, see sni {enable disable} on page 166. This option is used only if HTTPS-service "<service_name>" on page 162 is configured.	No default.
chunk-encoding {enable disable}	Enable to encode the response packets. This option applies only to the packets sent from FortiWeb to the clients. After FortiWeb receives a packet from the back-end server, it will decode the packet first (if it's encoded), scan it against the security rules, and then send the encoded packet (if the <code>chunk-encoding</code> is set to <code>enable</code>) to the clients. However, if no web protection profile is selected in the server policy, the chunk-encoding option won't take effect. In this case, FortiWeb forwards whatever it receives from the back-end server to the clients without performing the encoding operation. Please note in previous releases we use <code>chunk-decode-enabled</code>. If you configured <code>chunk-decode-enabled enable</code> previously, then in this release it will automatically be switched to <code>chunk-encoding disable</code>, and vice versa.	disable

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 <code>X-Client-Cert</code>: 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
client-certificate-forwarding-cert-header "<header_str>"	Enter a custom certificate header that will include the Base64 certificate of the X.509 personal certificate presented by the client during the SSL/TLS handshake when it forwards the traffic to the protected web server.	x-client-cert
client-certificate-forwarding-sub-header "<header_str>"	Enter a custom subject header that will include the subject of the X.509 personal certificate presented by the client during the SSL/TLS handshake when it forwards the traffic to the protected web server.	x-client-dn
client-real-ip {enable disable}	Enter <code>enable</code> 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
client-real-ip-random-port {enable disable}	Enable to use a random port for the client real IP. It recommend to enable random port if the following configurations are set, otherwise it may lead to traffic disruption: • deployment-mode is HTTP-content-routing, and;	disable

Variable	Description	Default
	• prefer-current-session is disabled, and; • client-real-ip is enabled, and; • real-ip-addr is not specified.	
real-ip-addr <real-ip-addr_str>	Specify an IP address or address range to directly connect to the back-end server.	No default.
client-timeout <seconds_int>	Enter the amount of time (in seconds) that FortiWeb will keep open a connection with an idle client that isn't sending data. The valid range is 1–1200. A value of 0 means that there is no timeout. Please note that this option doesn't work for HTTP/2 traffic.	0
comment "<comment_str>"	Enter 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.
data-capture-port <port_int>	Enter 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.	
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. • <code>server-pool</code>—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>" on page 165. This option is available only if the operating mode is Reverse Proxy mode. • <code>HTTP-content-routing</code>—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	No default.

Variable	Description	Default
	Reverse Proxy mode. • <code>offline-detection</code> — Allows connections to pass through the FortiWeb appliance and applies an Offline Protection profile. Also configure <code>server-pool "<server-pool_name>"</code> on page 165. This is the only option available if operating mode is Offline Protection. • <code>transparent-servers</code>—Allows connections to pass through the FortiWeb appliance and applies a protection profile. Also configure <code>server-pool "<server-pool_name>"</code> on page 165. This is the only option available when the operating mode is either True Transparent Proxy or Transparent Inspection. • <code>wccp-servers</code>—FortiWeb is a Web Cache Communication Protocol (WCCP) client that receives traffic from a FortiGate configured as a WCCP server. Also configure <code>server-pool "<server-pool_name>"</code> on page 165. This is the only option available when the operation mode is WCCP.	
<code>ftp-protection-profile <profile_name></code>	Enter the FTP security profile to apply to connections that this policy monitors. If you haven't created a profile yet, see waf ftp-protection-profile or instructions about creating one.	No default.
<code>half-open-threshold <packets_int></code>	Enter the maximum number of TCP <code>SYN</code> 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 10–10,000. Available only when the operating mode is Reverse Proxy or True Transparent Proxy and <code>syncookie {enable disable}</code> on page 172 is enabled.	8192

Variable	Description	Default
hpkp-header "<hpkp_name>"	Select an HPKP profile, if any, to use to verify certificates when clients attempt to access a server. HPKP prevents attackers from carrying out <i>Man in the Middle</i> (MITM) attacks with forged certificates. Available only when the operating mode is Reverse Proxy.	No default.
hsts-header {enable disable}	Enable to combat MITM attacks on HTTP by injecting the RFC 6797 (http://tools.ietf.org/html/rfc6797) strict transport security header into the reply, such as: <pre>Strict-Transport-Security: max-age=31536000; includeSubDomains;Preload</pre> 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>" on page 162 is configured.	disable
hsts-max-age <timeout_int>	Enter the time to live in seconds for the HSTS header. Available only if hsts-header {enable disable} on page 159 is enabled. The valid range is 3,600–31,536,000.	7776000

Variable	Description	Default
HTTP2 {enable disable}	FortiWeb's HTTP/2 security inspection is only supported for Reverse Proxy mode and True Transparent Proxy mode. This option enables FortiWeb operating in Reverse Proxy mode (see opmode {offline-protection reverse-proxy transparent transparent-inspection wccp} on page 374) to negotiate HTTP/2 with clients via SSL ALPN (Application-Layer Protocol Negotiation) during the SSL handshake if the client's browser supports HTTP/2 protocol. With the HTTP/2 being enabled, FortiWeb can recognize HTTP/2 traffic and apply the security services to it. To enable HTTP/2 communication between the FortiWeb and back-end web servers for HTTP/2 inspections in Reverse Proxy mode, see HTTP2 {enable disable} on page 193. Available only when <code>opmode</code> is set to <code>reverse-proxy</code>, <code>deployment-mode {server-pool HTTP-content-routing offline-protection transparent-servers wccp-servers}</code> on page 157 is set to <code>server-pool</code> and <code>HTTPS-service "<service_name>"</code> on page 162 is set correctly. FortiWeb supports HTTP/2 only for HTTPS connections and HTTP Content Routing is not supported for HTTP/2. When <code>opmode</code> is set to <code>transparent</code> and <code>deployment-mode</code> is set to <code>transparent-servers</code>, this is not available. It only requires HTTP2 {enable disable} on page 193 to enable the HTTP/2 security inspections in True Transparent Proxy mode; this option here is not required. For more details about HTTP/2 support, see the FortiWeb Administration Guide: http://docs.fortinet.com/fortiweb/admin-guides	disable

Variable	Description	Default
http2-window-size <int>	Enter the window size (determining the amount of data in bytes that FortiWeb is willing to receive at any given time) for HTTP/2 connections between FortiWeb and the client. The valid range is 65,535-2,147,483,647 bytes.	65,535
HTTP-header-timeout <seconds_int>	Enter the amount of time (in seconds) that FortiWeb will wait for the whole HTTP request header after a client sets up a TCP connection. The valid range is 0–1200. A value of 0 means that there is no timeout.	0
http-parse-max-size <integer>	Enter the maximum size for HTTP parser to check headers and parameters. The valid range is 524288-2097152.	524288
HTTP-pipeline {enable disable}	Specify 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
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).	disable

Variable	Description	Default
	Available only when the operation mode is Reverse Proxy.	
redirect-naked-domain {enable disable}	Enable to redirect naked domain requests to "www" domain requests. This option is available only in Reverse Proxy mode.	disable
HTTPS-service "<service_name>"	Enter the custom or predefined service that defines the port number on which the virtual server receives HTTPS traffic. The maximum length is 63 characters. To display the list of existing services, enter: 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.
proxy-protocol {enable disable}	Enable this option when proxy servers or load balancers are installed before FortiWeb, for example, when a load balancer with proxy protocol enabled is deployed before FortiWeb-VM on AWS. When Proxy Protocol is enabled, FortiWeb can receive client connection information in the proxy protocol package passed through proxy servers and load balancers.	disable
use-proxy-protocol-addr {enable disable}	Enable to use the source address of the proxy protocol in server policy. If disabled, the source address of the connection will be used.	enable
replacemsg <replacemsg_name>	Select the replacement message to apply to the policy.	No default.
intermediate-certificate-group "<CA-group_name>"	Enter 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 63 characters. To display the list of existing groups, enter: edit ?	No default.

Variable	Description	Default
	Available only if HTTPS-service "<service_name>" on page 162 is configured.	
internal-cookie-HTTPOnly {enable disable}	Enable to assign an <code>HTTPOnly</code> flag to internal cookies. This feature is independent of the Cookie Security policy, if any, that you have in use.	enable
internal-cookie-secure {enable disable}	Enable to assign a <code>secure</code> flag to internal cookies . This flag can only be assigned if the connection is over SSL. This feature is independent of the Cookie Security policy, if any, that you have in use.	disable
internal-cookie-samesite {enable disable}	Enable to assign a <code>SameSite</code> flag to internal cookies. This feature is independent of the Cookie Security policy, if any, that you have in use. If enabled, it applies to User Tracking, Anomaly Detection, Site Publish, and Client Management.	disable
internal-cookie-samesite-value {strict lax none}	- strict: any request from the third parties will not carry such cookies; - lax: any request from the third parties will not carry such cookies except for GET requests that navigate to the destination URL. - none: set the value as none if a cookie is required to be sent by cross origin.	lax
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. Disable to allow FortiWeb to perform attack deny/redirect actions as defined by the server protection rules.	disable

Variable	Description	Default
<code>noparse {enable disable}</code>	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 "debug application HTTP" on page 1 and debug flow trace on page 759. 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} on page 62.	<code>disable</code>
<code>prefer-current-session {enable disable}</code>	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 {server-pool HTTP-content-routing offline-protection transparent-servers wccp-servers} on page 157 is <code>HTTP-content-routing</code>.	<code>disable</code>
<code>protocol {HTTP FTP ADFSPIP}</code>	Select one of the following: <code>HTTP</code>—Specifies that the server policy governs HTTP traffic. Specific options for configuring an HTTP server policy become available. <code>FTP</code>—Specifies that the server policy governs FTP traffic. Specific options for configuring an FTP server policy become available. <code>ADFSPIP</code>—Specifies that the server policy governs AD FS traffic. Specific options for configuring an AD FS server policy become available.	<code>HTTP</code>

Variable	Description	Default
server-pool "<server-pool_name>"	Enter the name of the server pool whose members receive the connections. To display the list of existing servers, enter: <pre>edit ?</pre> This field is applicable only if deployment-mode {server-pool HTTP-content-routing offline-protection transparent-servers wccp-servers} on page 157 is <code>server-pool</code>, <code>offline-protection</code> or <code>transparent-servers</code>. 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.
service "<service_name>"	Enter the custom or predefined service that defines the port number on which the virtual server receives HTTP traffic. The maximum length is 63 characters. To display the list of existing services, enter: <pre>edit ?</pre> Available only when the operating mode is Reverse Proxy.	No default.
sessioncookie-enforce {enable disable}	<code>enable</code>—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. <code>disable</code>—When FortiWeb maintains session persistence using cookies, it tracks or inserts the cookie for the first transaction of a session	disable

Variable	Description	Default
	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 details about configuring session persistence, see server-policy persistence-policy on page 146.	
sni {enable disable}	Enable to use a Server Name Indication (SNI) configuration instead of or in addition to the server certificate specified by <code>certificate <certificate_name></code>. 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. For details, see system certificate sni on page 264. If you specify both a SNI configuration and a certificate, FortiWeb uses the certificate specified by <code>certificate "<certificate_name>"</code> on page 155 when the requested domain does not match a value in the SNI configuration. If you enable <code>sni-strict {enable disable}</code> on page 167, FortiWeb always ignores the value of <code>certificate "<certificate_name>"</code> on page 155. Available only if <code>HTTPS-service "<service_name>"</code> on page 162 is configured.	disable
sni-certificate "<sni_name>"	Enter 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 <code>certificate "<certificate_name>"</code> on page 155 instead.	No default.

Variable	Description	Default
	Available only if HTTPS-service "<service_name>" on page 162 is configured.	
sni-strict {enable disable}	Select to configure FortiWeb to ignore the value of certificate "<certificate_name>" on page 155 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
certificate-type {enable disable}	Enable allow FortiWeb to automatically retrieve CA certificates from Let's Encrypt.	disable
lets-certificate <name>	Select the Letsencrypt certificate you have created. See system certificate letsencrypt .	No default.
ssl {enable disable}	Enable so that connections between clients and FortiWeb use SSL/TLS. Enabling <code>ssl</code> will allow you to configure additional SSL options and settings, including specifying supported SSL protocols and uploading certificates.	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 <code>ssl-custom-cipher</code> . This is not allowed to set to <code>custom</code> if <code>HTTP2</code> is set to <code>enable</code> . For details, see the <i>FortiWeb Administration Guide</i> : http://docs.fortinet.com/fortiweb/admin-guides Available only if HTTPS-service "<service_name>" on page 162 is configured.	medium
ssl-client-verify "<verifier_name>"	Enter 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.	No default.

Variable	Description	Default
	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 system certificate verify on page 269) • Be signed by a certificate authority (CA) whose certificate you have imported into the FortiWeb appliance; 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>" on page 162) • Contain a <code>CA</code> field whose value matches the CA certificate • Contain an <code>Issuer</code> field whose value matches the <code>Subject</code> field in the CA certificate Personal certificates, sometimes also called user certificates, establish the identity of the person connecting to the website. You can require that clients present a certificate alternatively or in addition to HTTP authentication. For details, see the <i>FortiWeb Administration Guide</i>: http://docs.fortinet.com/fortiweb/admin-guides The maximum length is 63 characters. To display the list of existing verifiers, type: <pre>edit ?</pre> This option is used only if HTTPS-service "<service_name>" on page 162 is configured. The client must support TLS 1.0, TLS 1.1, or TLS 1.2.	
ssl-custom-cipher {<cipher_1> <cipher2> <cipher3> ...}	Specify one or more cipher suites that FortiWeb allows.	ECDHE- ECDSA- AES256-GCM- SHA384

Variable	Description	Default
	Separate the name of each cipher with a space. To remove from or add to the list of ciphers, retype the entire list.	ECDHE-RSA-AES256-GCM-SHA384
	Valid values are:	ECDHE-
	ECDHE-ECDSA-AES256-GCM-SHA384	ECDSA-
	ECDHE-RSA-AES256-GCM-SHA384	CHACHA20-
	DHE-DSS-AES256-GCM-SHA384	POLY1305
	DHE-RSA-AES256-GCM-SHA384	ECDHE-RSA-
	ECDHE-ECDSA-CHACHA20-POLY1305	CHACHA20-
	ECDHE-RSA-CHACHA20-POLY1305	POLY1305
	DHE-RSA-CHACHA20-POLY1305	ECDHE-
	ECDHE-ECDSA-AES256-CCM8	ECDSA-
	ECDHE-ECDSA-AES256-CCM	AES128-GCM-
	DHE-RSA-AES256-CCM8	SHA256
	DHE-RSA-AES256-CCM	ECDHE-RSA-
	ECDHE-ECDSA-AES128-GCM-SHA256	AES128-GCM-
	ECDHE-RSA-AES128-GCM-SHA256	SHA256
	DHE-DSS-AES128-GCM-SHA256	ECDHE-
	DHE-RSA-AES128-GCM-SHA256	ECDSA-
	ECDHE-ECDSA-AES128-CCM8	AES256-
	ECDHE-ECDSA-AES128-CCM	SHA384
	DHE-RSA-AES128-CCM8	ECDHE-RSA-
	DHE-RSA-AES128-CCM	AES256-
	ECDHE-ECDSA-AES256-SHA384	SHA384
	ECDHE-RSA-AES256-SHA384	ECDHE-
	DHE-RSA-AES256-SHA256	ECDSA-
	DHE-DSS-AES256-SHA256	AES128-
	ECDHE-ECDSA-CAMELLIA256-SHA384	SHA256
	ECDHE-RSA-CAMELLIA256-SHA384	ECDHE-RSA-
	DHE-RSA-CAMELLIA256-SHA256	AES128-
	DHE-DSS-CAMELLIA256-SHA256	SHA256
	ECDHE-ECDSA-AES128-SHA256	ECDHE-
	ECDHE-RSA-AES128-SHA256	ECDSA-
	DHE-RSA-AES128-SHA256	AES256-SHA
	DHE-DSS-AES128-SHA256	ECDHE-RSA-
	ECDHE-ECDSA-CAMELLIA128-SHA256	AES256-SHA
	ECDHE-RSA-CAMELLIA128-SHA256	SHA256
	DHE-RSA-CAMELLIA128-SHA256	ECDHE-
	DHE-DSS-CAMELLIA128-SHA256	ECDSA-
	ECDHE-ECDSA-AES256-SHA	AES128-SHA

Variable	Description	Default
	ECDHE-RSA-AES256-SHA	AES128-GCM-SHA256
	DHE-RSA-AES256-SHA	
	DHE-DSS-AES256-SHA	AES256-SHA256
	DHE-RSA-CAMELLIA256-SHA	
	DHE-DSS-CAMELLIA256-SHA	AES128-SHA256
	ECDHE-ECDSA-AES128-SHA	
	ECDHE-RSA-AES128-SHA	
	DHE-RSA-AES128-SHA	
	DHE-DSS-AES128-SHA	
	DHE-RSA-CAMELLIA128-SHA	
	DHE-DSS-CAMELLIA128-SHA	
	AES256-GCM-SHA384	
	AES256-CCM8	
	AES256-CCM	
	AES128-GCM-SHA256	
	AES128-CCM8	
	AES128-CCM	
	AES256-SHA256	
	CAMELLIA256-SHA256	
	AES128-SHA256	
	CAMELLIA128-SHA256	
	AES256-SHA	
	CAMELLIA256-SHA	
	AES128-SHA	
	CAMELLIA128-SHA	
	DHE-RSA-SEED-SHA	
	ECDHE_RSA_DES_CBC3_SHA	
	DES_CBC3_SHA	
tls13-custom-cipher {<cipher_1> <cipher2> <cipher3> ...}	Specify one or more TLS 1.3 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: TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256 TLS_AES_128_CCM_SHA256 TLS_AES_128_CCM_8_SHA256	TLS_AES_256_GCM_SHA384

Variable	Description	Default
<code>rfc7919-comply {enable disable}</code>	Enable to apply cipher suites that comply with RFC-9719.	disable
<code>supported-groups {X25519 prime256v1 secp384r1 secp521r1 brainpoolP256r1 brainpoolP384r1 brainpoolP512r1 ffdhe2048 ffdhe3072 ffdhe4096 ffdhe6144 ffdhe8192}</code>	Select the RFC-9719 ciphers to be supported. The Supported Group is Elliptic Curve Parameters, while SSL/TLS negotiation could choose different Elliptic Curve algorithms, so please make sure to choose the corresponding ciphers in <code>ssl-custom-cipher</code>. - At least one FFDHE group should be selected. - At least one DHE cipher should be added. Due to design limitation, you need to select <code>custom</code> in <code>ssl-cipher {medium high custom}</code> and make sure to include at least one DHE cipher in the selected list. Using <code>High</code> or <code>Medium</code> together with RFC-9719 will lead to unexpected error. We will fix it in the future release. The system will return error if any of the above two conditions is not met. Please note RFC7919 does not comply with TLS 1.3, so if you have only enabled <code>tls-v13</code>, then RFC7919 will not take effect even if it's enabled. To apply both TLS 1.3 and RFC7919, it's recommended to enable a non-TLS 1.3 protocol, then select at least one DHE cipher.	No default
<code>ssl-noreg {enable disable}</code>	Specify 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>" on page 162 is configured.	enable
<code>ssl-session-timeout <ssl-session-timeout_int></code>	When FortiWeb is configured as an SSL server, you can set SSL session timeout intervals via the CLI. This is available only in Reverse Proxy and True Transparent	No default.

Variable	Description	Default
	Proxy modes.	
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 system snmp community on page 375.	No default.
syncookie {enable disable}	Enable to detect TCP <code>SYN</code> flood attacks. For details, see the <i>FortiWeb Administration Guide</i>: http://docs.fortinet.com/fortiweb/admin-guides Available only when the operating mode is Reverse Proxy or True Transparent Proxy.	disable
tcp-recv-timeout <seconds_int>	Enter the amount of time (in seconds) that FortiWeb will wait for a client to send a request after the client sets up a TCP connection. The valid range is 0–300. A value of 0 means that there is no timeout.	0
tls-v10 {enable disable}	Specifies whether clients can connect securely to FortiWeb using the TLS 1.0 cryptographic protocol. This must be set to <code>disable</code> if HTTP2 {enable disable} on page 160 is set to <code>enable</code>. Available only if HTTPS-service "<service_name>" on page 162 is configured.	enable
tls-v11 {enable disable}	Specifies whether clients can connect securely to FortiWeb using the TLS 1.1 cryptographic protocol. This must be set to <code>disable</code> if HTTP2 {enable disable} on page 160 is set to <code>enable</code>. Available only if HTTPS-service "<service_name>" on page 162 is configured.	enable

Variable	Description	Default
<code>tls-v12 {enable disable}</code>	Specifies whether clients can connect securely to FortiWeb using the TLS 1.2 cryptographic protocol. Available only if HTTPS-service "<service_name>" on page 162 is configured.	<code>enable</code>
<code>tls-v13 {enable disable}</code>	Specifies whether clients can connect securely to FortiWeb using the TLS 1.3 cryptographic protocol. Available only if HTTPS-service "<service_name>" on page 162 is configured.	<code>disable</code>
<code>urllib {enable disable}</code>	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>" on page 162 is configured.	<code>disable</code>
<code>urllib-group "<urllib-group_name>"</code>	Enter 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 details about creating a group, see system certificate urllib on page 268 .	No default.
<code>urllib-hlen <len_int></code>	Specify 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. The valid range is 16–10240.	No default.
<code>vserver "<vserver_name>"</code>	Enter 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 63 characters.	No default.

Variable	Description	Default
	To display the list of existing virtual servers, enter: <pre>edit ?</pre> Available only if the operating mode is Reverse Proxy.	
v-zone "<bridge_name>"	Enter 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, enter: <pre>edit ?</pre> Available only if the operating mode is True Transparent Proxy or Transparent Inspection.	No 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 <code>Key Usage</code> field that contains <code>Digital Signature</code> or have a <code>ExtendedKeyUsage</code> or <code>EnhancedKeyUsage</code> field whose value contains <code>Client Authentication</code> 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.	
<entry_index>	Enter the index number of the individual	No default.

Variable	Description	Default
	entry in the table.	
content-routing-policy-name "<content-routing_name>"	Enter the name of a HTTP content routing policy that this server policy uses. To display the list of existing error pages, enter: edit ?	No default.
is-default {yes no}	Enter 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.
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
implicit_ssl {enable disable}	Enable so that FortiWeb will communicate with the pool member using implicit SSL.	No default.
ssl-quiet-shutdown {enable disable}	For HTTPS connection, when disabled, FortiWeb sends ssl alert message to the client or server pool first, and then FIN. When enabled, FortiWeb directly sends FIN message instead of sending ssl alert message.	disable
traffic-mirror {enable disable}	Enable to send traffic to third party IPS/IDS devices through network interfaces for traffic monitoring. Available only when protocol {HTTP FTP ADFSPIP} on page 164 is HTTP.	disable
traffic-mirror-profile <traffic-mirror-profile_str>	Select the mirror policy created.	No default.
traffic-mirror-type {client-side server-side both-side}	Select the traffic mirror type. For True Transparent Proxy mode, only Client Side type is available, which only allows traffic from client side to be sent to IPS/IDS devices. For Reverse Proxy mode, you can select Client Side, Server Side, or Client and Server.	No default.
multi-certificate {enable disable}	Enable to allow FortiWeb to use multiple local certificates.	disable
adfs-certificate-service <adfs-certificate-	Configure this option if the AD FS server	No default.

Variable	Description	Default
service_str}	requires client certificate for authentication. Select the pre-defined service TLSCIENTPORT if FortiWeb uses service port 49443 to listen the certification authentication requests.	
adfs-certificate-ssl-client-verify <adfs-certificate-ssl-client-verify_str>}	Select the certificate validation rule you have created.	No default.
certificate-group <certificate-group_str>}	Select the multi-certificate file you have created.	No default.
acceleration-policy <acceleration-policy_str>	Select the acceleration policy you have created.	No default.
web-cache {enable disable}	Enable to create a web cache policy to allow FortiWeb to cache responses from your servers.	disable
real-ip-addr <real-ip-addr_str>	Specify an IP address or address range to directly connect to the back-end server.	No default.
retry-on {enable disable}	Enable to configure whether to retry a failed TCP connection or HTTP request in Reverse Proxy mode. A TCP connection failure retry can help when pserver is unreachable unexpectedly, FortiWeb will reconnect the single server or switch to the other server when more than one pserver is available in the server pool. An HTTP layer retry can help when pserver can be connected but it returns certain failure response codes, such as 404, 408, 500, 501, 502, 503, and 504. FortiWeb will reconnect the single server or switch to the other server when more than one pserver is available in the server pool.	disable
retry-on-cache-size <retry-on-cache-size_int>	Enter a cache size limit for the HTTP request packet. HTTP failure retry will take effect once the request packet size is smaller than this defined size. TCP connection failure retry will take effect once the HTTP request packet	512

Variable	Description	Default
	size in TCP connection is smaller than this defined size.	
retry-on-connect-failure {enable disable}	Enable to configure the retry times in case of any TCP connection failure.	disable
retry-times-on-connect-failure <retry-times-on-connect-failure_int>	Enter the retry times when FortiWeb reconnects the single server or switch to the other pserver. The valid range is 1-5.	3
retry-on-HTTP-layer {enable disable}	Enable to configure the retry times and failure response code in case of any HTTP connection failure. Only GET and HEAD methods are supported now.	enable
retry-times-on-HTTP-layer <retry-times-on-HTTP-layer_int>	Enter the retry times when FortiWeb reconnects the single server or switch to the other pserver. The valid range is 1-5.	3
retry-on-HTTP-response-codes {404 408 500 501 502 503 504}	Select the failure return code when pserver can be connected to determine enabling HTTP failure retry.	All values
replacemsg-on-connect-failure {disable enable}	If this option is enabled, when the health check is disabled and the back-end server is not responsive, FortiWeb will send the 503 error code to the client. When enabled, you should also configure <code>tcp-conn-timeout</code> to specify the timeout value.	disable
tcp-conn-timeout <integer>	When the health check is disabled and the back-end server is not responsive, FortiWeb will wait for the specified time until it sends the 503 error code. It's recommended to set a value smaller than 20 (seconds). This is to avoid too many times of retry being accumulated during the waiting time, which may cause the connection to be closed before FortiWeb has the chance to send the error code. This option is at the server policy level. You can also set the <code>tcp-usertimeout</code> under <code>system network-option</code> which affects all server policies on FortiWeb appliance. If the timeout is configured both at the policy and the appliance level, FortiWeb will take the value whichever is smaller.	120

Variable	Description	Default
	Sometimes when there is a third device, such as a gateway, deployed between FortiWeb and the back-end server, FortiWeb will directly get the status code from the third device instead of waiting along the timeout period. The valid range for this option is 0-600 (seconds). 0 means FortiWeb will send 503 error code as soon as it detects the back-end server is not responsive.	
tlog {enable disable}	Enable to log traffic events such as HTTP requests and responses, and the expiration of HTTP sessions. To avoid unnecessary resource consumption, the system will not generate traffic log for all server policies unless specified. After enabling this option, you also need to enable the traffic log setting in Log&Report. - If traffic log is disabled in Log&Report, the system won't generate traffic log even if you have enabled it in Server Policy. - If traffic log is: - Enabled in Log&Report, - Enabled in server policy A, - Disabled in server policy B, then the system will only generate traffic log for server policy A. Tip: Because resources for this feature increase as your traffic increases, if you do not need traffic data, disable this feature to improve performance and improve hardware life.	disable
ldap-health {enable disable}	Enable LDAP server's health check.	disable
ztna-profile <string>	Specify the ZTNA (Zero Trust Network Access) profile. For more information, see Configuring a ZTNA Profile.	no default
reply-100-continue {enable disable}	When disabled, the clients should wait for FortiWeb to forward the 100-	enable

Variable	Description	Default
	<code>continue</code> response sent by server. When enabled, FortiWeb will not wait for the server's <code>100-continue</code> response. Instead it directly reply <code>100-continue</code> header to clients to reduce delay. Note:FortiWeb only supports HTTP/1.1, so the <code>100-continue</code> response sent by FortiWeb will be HTTP/1.1 <code>100-continue</code>.	
<code>forward-expect-100-continue {enable disable}</code>	- When disabled, FortiWeb will remove the <code>Expect: 100-continue</code> header from the request packets then forward them to servers. - When enabled, the <code>Expect: 100-continue</code> will be forwarded to server. It's recommended to set <code>reply-100-continue</code> as enabled and <code>forward-expect-100-continue</code> as disabled, so that FortiWeb can directly reply <code>100-continue</code> header to reduce delay, then remove the <code>Expect: 100-continue</code> header from request packets to avoid unnecessary header being forwarded.	disable
<code>transaction-based-persistence {enable disable}</code>	Enable this option so that persistence information will be checked by each transaction, rather than the connection itself. Transactions with distinct persistence information will be directed to different back-end servers to ensure optimal load balancing. This functionality is beneficial in scenario such as FortiWeb is deployed behind Cloudflare which forwards different customer's traffic within the same connection.	disable
<code>no-ssl-error-log {enable disable}</code>	Enable to stop FortiWeb from logging SSL errors for this server policy. This setting is useful when you use high-level security settings, which generate a high volume of these types of errors.	disable

Variable	Description	Default
	Instead of setting the <code>no-ssl-error</code> value individually for each server policy, you can configure a global value through <code>config log attack-log</code> so that all server policies adhere to it. Please note that if there is a discrepancy between the values set individually for server policies and the global value in <code>config log attack-log</code> , the global value takes precedence.	
<code>server-latency-alert <integer></code>	Sets the server latency threshold in milliseconds (range: 0–65000). If the average latency across the last 15 connections exceeds this threshold, FortiWeb generates an event log once per minute. A value of 0 disables this check. Latency includes server RTT and application response time, and is updated only when new traffic is processed. To avoid redundant logs, FortiWeb logs an event only if the latency was updated and still exceeds the threshold since the last check.	No default.
<code>url-normalize-backslash {enable disable}</code>	When enabled, FortiWeb can handle backslash (\) as slash (/) when parsing URLs, for instance, "yoursite\WEB-INF\web.xml" can be handled as "yoursite/WEB-INF/web.xml".	disable
<code>payload-based-content-type {enable disable}</code>	By default, the payload body is scanned for attacks under any condition, regardless of its content type. However, conducting a payload body scan for specific content types may be unnecessary and could potentially result in numerous false positives. To avoid such situations, you can enable <code>payload-based-content-type</code> to skip payload body scan for most of the content types except for the following high-risk ones. Meanwhile, if the system cannot determine the content type of a payload, it will be deemed high-risk and subject to a security scan. • multipart/related • application/soap+xml	disable

Variable	Description	Default
	• text/xml, application/xml, application/vnd.syncml+xml, application/vnd.ms-sync.wbxml • multipart/form-data (boundary is required) • text/html • application/x-www-form-urlencoded • text/plain • application/x-amf • text/css • application/x-javascript • multipart/x-mixed-replace • application/javascript • application/rpc • text/javascript • application/rss+xml • application/xhtml+xml • message/HTTP • application/json, text/json • all other application/...xml... • application/octet-stream • application/mapi-http	
tag <tag_name>	Enter the tags you want to attach to this server policy. This helps in labeling server policy for future usage such as sorting, filtering and acknowledging policies. It's created by config system object-tagging.	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

- [server-policy allow-hosts on page 106](#)
- [system certificate local on page 258](#)
- [system certificate ocsp-stapling on page 262](#)
- [server-policy HTTP-content-routing-policy on page 118](#)
- [server-policy server-pool on page 182](#)
- [server-policy service custom on page 207](#)
- [server-policy vserver on page 215](#)
- [system snmp community on page 375](#)
- [system settings on page 372](#)
- [system v-zone on page 388](#)
- [waf web-protection-profile inline-protection on page 696](#)
- [waf web-protection-profile offline-protection on page 706](#)
- ["debug application dssl" on page 1](#)
- ["debug application HTTP" on page 1](#)
- ["debug application ssl" on page 1](#)
- ["debug application ustack" on page 1](#)
- [debug flow filter on page 756](#)
- [policy on page 797](#)

server-policy server-pool

Use this command to configure an HTTP, FTP, or AD FS server pool.

Server pools define a group of one or more physical or domain servers (web servers) that FortiWeb distributes connections among, or where the connections pass through to, depending on the operation mode. Reverse Proxy mode actively distributes connections; Offline Protection and either of the transparent modes do not actively distribute connections.

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.

For details, see [server-policy policy on page 150](#) and [server-policy HTTP-content-routing-policy on page 118](#).

To determine which type of server policy to create, configure [protocol {HTTP | FTP | ADFSPIP} on page 187](#). If you're planning to configure an FTP server policy, you'll need to confirm that [system feature-visibility on page 288](#) is enabled. For details, see [system feature-visibility on page 288](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For details, see [Permissions on page 46](#).

Syntax

```

config server-policy server-pool
edit "<server-pool_name>"
    set comment "<comment_str>"
    set health "<health-check_name>"
    set HTTP-reuse {aggressive | always | never | safe}
    set lb-algo {least-connections | round-robin | weighted-round-robin | uri-hash |
        full-uri-hash | host-hash | host-domain-hash | src-ip-hash | least-response-
        time | probabilistic-weighted-least-response-time}
    set persistence "<persistence-policy_name>"
    set protocol {HTTP | FTP | ADFSPIP}
    set reuse-conn-idle-time <int>
    set reuse-conn-max-count <int>
    set reuse-conn-max-request <int>
    set reuse-conn-total-time <int>
    set server-balance {enable | disable}
    set server-pool-id
    set type {offline-protection | reverse-proxy | transparent-servers-for-ti |
        transparent-servers-for-tp | transparent-servers-for-wccp}
    set proxy-protocol {enable | disable}
    set proxy-protocol-version {v1 | v2}
    set adfs-server-name <adfs-server-name_str>
config pserver-list
edit <entry_index>
    set analyzer-policy "<fortianalyzer-policy_name>"
    set backup-server {enable | disable}
    set certificate "<certificate_name>"
    set certificate-verify "<verifier_name>"
    set client-certificate "<client-certificate_name>"
    set client-certificate-forwarding {enable | disable}
    set client-certificate-forwarding-cert-header "<header_str>"
    set client-certificate-forwarding-sub-header "<header_str>"
    set client-certificate-proxy {enable | disable}
    set client-certificate-proxy-sign-ca <sign_ca>
    set conn-limit <conn-limit_int>
    set domain "<server_fqdn>"
    set health-check-inherit {enable | disable}
    set hlck-domain <hlck-domain_str>
    set hpkp-header "<hpkp_name>"
    set hsts-header {enable | disable}
    set hsts-max-age <timeout_int>
    set HTTP2 {enable | disable}
    set http2-window-size <int>
    set implicit_ssl {enable | disable}
    set intermediate-certificate-group "<CA-group_name>"
    set ip {"address_ipv4" | "address_ipv6"}
    set port <port_int>
    set server-certificate-verify {enable | disable}
    set server-certificate-verify-action {alert | alert_deny | redirect}
    set server-certificate-verify-policy "<policy_name>"
    set recover <recover_int>
    set server-side-sni {enable | disable}
    set server-type {physical | domain | sdn-connector}
    set sdn-addr-type {private | public | all}
    set sdn {aws | azure}
    set filter <string>

```

```

set session-id-reuse {enable | disable}
set session-ticket-reuse {enable | disable}
set sni {enable | disable}
set sni-certificate "<sni_name>"
set sni-strict {enable | disable}
set certificate-type {enable | disable}
set lets-certificate <name>
set ssl {enable | disable}
set ssl-cipher {medium | high | custom}
set ssl-custom-cipher {<cipher_1> <cipher2> <cipher3> ...}
set tls13-custom-cipher on page 201
set rfc7919-comply {enable | disable}
set supported-groups {X25519 | prime256v1 | secp384r1 | secp521r1 |
    brainpoolP256r1 | brainpoolP384r1 | brainpoolP512r1 | ffdhe2048 |
    ffdhe3072 | ffdhe4096 | ffdhe6144 | ffdhe8192}
set ssl-noreg {enable | disable}
set ssl-quiet-shutdown {enable | disable}
set ssl-session-timeout <ssl-session-timeout_int> on page 206
set status {disable | enable | maintain}
set tls-v10 {enable | disable}
set tls-v11 {enable | disable}
set tls-v12 {enable | disable}
set tls-v13 {enable | disable} on page 204
set url-cert {enable | disable}
set urlcert-group "<urlcert-group_name>"
set urlcert-hlen <len_int>
set warm-rate <warm-rate_int>
set warm-up <warm-up_int>
set weight <weight_int>
set adfs-username <adfs-username_str>
set adfs-password <adfs-password_str>
set multi-certificate {enable | disable}
set certificate-group <certificate-group_str>
set enforce-trust-establishment {enable | disable}
next
end
next
end
end

```

Variable	Description	Default
"<server-pool_name>"	Enter the name of the server pool. The maximum length is 63 characters. To display the list of existing servers, enter: edit ?	No default.
comment "<comment_str>"	Enter 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.

Variable	Description	Default
health "<health-check_name>"	Enter the name of a server health check FortiWeb uses to determine the responsiveness of server pool members. The maximum length is 63 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 <code>disable</code> for <code>health-check-inherit</code> and the health check to use for health. To display the list of existing health checks, enter: <code>edit ?</code> Available only if <code>type {offline-protection reverse-proxy transparent-servers-for-ti transparent-servers-for-tp transparent-servers-for-wccp}</code> on page 189 is <code>reverse-proxy</code> and <code>server-balance {enable disable}</code> on page 188 is <code>enable</code>. 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 or an SNMP trap. For details, see system snmp community on page 375.	No default.
HTTP-reuse {aggressive always never safe}	Configure multiplexing so that FortiWeb uses a single connection to a server for requests from multiple clients. Enter one of these options: <code>aggressive</code>—The first request from a client can use a cached server connection only when the cached server connection has been used by more than one client. <code>always</code>—Client requests will use an available connection cached server connection. <code>never</code>—Disable multiplexing. <code>safe</code>—A client will establish a new connection for the first request, but will use an available cached server connection for subsequent requests. Note: This option is available only when the <code>protocol {HTTP FTP ADFSPIP}</code> on page 187 is <code>HTTP</code>.	never

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 least-response-time probabilistic-weighted-least-response-time}	Select the load-balancing algorithms that FortiWeb uses when it distributes new connections among server pool members. <code>least-connections</code>—Distributes new connections to the member with the fewest number of existing, fully-formed connections. <code>round-robin</code>—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. <code>weighted-round-robin</code>—Distributes new connections using the round robin method, except that members with a higher weight value receive a larger percentage of connections. <code>uri-hash</code>—Distributes new TCP connections using a hash algorithm based on the URI found in the HTTP header, excluding hostname. <code>full-uri-hash</code>—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. <code>host-hash</code>—Distributes new TCP connections using a hash algorithm based on the hostname in the HTTP Request header Host field. <code>host-domain-hash</code>—Distributes new TCP connections using a hash algorithm based on the domain name in the HTTP Request header Host field. <code>src-ip-hash</code>—Distributes new TCP connections using a hash algorithm based on the source IP address of the request. <code>least-response-time</code>—Distributes the incoming traffic to the server with the shortest average response time and the lowest number of connections, thus making the client connect to the most efficient back-end server. <code>probabilistic-weighted-least-response-time</code>—For the <code>least-response-time</code>, in extreme cases there might be a server consistently has relatively low response time compared to others, which causes most of traffic to be distributed to one server. As a solution to this case, <code>probabilistic-weighted-least-response-time</code> distributes traffic based on least response time as well as probabilities. The least response	round-robin

Variable	Description	Default
	time server is most likely to receive traffic, while the rest servers still have a chance to process some of the traffic. Note: When protocol {HTTP FTP ADFSPIP} on page 187 is set to <code>FTP</code>, only <code>round-robin</code>, <code>weighted-round-robin</code>, <code>least-connections</code>, and <code>src-ip-hash</code> are available. For hash-based methods, if you specify a value for <code>persistence</code>, 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 {offline-protection reverse-proxy transparent-servers-for-ti transparent-servers-for-tp transparent-servers-for-wccp} on page 189 is <code>reverse-proxy</code> and server-balance {enable disable} on page 188 is <code>enable</code>.	
<code>persistence "<persistence-policy_name>"</code>	Enter the name of the persistence policy that specifies a session persistence method and timeout to apply to the pool. For details, see server-policy persistence-policy on page 146. Note: This option is available only when the protocol {HTTP FTP ADFSPIP} on page 187 is <code>HTTP</code>.	No default.
<code>adfs-server-name <adfs-server-name_str></code>	Enter a name for the AD FS Server. It should be the federation service name. This option is mandatory if the AD FS Server needs to verify the server name in the SSL handshake. This is only available if the server pool type is ADFSPIP.	No default.
<code>protocol {HTTP FTP ADFSPIP}</code>	Select one of the following: <code>HTTP</code>—Specifies that the server pool governs HTTP traffic. Specific options for configuring an HTTP server pool become available. <code>FTP</code>—Specifies that the server pool governs FTP traffic. Specific options for configuring an FTP server pool become available. <code>ADFSPIP</code>—Specifies that the server pool governs ADFSPIP traffic. Specific options for configuring an ADFSPIP server pool become available.	HTTP

Variable	Description	Default
proxy-protocol {enable disable}	If the back-end server enables proxy protocol, you need to enable the Proxy Protocol option on FortiWeb so that the TCP SSL and HTTP traffic can successfully go through. The real IP address of the client will be included in the proxy protocol header. Available only if the type {offline-protection reverse-proxy transparent-servers-for-ti transparent-servers-for-tp transparent-servers-for-wccp} is Reverse Proxy, True Transparent Proxy, Offline Protection, or Transparent Inspection.	disable
proxy-protocol-version {v1 v2}	Select the proxy protocol version for the back-end server. Available only if the type {offline-protection reverse-proxy transparent-servers-for-ti transparent-servers-for-tp transparent-servers-for-wccp} is Reverse Proxy, or True Transparent Proxy.	v1
reuse-conn-idle-time <int>	Enter an idle time limit for a cached server connection. If a cached server connection remains idle for the set duration, it will be closed. The valid range is 1–1000.	10
reuse-conn-max-count <int>	Enter the maximum number of allowed cached server connections. If FortiWeb meets the set number, no more cached server connections will be established. The valid range is 1–1000 for each pserver. Note: The minimum number of cached connections depends on the number of CPU kernels of the FortiWeb platform. For example, a FortiWeb 4000E has 40 CPU kernels, so there are always at least 40 reusable connections for each pserver. In addition, the valid range is set for each pserver; if there are two pservers and you enter a value of 1000, there will be up to 2000 reusable connections.	100
reuse-conn-max-request <int>	Enter the maximum number of HTTP responses that the cached server connection may handle. If a cached server connection meets the set number, it will be closed. The valid range is 1–1000.	100
reuse-conn-total-time <int>	Enter the maximum time limit in which a cached server connection may be reused. If a cached server connection exists for longer than the set limit, it will be closed. The valid range is 1–1000.	100
server-balance {enable disable}	Specifies whether the pool contains a single server or multiple members.	disable

Variable	Description	Default
	If the value is <code>enabled</code>, 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 <code>type {offline-protection reverse-proxy transparent-servers-for-ti transparent-servers-for-tp transparent-servers-for-wccp}</code> on page 189 is <code>reverse-proxy</code>.	
<code>server-pool-id</code>	A 64-bit random integer assigned to each server policy. The <code>policy-id</code> is a unique identification number for each server policy. When administrative domains (ADOMs) are enabled, ADOMs can create unique server policies with policy names that are identical to other server policies created by different ADOMs, so the <code>policy-id</code> can easily differentiate between different policies created by different ADOMs that may share the same policy name.	No default.
<code>type {offline-protection reverse-proxy transparent-servers-for-ti transparent-servers-for-tp transparent-servers-for-wccp}</code>	Select the current operation mode of the appliance to display the corresponding pool options. For details, see <code>opmode {offline-protection reverse-proxy transparent transparent-inspection wccp}</code> on page 374. Note: This option is applicable only when the <code>protocol {HTTP FTP ADFSPIP}</code> on page 187 is <code>HTTP</code>.	<code>reverse-proxy</code>
<code><entry_index></code>	Enter the index number of the member entry within the server pool. The valid range is 1–9,223,372,036,854,775,807. For round robin-style load-balancing, the index number indicates the order in which FortiWeb distributes connections.	No default.
<code>backup-server {enable disable}</code>	Enter <code>enable</code> 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.	<code>disable</code>

Variable	Description	Default
certificate "<certificate_name>"	Enter the name of the certificate that FortiWeb uses to decrypt SSL-secured connections. Available only if ssl {enable disable} on page 199 is <code>enable</code>. The maximum length is 63 characters. To display the list of existing certificates, enter: <pre>edit ?</pre> Note: This option is available only when the protocol {HTTP FTP ADFSPIP} on page 187 is <code>HTTP</code>.	No default.
certificate-verify "<verifier_name>"	Enter 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 ssl {enable disable} on page 199 is <code>enable</code> 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 website. For details about how the client's certificate is verified, see ssl-client-verify "<verifier_name>" on page 167. You can require that clients present a certificate alternatively or in addition to HTTP authentication. For details, see waf HTTP-authen HTTP-authen-rule on page 529. Available only if ssl {enable disable} on page 199 is <code>transparent-servers-for-tp</code> and <code>ssl</code> is <code>enable</code>. For Reverse Proxy mode, configure this setting in the server policy instead. See ssl-client-verify "<verifier_name>" on page 167. The maximum length is 63 characters. To display the list of existing verifiers, enter: <pre>edit ?</pre> Note: The client must support TLS 1.0, TLS 1.1, or TLS 1.2. Note: This option is available only when the protocol {HTTP FTP ADFSPIP} on page 187 is <code>HTTP</code>.	No default.
client-certificate "<client-certificate_name>"	Enter 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.	<code>disable</code>

Variable	Description	Default
	Available only if <code>type {offline-protection reverse-proxy transparent-servers-for-ti transparent-servers-for-tp transparent-servers-for-wccp}</code> on page 189 is <code>reverse-proxy</code> or <code>transparent-servers-for-tp</code> and <code>ssl {enable disable}</code> on page 199 is <code>enable</code>. To upload a client certificate for FortiWeb, see the <i>FortiWeb Administration Guide</i>: http://docs.fortinet.com/fortiweb/admin-guides Note: This option is available only when the <code>protocol {HTTP FTP ADFSPIP}</code> on page 187 is <code>HTTP</code>.	
<code>client-certificate-forwarding {enable disable}</code>	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 <code>type {offline-protection reverse-proxy transparent-servers-for-ti transparent-servers-for-tp transparent-servers-for-wccp}</code> on page 189 is <code>transparent-servers-for-tp</code> and <code>ssl {enable disable}</code> on page 199 is <code>enable</code>. Note: This option is available only when the <code>protocol {HTTP FTP ADFSPIP}</code> on page 187 is <code>HTTP</code>.	<code>disable</code>
<code>client-certificate-forwarding-cert-header "<header_str>"</code>	Enter a custom certificate header that will include the Base64 certificate of the X.509 personal certificate presented by the client during the SSL/TLS handshake when it forwards the traffic to the protected web server. Note: This option is available only when the <code>protocol {HTTP FTP ADFSPIP}</code> on page 187 is <code>HTTP</code>.	<code>x-client-cert</code>
<code>client-certificate-forwarding-sub-header "<header_str>"</code>	Enter a custom subject header that will include the subject of the X.509 personal certificate presented by the client during the SSL/TLS handshake when it forwards the traffic to the protected web server. Note: This option is available only when the <code>protocol {HTTP FTP ADFSPIP}</code> on page 187 is <code>HTTP</code>.	<code>x-client-dn</code>
<code>client-certificate-proxy {enable disable}</code>	Enable to configure seamless PKI integration. When this option is configured, FortiWeb attempts to verify client certificates when users make requests and resigns new certificates that it sends to the server. Also configure <code>client-certificate-proxy-sign-ca <sign_ca></code> on page 192. Note: This option is available only when the <code>protocol {HTTP FTP ADFSPIP}</code> on page 187 is <code>HTTP</code>.	<code>disable</code>

Variable	Description	Default
client-certificate-proxy-sign-ca <sign_ca>	Select a Sign CA FortiWeb will use to verify and resign new client certificates. Note: This option is available only when the protocol {HTTP FTP ADFSPIP} on page 187 is HTTP.	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 0–1,048,576.	0
domain "<server_fqdn>"	Enter the fully-qualified domain name of the web server to include in the pool, such as <code>www.example.com</code> . 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 {physical domain sdn-connector} on page 196 is domain.	No default.
health-check-inherit {enable disable}	Select either: • enable—Use the health check specified by <code>health</code> in the server pool configuration. • disable—Use the health check specified by <code>health</code> in this pool member configuration.	enable
hlck-domain <hlck-domain_str>	Enter the domain name of the server pool.	No default.
hpkp-header "<hpkp_name>"	Enter an HPKP profile, if any, to use to verify certificates when clients attempt to access a server. HPKP prevents attackers from carrying out Man in the Middle (MITM) attacks with forged certificates. Available only when the operating mode is True Transparent Proxy. Note: This option is available only when the protocol {HTTP FTP ADFSPIP} on page 187 is HTTP.	disable
hsts-header {enable disable}	Enable to combat MITM attacks on HTTP by injecting the RFC 6797 (http://tools.ietf.org/html/rfc6797) strict transport security header into the reply, such as:	disable

Variable	Description	Default
	Strict-Transport-Security: max-age=31536000; includeSubDomains;Preload 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 {offline-protection reverse-proxy transparent-servers-for-ti transparent-servers-for-tp transparent-servers-for-wccp} on page 189 is <code>transparent-servers-for-tp</code> and ssl {enable disable} on page 199 is <code>enable</code>. Note: This option is available only when the protocol {HTTP FTP ADFSPIP} on page 187 is <code>HTTP</code>.	
<code>hsts-max-age <timeout_int></code>	Enter the time to live in seconds for the HSTS header. This setting applies only if hsts-header {enable disable} on page 192 is <code>enable</code>. Note: This option is available only when the protocol {HTTP FTP ADFSPIP} on page 187 is <code>HTTP</code>.	7776000
<code>HTTP2 {enable disable}</code>	Enable to allow HTTP/2 communication between the FortiWeb and this back-end web server for HTTP/2 security inspections in Reverse Proxy mode; or enable HTTP/2 security inspections in True Transparent Proxy mode. When HTTP/2 security inspection is enabled in Reverse Proxy mode (see server-policy policy on page 150): <code>enable</code>—Make sure the traffic is transferred in HTTP/2 between FortiWeb and this web server, if this web server supports HTTP/2. Note: Make sure that this back web server really supports HTTP/2 before you enable this, or connections will go failed. <code>disable</code>—Make FortiWeb to converse HTTP/2 to HTTP/1.x for this web server, or converse HTTP/1.x to HTTP/2 for the clients, if this web server does not support HTTP/2. When FortiWeb operates in True Transparent Proxy mode (see opmode {offline-protection reverse-proxy transparent transparent-inspection wccp} on page 374): <code>enable</code>—Enable HTTP/2 security inspection. It only requires this option to be enabled and the SSL be well-configured to enable the HTTP/2	disable

Variable	Description	Default
	security inspection. No HTTP/2 configuration is required for server-policy policy on page 150. When HTTP/2 inspection is enabled in True Transparent Proxy mode, FortiWeb performs no protocol conversions between HTTP/1.x and HTTP/2, which means HTTP/2 connections will not be established between clients and back-end web servers if the web servers do not support HTTP/2. 2. <code>disable</code>—Disable HTTP/2 security inspection. Note: 1. This option is available only if <code>type {offline-protection reverse-proxy transparent-servers-for-ti transparent-servers-for-tp transparent-servers-for-wccp}</code> on page 189 is set to <code>reverse-proxy</code> or <code>transparent-servers-for-tp</code>; and when <code>type</code> is <code>transparent-servers-for-tp</code>, this option is available only if <code>ssl {enable disable}</code> on page 199 is <code>enable</code>. 2. Please confirm your FortiWeb operation mode and the HTTP versions your back-end web servers are running first to make appropriate configuration here, so that HTTP/2 inspection can work correctly with your web servers. 3. For details about HTTP/2 support, see the FortiWeb Administration Guide: http://docs.fortinet.com/fortiweb/admin-guides Note: This option is available only when the <code>protocol {HTTP FTP ADFSPIP}</code> on page 187 is <code>HTTP</code>.	
<code>http2-window-size <int></code>	Enter the window size (determining the amount of data in bytes that FortiWeb is willing to receive at any given time) for HTTP/2 connections between the back-end server and FortiWeb. The valid range is 65,535-2,147,483,647 bytes.	131,070
<code>implicit_ssl {enable disable}</code>	Enable so that FortiWeb will communicate with the pool member using implicit SSL. Note: This option is available only when the <code>protocol {HTTP FTP ADFSPIP}</code> on page 187 is set to <code>FTP</code>.	disable
<code>intermediate-certificate-group "<CA-group_name>"</code>	Enter 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.	No default.

Variable	Description	Default
	If clients receive certificate warnings that the server certificate configured in <code>certificate "<certificate_name>"</code> on page 190 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. For details, see the FortiWeb Administration Guide: http://docs.fortinet.com/fortiweb/admin-guides Available only if <code>type {offline-protection reverse-proxy transparent-servers-for-ti transparent-servers-for-tp transparent-servers-for-wccp}</code> on page 189 is <code>transparent-servers-for-tp</code> and <code>ssl {enable disable}</code> on page 199 is <code>enable</code>. For Reverse Proxy mode, configure this setting in the server policy instead. For details, see <code>intermediate-certificate-group "<CA-group_name>"</code> on page 162. Note: This option is available only when the <code>protocol {HTTP FTP ADFSPIP}</code> on page 187 is <code>HTTP</code>.	
<code>ip {"address_ipv4" "address_ipv6"}</code>	Enter 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 <code>server-type {physical domain sdn-connector}</code> on page 196 is <code>physical</code>.	No default.
<code>port <port_int></code>	Enter the TCP port number where the pool member listens for connections. The valid range is 1–65,535.	80 (HTTP)/21 (FTP)
<code>recover <recover_int></code>	Specify 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 0–86,400. After the recovery period elapses, FortiWeb assigns connections at the rate specified by <code>warm-rate <warm-rate_int></code> on page 205. 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	0

Variable	Description	Default
	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 {disable enable maintain} on page 202 to <code>maintain</code>.	
<code>server-side-sni {enable disable}</code>	Specify 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. Note: This option is available only when the protocol {HTTP FTP ADFSPIP} on page 187 is <code>HTTP</code>.	<code>disable</code>
<code>server-type {physical domain sdn-connector}</code>	Specify whether to specify the pool member by IP address, domain, or automatically pulled by SDN connector. If your application servers are deployed on AWS or Azure, you can select <code>sdn-connector</code> to authorize FortiWeb to access the VM instances in your public cloud account, in order to automatically obtain the IP addresses.	<code>physical</code>
<code>sdn-addr-type {private public all}</code>	Select whether you want FortiWeb to get the public or private addresses of your application's VM instances, or select <code>all</code> to get both the public and the private addresses. Note: If you are using private IP addresses, ensure that FortiWeb can successfully establish connections with your application's VM instances in order to forward the traffic. Available only if the <code>server-type</code> is <code>sdn-connector</code>.	<code>private</code>
<code>sdn {aws azure}</code>	Select the SDN connector you have created. See system sdn-connector Available only if the <code>server-type</code> is <code>sdn-connector</code>.	No default.

Variable	Description	Default
filter <string>	Once you select the SDN collector that you have created, the available filter options for your VMs in your public cloud account will be listed here. You can select multiple filter options among instance IDs, image IDs, tags, etc. FortiWeb will find the VM instance, for example, whose instance ID is i-12345678 in your AWS account, then obtain the IP address of this instance and record it as the origin server's IP. AWS - instance-id (e.g. instance-id=i-12345678) - image-id (e.g. image-id=ami-123456) - key-name (e.g. key-name=aws-key-name) - subnet-id (e.g. subnet-id=sub-123456) - tag: <i>TagName</i> (The tag attached to the instance. <i>TagName</i> is a variable. It can be any value you have named for the tag. e.g. tag:Type=appserver. Up to 8 tags are supported.) Azure - vm-name (e.g. vm-name=myVM01) - tag: <i>TagName</i> (The tag attached to the virtual machine. <i>TagName</i> is a variable. It can be any value you have named for the tag, e.g. tag:Type=appserver. Up to 8 tags are supported.) Available only if the <code>server-type</code> is <code>sdn-connector</code>.	No default.
session-id-reuse {enable disable}	Enable so that FortiWeb reuses the session ID when establishing an SSL connection to a pserver. If the SSL connection has a server name, FortiWeb can only reuse a session ID for the specified pserver. If both a session ticket and ID exist for a pserver, FortiWeb will reuse the ticket. Note: This option is available only when <code>ssl {enable disable}</code> on page 199 is enabled.	disable
session-ticket-reuse {enable disable}	Enable so that FortiWeb reuses the session ticket when establishing an SSL connection to a pserver. If the SSL connection has a server name, FortiWeb can only reuse a session ticket for the specified pserver. Note: This option is available only when <code>ssl {enable disable}</code> on page 199 is enabled.	disable
sni {enable disable}	Enable to use a Server Name Indication (SNI) configuration instead of or in addition to the server certificate specified by <code>certificate "<certificate_name>"</code> on page 190.	disable

Variable	Description	Default
	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. For details, see system certificate sni on page 264. If you specify both a SNI configuration and a certificate, FortiWeb uses the certificate specified by certificate "<certificate_name>" on page 190 when the requested domain does not match a value in the SNI configuration. If you enable sni-strict {enable disable} on page 198, FortiWeb always ignores the value of certificate "<certificate_name>" on page 190. Available only if type {offline-protection reverse-proxy transparent-servers-for-ti transparent-servers-for-tp transparent-servers-for-wccp} on page 189 is transparent-servers-for-tp and ssl {enable disable} on page 199 is enable. Note: This option is available only when the protocol {HTTP FTP ADFSPIP} on page 187 is HTTP.	
sni-certificate "<sni_name>"	Enter 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>" on page 190 instead. Available only if sni {enable disable} on page 197 is enabled. Note: This option is available only when the protocol {HTTP FTP ADFSPIP} on page 187 is HTTP.	No default.
sni-strict {enable disable}	Select to configure FortiWeb to ignore the value of certificate "<certificate_name>" on page 190 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. Note: This option is available only when the protocol {HTTP FTP ADFSPIP} on page 187 is HTTP.	disable
certificate-type {enable disable}	Enable allow FortiWeb to automatically retrieve CA certificates from Let's Encrypt.	disable

Variable	Description	Default
lets-certificate <name>	Select the Letsencrypt certificate you have created. See system certificate letsencrypt .	No 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>" on page 190. 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>" on page 190 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. For details, see server-policy policy on page 150. 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.
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 {<cipher_1> <cipher2> <cipher3> ...} on page 200. Do not set to <code>custom</code> if HTTP2 {enable disable} on page 193 is set to <code>enable</code>. For details, see the <i>FortiWeb Administration Guide</i>: http://docs.fortinet.com/fortiweb/admin-guides	medium

Variable	Description	Default
	Available only if <code>type {offline-protection reverse-proxy transparent-servers-for-ti transparent-servers-for-tp transparent-servers-for-wccp}</code> on page 189 is <code>reverse-proxy</code> , <code>transparent-servers-for-tp</code> , or <code>transparent-servers-for-wccp</code> , and <code>ssl {enable disable}</code> on page 199 is <code>enable</code> .	
<code>ssl-custom-cipher {<cipher_1> <cipher2> <cipher3> ...}</code>	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-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 DHE-DSS-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-CHACHA20-POLY1305 ECDHE-RSA-CHACHA20-POLY1305 DHE-RSA-CHACHA20-POLY1305 ECDHE-ECDSA-AES256-CCM8 ECDHE-ECDSA-AES256-CCM DHE-RSA-AES256-CCM8 DHE-RSA-AES256-CCM ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 DHE-DSS-AES128-GCM-SHA256 DHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-CCM8 ECDHE-ECDSA-AES128-CCM DHE-RSA-AES128-CCM8 DHE-RSA-AES128-CCM ECDHE-ECDSA-AES256-SHA384 ECDHE-RSA-AES256-SHA384 DHE-RSA-AES256-SHA256 DHE-DSS-AES256-SHA256 ECDHE-ECDSA-CAMELLIA256-SHA384 ECDHE-RSA-CAMELLIA256-SHA384 DHE-RSA-CAMELLIA256-SHA256 DHE-DSS-CAMELLIA256-SHA256 ECDHE-ECDSA-AES128-SHA256 ECDHE-RSA-AES128-SHA256 DHE-RSA-AES128-SHA256	ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-CHACHA20-POLY1305 ECDHE-RSA-CHACHA20-POLY1305 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-SHA256 ECDHE-ECDSA-AES256-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-ECDSA-AES128-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-ECDSA-SHA256 ECDHE-RSA-AES128-SHA256

Variable	Description	Default
	DHE-DSS-AES128-SHA256	ECDHE-RSA-
	ECDHE-ECDSA-CAMELLIA128-SHA256	AES256-SHA
	ECDHE-RSA-CAMELLIA128-SHA256	ECDHE-
	DHE-RSA-CAMELLIA128-SHA256	ECDSA-
	DHE-DSS-CAMELLIA128-SHA256	AES128-SHA
	ECDHE-ECDSA-AES256-SHA	ECDHE-RSA-
	ECDHE-RSA-AES256-SHA	AES128-SHA
	DHE-RSA-AES256-SHA	AES256-GCM-
	DHE-DSS-AES256-SHA	SHA384
	DHE-RSA-CAMELLIA256-SHA	AES128-GCM-
	DHE-DSS-CAMELLIA256-SHA	SHA256
	ECDHE-ECDSA-AES128-SHA	AES256-
	ECDHE-RSA-AES128-SHA	SHA256
	DHE-RSA-AES128-SHA	AES128-
	DHE-DSS-AES128-SHA	SHA256
	DHE-RSA-CAMELLIA128-SHA	
	DHE-DSS-CAMELLIA128-SHA	
	AES256-GCM-SHA384	
	AES256-CCM8	
	AES256-CCM	
	AES128-GCM-SHA256	
	AES128-CCM8	
	AES128-CCM	
	AES256-SHA256	
	CAMELLIA256-SHA256	
	AES128-SHA256	
	CAMELLIA128-SHA256	
	AES256-SHA	
	CAMELLIA256-SHA	
	AES128-SHA	
	CAMELLIA128-SHA	
	DHE-RSA-SEED-SHA	
	ECDHE_RSA_DES_CBC3_SHA	
	DES_CBC3_SHA	
tls13-custom-cipher	Specify one or more TLS 1.3 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:	TLS_AES_256_GCM_SHA384

Variable	Description	Default
	TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256 TLS_AES_128_CCM_SHA256 TLS_AES_128_CCM_8_SHA256	
rfc7919-comply {enable disable}	Enable to apply cipher suites that comply with RFC-9719.	disable
supported-groups {X25519 prime256v1 secp384r1 secp521r1 brainpoolP256r1 brainpoolP384r1 brainpoolP512r1 ffdhe2048 ffdhe3072 ffdhe4096 ffdhe6144 ffdhe8192}	Select the RFC-9719 ciphers to be supported. The Supported Group is Elliptic Curve Parameters, while SSL/TLS negotiation could choose different Elliptic Curve algorithms, so please make sure to choose the corresponding ciphers in <code>ssl-custom-cipher</code>. - At least one FFDHE group should be selected. - At least one DHE cipher should be added. Due to design limitation, you need to select <code>custom</code> in <code>ssl-cipher</code> {medium high custom} and make sure to include at least one DHE cipher in the selected list. Using <code>High</code> or <code>Medium</code> together with RFC-9719 will lead to unexpected error. We will fix it in the future release. The system will return error if any of the above two conditions is not met. Please note RFC7919 does not comply with TLS 1.3, so if you have only enabled <code>tls-v13</code>, then RFC7919 will not take effect even if it's enabled. To apply both TLS 1.3 and RFC7919, it's recommended to enable a non-TLS 1.3 protocol, then select at least one DHE cipher.	No 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 <code>type</code> {offline-protection reverse-proxy transparent-servers-for-ti transparent-servers-for-tp transparent-servers-for-wccp} on page 189 is <code>transparent-servers-for-tp</code> and <code>ssl</code> {enable disable} on page 199 is <code>enable</code>. Note: This option is available only when the <code>protocol</code> {HTTP FTP ADFSPIP} on page 187 is <code>HTTP</code>.	enable
status {disable enable maintain}	To specify the status of the pool member, enter one of the following values: <code>enable</code>—Specifies that this pool member can	enable

Variable	Description	Default
	receive new sessions from FortiWeb. <code>disable</code>—Specifies that this pool member does not receive new sessions from FortiWeb and FortiWeb closes any current sessions as soon as possible. <code>maintain</code>—Specifies that this pool member does not receive new sessions from FortiWeb but FortiWeb maintains any current connections.	
<code>tls-v10 {enable disable}</code>	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. This must be set to <code>disable</code> if HTTP2 {enable disable} on page 193 is set to <code>enable</code>. Available only if type {offline-protection reverse-proxy transparent-servers-for-ti transparent-servers-for-tp transparent-servers-for-wccp} on page 189 is <code>reverse-proxy</code>, <code>transparent-servers-for-tp</code>, or <code>transparent-servers-for-wccp</code>, and ssl {enable disable} on page 199 is <code>enable</code>.	<code>enable</code>
<code>tls-v11 {enable disable}</code>	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. This must be set to <code>disable</code> if HTTP2 {enable disable} on page 193 is set to <code>enable</code>. Available only if type {offline-protection reverse-proxy transparent-servers-for-ti transparent-servers-for-tp transparent-servers-for-wccp} on page 189 is <code>reverse-proxy</code>, <code>transparent-servers-for-tp</code>, or <code>transparent-servers-for-wccp</code>, and ssl {enable disable} on page 199 is <code>enable</code>.	<code>enable</code>
<code>tls-v12 {enable disable}</code>	For Reverse Proxy mode, specifies whether secure connections between FortiWeb and the server pool member can use the TLS 1.2 cryptographic protocol.	<code>enable</code>

Variable	Description	Default
	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 {offline-protection reverse-proxy transparent-servers-for-ti transparent-servers-for-tp transparent-servers-for-wccp} on page 189 is <code>reverse-proxy</code>, <code>transparent-servers-for-tp</code>, or <code>transparent-servers-for-wccp</code>, and ssl {enable disable} on page 199 is <code>enable</code>.	
<code>tls-v13 {enable disable}</code>	For Reverse Proxy mode, specifies whether secure connections between FortiWeb and the server pool member can use the TLS 1.3 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 1.3 cryptographic protocol. Available only if type {offline-protection reverse-proxy transparent-servers-for-ti transparent-servers-for-tp transparent-servers-for-wccp} on page 189 is <code>reverse-proxy</code>, <code>transparent-servers-for-tp</code>, or <code>transparent-servers-for-wccp</code>, and ssl {enable disable} on page 199 is <code>enable</code>.	<code>disable</code>
<code>url-cert {enable disable}</code>	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>" on page 162 is configured. Note: This option is available only when the protocol {HTTP FTP ADFSPIP} on page 187 is <code>HTTP</code>.	<code>disable</code>
<code>urlcert-group "<urlcert-group_name>"</code>	Enter 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 details about creating a group, see system certificate urlcert on page 268. Note: This option is available only when the protocol {HTTP FTP ADFSPIP} on page 187 is <code>HTTP</code>.	No default.
<code>urlcert-hlen <len_int></code>	Enter the maximum allowed length for an HTTP request with a URL that matches an entry in the URL-based client certificate group, in kilobytes.	No default.

Variable	Description	Default
	FortiWeb blocks any matching requests that exceed the specified size. This setting prevents a request from exceeding the maximum buffer size. The valid range is 16–128. Note: This option is available only when the protocol {HTTP FTP ADFSPIP} on page 187 is HTTP.	
warm-rate <warm-rate_int>	Specify the maximum connection rate (per second) while the pool member is starting up. The default is 10 connections per second. The valid range is 1–86,400. 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 <warm-up_int> on page 205 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
warm-up <warm-up_int>	Specify for how long (in seconds) 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 0–86,400.	0
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 1–9,999.	0

Variable	Description	Default
ssl-session-timeout <ssl-session-timeout_int>	When FortiWeb is configured as an SSL server, you can set SSL session timeout intervals via the CLI. This is available only in Reverse Proxy and True Transparent Proxy modes.	No default.
ssl-quiet-shutdown {enable disable}	For HTTPS connection, when disabled, FortiWeb sends ssl alert message to the client or server pool first, and then FIN. When enabled, FortiWeb directly sends FIN message instead of sending ssl alert message.	Disable
server-certificate-verify {enable disable}	Enable so that FortiWeb appliance will verify certificates presented by HTTP server.	Disable
server-certificate-verify-policy "<policy_name>"	Enter the certificate verify policy name.	No default.
server-certificate-verify-action {alert alert_deny redirect}	Select which action the FortiWeb appliance will take when it detects a certificate violation.	No default.
adfs-username <adfs-username_str>	Type the username that will be used by FortiWeb to connect with the AD FS server. You should include the domain to which FortiWeb and the AD FS server belong. For example, damain1\administrator.	No default.
adfs-password <adfs-password_str>	Type the password that will be used by FortiWeb to connect with the AD FS server.	No default.
multi-certificate {enable disable}	Enable this option to allow FortiWeb to use multiple local certificates. Available when: ssl {enable disable} on page 199 is enabled, and FortiWeb is operating in TTP or WCP mode that performs SSL inspection.	disable
certificate-group <certificate-group_str>	Select the the multi-certificate file you have created.	No default.
enforce-trust-establishment {enable disable}	Enable to establish trust with ADFS servers before building up connections.	disable

Example

This example configures a server pool named `server-pool1`. It consists of two physical servers: `192.0.2.10` and `192.0.2.11`.

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 "192.0.2.10"
        set ssl disable
        set port 8081
      next
      edit 2
        set status enable
        set server-type physical
        set ip "192.0.2.11"
        set ssl disable
        set port 8082
      next
    end
  next
end
```

Related topics

- [server-policy policy on page 150](#)
- [server-policy HTTP-content-routing-policy on page 118](#)
- [system certificate local on page 258](#)
- [server-policy health on page 112](#)
- [server-policy persistence-policy on page 146](#)
- [waf ftp-protection-profile on page 510](#)
- [system feature-visibility on page 288](#)

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 [server-policy policy on page 150](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For details, see [Permissions on page 46](#).

Syntax

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

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

- [server-policy vserver on page 215](#)
- [server-policy policy on page 150](#)
- [server-policy custom-application application-policy on page 1](#)

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 [server-policy policy on page 150](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For details, see [Permissions on page 46](#).

Syntax

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

Variable	Description	Default
"<service_name>"	Enter the name of a predefined network service, such as HTTP or HTTPS. The maximum length is 63 characters. To display the list of existing services, enter: 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

- [server-policy vserver on page 215](#)
- [server-policy policy on page 150](#)
- [server-policy service custom on page 207](#)

server-policy setting

Use this command to configure the server policy settings.

Syntax

```
config server-policy setting
  set core-file-count <core-file-count_int>
  set enable-core-file {enable | disable | enable-best-effort}
  set enable-session-statistics {enable | disable}
  set enable-single-worker {enable | disable}
  set hsm {enable | disable}
  set hsm-manufacturer {luna | primus}
  set no-session-limit {enable | disable}
  set no-ssl-encrypt-then-mac {enable | disable}
  set offline-session-timeout {seconds_int}
  set use-first-ack-mac {enable | disable}
  set dpdk {enable | disable}
  set high-compatibility-mode {enable | disable}
  set graceful-shutdown {enable | disable}
  set server-pool-connection-limit-log {enable | disable}
  set tls13-early-data-mode {enable | disable}
  set record-content-routing-error-log {enable | disable}
  set server-invalid-no-reponse {enable | disable}
  set using-dns-proxy {enable | disable} on page 212
  set df-flag {enable | disable}
  set tls12-compatible-sigalg {enable | disable}
  set corefile-ha-failover {enable | disable}
  set reverse-dns-cache-timeout <int>
  set crldp-update-interval <int>
  set crldp-ttl-failed <int>
  set restrict-weak-sign-algo {enable | disable}
end
```

Variable	Description	Default
core-file-count <core-file-count_int>	The maximum core dump file number. The valid values are 3 and 5.	No default
enable-core-file {enable disable enable-best-effort}	disable: Disable coredump for proxyd. enable: Enable coredump action for proxyd. It will stop if coredump cannot finish in hung task timeout seconds. enable-best-effort: Enable coredump action for proxy. It will stop until the entire core file is generated. This option is useful to analyze a tough issue, though it may cause your service to stop responding for a long time	disable
enable-session-statistics {enable disable}	Enable/disable session statistics for FortiView.	No default
enable-single-worker {enable disable}	Enable/disable single worker mode. If enabled, there will be only one worker thread to handle the traffic. It's usually	No default

Variable	Description	Default
	used for diagnose only.	
hsm {enable disable}	Specifies whether the settings you use to integrate FortiWeb with an HSM (hardware security module) are displayed in the web UI.	No default
hsm-manufacturer {luna primus}	Specify the HSM manufacturer. Currently, FortiWeb supports LUNA HSM and Primus HSM.	luna
no-session-limit {enable disable}	Enable not to limit the maximum concurrency sessions of FortiWeb-VM. If this option is disabled, the maximum concurrent sessions for all the policies on a VM is 20,000 (2vCPUs), 50,000 (4vCPUs), or 100,000 (8vCPUs); For each policy, the number is 8,000 (2vCPUs), 15,000 (4vCPUs), or 50,000 (8vCPUs).	No default
no-ssl-encrypt-then-mac {enable disable}	Disable to include the encrypt-then-mac extension in the packets sent by the client.	disable
use-first-ack-mac {enable disable}	Once enabled, machine learning only observes the source MAC of two ACK packets for a URL at Three-way handshake. If disabled, machine leaning observes all ACK packets, which continues refreshing MAC, with the performance affected.	enable
dpdk {enable disable}	Enable/disable DPDK for packet processing.	No default
high-compatibility-mode {enable disable}	When this option is enabled, all SSL traffic is decrypted and encrypted using the CPU. While this mode is compatible with most environments, it is not efficient, as it places a heavy load on the CPU. To improve SSL traffic processing efficiency, you can set this option to "disable", allowing SSL encryption and decryption to be handled by the hardware SSL acceleration card. This significantly enhances the performance of session establishment and processing. To verify whether your hardware platform supports an SSL acceleration card, run the following command: <pre># diagnose hardware check sslcard</pre> If the output shows "pass", it indicates that your platform has a properly functioning SSL acceleration card. Note: On platforms that do not support an SSL acceleration card—including FortiWeb-VM—SSL encryption and decryption will continue to be handled by the CPU, even if this option is set to "disable."	disable

Variable	Description	Default
	In summary, it is recommended to set this option to "enable" only in environments that require high compatibility, such as when using a Hardware Security Module (HSM) for SSL sessions. In such cases, offloading SSL processing to the acceleration card may cause compatibility issues, so the option should be set to "enable".	
offline-session-timeout {seconds_int}	This setting only works in Offline Protection mode. It's a session optimization option. FortiWeb's resources will be unnecessarily consumed if the connection always keeps on. With this option, you can configure the session timeout value to avoid them staying on for too long. The valid range is seconds 30–1200 seconds.	No default
graceful-shutdown {enable disable}	If disabled, the peer TCP connections are reset during system shutdown.	enable
server-pool-connection-limit-log {enable disable}	Enable to send a warning level event log when the connection number of each real server reaches the limitation.	disable
tls13-early-data-mode {enable disable}	Enable O-RTT in TLS 1.3.	disable
record-content-routing-error-log {enable disable}	If enabled, the reason of the content routing failure will be recorded in event log.	disable
server-invalid-no-reponse {enable disable}	Enable this option so that closes the client connection when all the servers in the server pool are unresponsive.	disable
using-dns-proxy {enable disable}	This option is enabled by default. If it is disabled, the system uses <code>getaddrinfo</code> to resolve the domain name.	enable
df-flag {enable disable}	Enable to allow FortiWeb to send non DF-flag packet to pass the device with low MTU.	disable
tls12-compatible-sigalg {enable disable}	When <code>tls12-compatible-sigalg</code> is enabled, signature algorithm negotiation in TLS handshake for FortiWeb behaves exactly the same as OpenSSL 1.1.0. Please note executing this command causes the proxyd to restart so all current sessions will be dropped. This command is specific to very rare case. Do not use it unless suggested by Fortinet support team.	disable
corefile-ha-failover {enable disable}	Enable to trigger HA fail-over upon proxyd coredump, so that the secondary node can immediately take over the traffic when coredump file is being generated on the primary node. Note the following when using this command:	disable

Variable	Description	Default
	- You should set <code>enable-core-file</code> to enable or <code>enable-best-effort</code> for the <code>corefile-ha-failover</code> to work. - The <code>enable-core-file</code> and <code>corefile-ha-failover</code> attributes will NOT be synchronized to other devices in the same HA group, so you need to configure these configurations on each device if needed. - Currently only the <code>proxyd</code> daemon <code>coredump</code> can trigger <code>corefile-ha-failover</code>. Other daemons can't trigger it. - This function works in active-passive and active-active standard HA modes. It is not suggested to enable it in HA Manager mode on public clouds, because usually the load balancer in front of the FortiWeb devices will do health check and guarantee that traffic is dispatched to the healthy nodes. - It is recommended to enable this option only on one FortiWeb, usually the primary device. Otherwise a <code>proxyd</code> <code>coredump</code> occurring on both devices may lead to HA fail-over back and forth between two devices.	
<code>reverse-dns-cache-timeout <int></code>	The system caches the reverse DNS lookup results. You can set the <code>reverse-dns-cache-timeout</code> value so that the cached items can be removed after the expiration time. The valid value range is 1-1440.	60 (minutes)
<code>crldp-update-interval <int></code>	Specify the update interval (in seconds) for Certificate Revocation Lists (CRL) distribution point. CRL files can be outdated, so the CRL distribution point should check from time to time for each entry so as to keep them up-to-date. you can run the following commands to check the CRL retrieval debug information <pre>diagnose debug application crl_update <0-8> diag debug enable</pre>	3 (seconds)
<code>crldp-ttl-failed <int></code>	Specify the TTL (time-to-alive) in minutes for failed retrievals. If FortiWeb fails to retrieve CRL from the distribution point, it will make another attempt to retrieve it after the specified <code>crldp-ttl-failed</code> time. If the CRL is expired, the system will block the client traffic even if it has a valid certificate. You can allow the use of previously retrieved CRLs when the current CRL distribution point retrievals fail or are pending. <pre>config system certificate verify set crl-allow-expired enable end</pre>	5 (minutes)

Variable	Description	Default
	We highly recommend enabling it as a temporary solution only when the CRL has expired. Ideally, we strongly suggest using the most up-to-date CRL file at all times to ensure that the client with revoked certificates can be promptly blocked. For more information on CRL, see "Revoking certificates" in FortiWeb Administration Guide.	
restrict-weak-sign-algo {enable disable}	Enable to block TLS handshakes that use SHA-1 or SHA-224 for digital signatures. These algorithms are considered insecure and are deprecated in modern cryptographic standards. This setting is effective only when FIPS-CC mode is disabled. Changing this option will restart the <code>proxyd</code> process.	disable

Related topics

- [server-policy vserver on page 215](#)
- [server-policy policy on page 150](#)

server policy traffic-mirror

Use this command to configure FortiWeb to send traffic to third party IPS/IDS devices through network interfaces for traffic monitoring in Reverse Proxy and True Transparent Proxy modes.

See [system feature-visibility on page 288](#) for how to enable traffic mirror first.

Syntax

```
config server-policy traffic-mirror
  edit "<traffic-mirror_name>"
  config mirror-rule
    edit mirror-rule <mirror-rule_str>
      set mode {direct | switch | server}
      set interface <interface_int>
      set destination-mac <destination-mac_str>
      set server-ip <server-ip_str>
      set server-port <server-port_int>
    next
  end
next
end
```

Variable	Description	Default
"<traffic-mirror_name>"	Enter a name for the traffic mirror policy.	No default.
mirror-rule <mirror-rule_str>	Select the sequence number of the mirror rule created.	No default.
mode {direct switch server}	Select one of the three modes: Direct—the mirrored packets are directly sent to IPS/IDS devices. Switch—the mirrored packets are sent to IPS/IDS devices through the switch. Server—the mirrored packets are sent to the designated IP of IPS/IDS devices.	direct
interface <interface_int>	When the mode is Direct, select one FortiWeb port to connect to IPS/IDS device. When the mode is Switch, select one FortiWeb port to connect to default the switch.	No
destination-mac <destination-mac_str>	Type the MAC of IPS/IDS interface, where the traffic from FortiWeb goes to. Available only when mode {direct switch server} on page 215 is Switch.	No default.
server-ip <server-ip_str>	Enter the designated IP of IPS/IDS devices. Available only when mode {direct switch server} on page 215 is Server.	No default.
server-port <server-port_int>	Enter the HTTP port that the IPS/IDS devices can listen to. Available only when mode {direct switch server} on page 215 is Server.	No default.

Example

This example configures a traffic mirror policy.

```
config server-policy traffic-mirror
edit policy1
config mirror-rule
edit 2
set mode direct
set interface port1

end
next
end
```

Related topics

- [system feature-visibility on page 288](#)

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 192.0.2.1/24 could forward to the physical server 192.0.2.2.

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 [server-policy policy on page 150](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config server-policy vserver
  edit "<virtual-server_name>"
    config vip-list
      edit server-policy vserver
        set interface "<interface_name>"
        set status {enable | disable}
        set vip "<vip_str>"
        set use-interface-ip {enable | disable}
      next
    end
  next
end
```

Variable	Description	Default
"<virtual-server_name>"	Enter the name of the new or existing virtual server. The maximum length is 63 characters. To display the list of existing servers, enter: edit ?	disable
"<vip-list_id>"	Enter the sequence number of the virtual IP in the table.	No default.
status {enable disable}	Enable to accept traffic destined for this virtual server.	No default.

Variable	Description	Default
interface "<interface_ name>"	Enter the name of the network interface or bridge, such as <code>port1</code> or <code>bridge1</code> , to which the virtual server is bound, and on which traffic destined for the virtual server will arrive. The maximum length is 63 characters. To display the list of existing interfaces, enter: <code>edit ?</code>	No default.
vip "<vip_str>"	Enter the IPv4 or IPv6 address and subnet of the virtual server.	0.0.0.0 ::/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 <code>vip</code> or <code>vip6</code> .	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"
    config vip-list
      edit 2
        set interface port1
        set status enable
        set vip "192.0.2.1 255.255.255.0"
      next
    end
  next
end
```

Related topics

- [system interface on page 344](#)
- [server-policy policy on page 150](#)
- [server-policy service custom on page 207](#)
- [ping on page 838](#)
- [network ip on page 786](#)

server-policy ztna-profile

Use this command to configure ZTNA profile.

For more information on ZTNA, please refer to "Chapter: Zero Trust Network Access (ZTNA)" in *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config server-policy ztna-profile
  edit <ztna-profile_name>
    set action {pass | alert_deny | deny_no_log}
    config rule list
      edit <rule-list_index>
        set rule-name <ztna-rule_name>
      next
    end
  next
end
```

Variable	Description	Default
"<ztna-profile_name>"	Enter the name of the ZTNA profile. The maximum length is 63 characters. To display the list of existing profiles, enter: <code>edit ?</code>	No default.
action {pass alert_deny deny_no_log}	Select the specific action to be taken when the request matches the policy. <code>pass</code>—Accept the request. <code>alert_deny</code>—Block the request (or reset the connection) and generate an alert email and/or log message. <code>deny_no_log</code>—Deny a request. Do not generate a log message.	<code>pass</code>
<rule-list_index>	Enter the rule list index number.	No default.
ztna-rule_name	Enter the ZTNA rule name. See server-policy ztna-rule on page 219 for how to create ZTNA rules.	No default.

Related topics

- [system endpoint-control on page 799](#)
- [server-policy ztna-profile on page 217](#)
- [server-policy ztna-rule on page 219](#)

server-policy ztna-rule

Use this command to configure ZTNA rule.

For more information on ZTNA, please refer to "Chapter: Zero Trust Network Access (ZTNA)" in *FortiWeb Administration Guide*.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config server-policy ztna-rule
  edit <ztna-rule_name>
    set action {pass | alert_deny | deny_no_log}
    config ems-tag-condition
      edit <ems-tag-condition_index>
        set ems-tag <tag_name>
        set combine {and | or}
      next
    end
    config source-address-condition
      edit <source-address-condition_index>
        set source-address <IP_address>
      next
    end
    config geo-condition
      edit <geo-condition_index>
        set country-list <country>
      next
    end
  next
end
```

Variable	Description	Default
"<ztna-rule_name>"	Enter the name of the ZTNA rule. The maximum length is 63 characters. To display the list of existing rules, enter: edit ?	No default.
action {pass alert_deny deny_no_log}	Select the specific action to be taken when the request matches the rule. <code>pass</code>—Accept the request. <code>alert_deny</code>—Block the request (or reset the connection) and generate an alert email and/or log message. <code>deny_no_log</code>—Deny a request. Do not generate a log message.	pass

Variable	Description	Default
<ems-tag-condition_index>	Enter the EMS tag condition index number.	No default.
ems-tag	Enter the EMS tag to match. The EMS tags are automatically synchronized from FortiClient EMS.	No default.
combine {and or}	and means the request only matches if it has all tags specified; or means the request matches if it has any of the tags specified.	and
<source-address-condition_index>	Enter the source IP address condition index number.	No default.
source-address <IP_address>	Enter one of the following values in Source IPv4/IPv6/IP Range : - 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, 192.0.2.109). - A range of addresses (e.g., 192.0.2.1-192.0.2.255 or 10:200::10:1-10:200:10:100).	No default.
<geo-condition_index>	Enter the GEO country condition index number.	No default.
set country-list <country>	Enter countries to match.	No default.



If multiple conditions are added in one ZTNA rule, the matching logic is:

- For conditions in different types (Source IP, GEO and ZTNA Tags), their relationship is ALL.
- For conditions in the same type, their relationship is OR.

If a request matches with the conditions specified in the rule, FortiWeb will take corresponding actions specified in the rule.

Related topics

- [system endpoint-control on page 799](#)
- [server-policy ztna-rule on page 219](#)
- [server-policy ztna-profile on page 217](#)

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. For details, see [system admin on page 223](#).

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.

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 46](#)

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 loggrp {none | r | rw | w}
    set mlgrp {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>"	Enter the name of the access profile. The maximum length is 63 characters. To display the list of existing profiles, enter: edit ?	No default.
admingrp {none r rw w}	Enter 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. For details, see .	none
authusergrp {none r rw w}	Enter the degree of access that administrator accounts using this access profile will have to the HTTP authentication user configuration.	none
loggrp {none r rw w}	Enter the degree of access that administrator accounts using this access profile will have to the logging and alert email configuration.	none
mlgrp {none r rw w}	Enter the degree of access that administrator accounts using this access profile will have to the machine learning configuration.	none
mntgrp {none r rw w}	Enter 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}	Enter 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}	Enter 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}	Enter the degree of access that administrator accounts using this access profile will have to the server policy (formerly called traffic routing) configuration.	none
wadgrp {none r rw w}	Enter 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}	Enter the degree of access that administrator accounts using this access profile will have to the web protection profile configuration.	none

Variable	Description	Default
wvsgrp {none r rw w}	Enter 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 loggrp rw
    set mlgrp 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

- [system admin on page 223](#)
- [server-policy custom-application application-policy on page 1](#)
- [Permissions on page 46](#)

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 [system interface on page 344](#), , and [Connecting to the CLI on page 33](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system admin
edit "<administrator_name>"
    set access-profile "<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 trusthosts "<management-computer_ipv4mask>"
    set ip6trusthosts "<management-computer_ipv6mask>"
    set type {local-user | remote-user}
    set admin-usergroup "<remote-auth-group_name>"
    set wildcard {enable | disable}
    set sshkey "<sshkey_str>"
    set force-password-change {enable | disable} on page 228
next
end
```

Variable	Description	Default
"<administrator_name>"	Enter the name of the administrator account, such as <code>admin1</code> or <code>admin@example.com</code>, that can be referenced in other parts of the configuration. Do not use spaces or special characters except the 'at' symbol (<code>@</code>). The maximum length is 63 characters. To display the list of existing accounts, enter: <pre>edit ?</pre> 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.
access-profile "<access-profile_name>"	Enter the name of an access profile that gives the permissions for this administrator account. See also system accprofile on page 220. The maximum length is 63 characters.	No default.

Variable	Description	Default
	You can select prof_admin, a special access profile used by the <code>admin</code> administrator account. However, selecting this access profile will not confer all of the same permissions of the <code>admin</code> administrator. For example, the new administrator would not be able to reset lost administrator passwords. To display the list of existing profiles, enter: <pre>edit ?</pre> Tip: Alternatively, if your administrator accounts authenticate via a RADIUS query, you can assign their access profile through the RADIUS server using RFC 2548 (http://www.ietf.org/rfc/rfc2548.txt) Microsoft Vendor-specific RADIUS Attributes. On the RADIUS server, create an attribute named: <pre>ATTRIBUTE FortiWeb-Access-Profile 6</pre> 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} on page 225 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.	
<code>accprofile-override {enable disable}</code>	Enable to use the access profile indicated by the RADIUS query response, and ignore access-profile "<access-profile_name>" on page 224. This setting applies only if admin-usergroup "<remote-auth-group_name>" on page 227 is configured to use a RADIUS query to authenticate this account.	disable
<code>domains "<adom_name>"</code>	Enter the name of the administrative domain (ADOM) to assign and restrict this administrative account to. You can set multiple ADOMs, each separated with comma ",". This setting applies only if ADOMs are enabled in <code>config system global</code>.	No default.
<code>password "<password_str>"</code>	Enter 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.	No default.

Variable	Description	Default
	This setting applies only when <code>type</code> is <code>local-user</code> . 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.	
email-address "<contact_email>"	Enter an email address that can be used to contact this administrator. The maximum length is 63 characters.	No default.
first-name "<name_str>"	Enter the first name of the administrator. The maximum length is 63 characters.	No default.
last-name "<surname_str>"	Enter the surname of the administrator. The maximum length is 63 characters.	No default.
mobile-number "<cell-phone_str>"	Enter a cell phone number that can be used to contact this administrator. The maximum length is 63 characters.	No default.
phone-number "<phone_str>"	Enter a phone number that can be used to contact this administrator. The maximum length is 63 characters.	No default.
trusthosts "<management-computer_ipv4mask>"	Enter 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 10 trusted hosts, separated with space. To allow login attempts from any IP address, enter <code>0.0.0.0/0.0.0.0</code>. 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 details about administrative access protocols, see system interface on page 344. 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
ip6trusthosts "<management-computer_ipv6mask>"	Enter 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 10 trusted hosts, separated with space. To allow login attempts from any IP address, enter <code>::/0</code>.	::/0

Variable	Description	Default
	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 details about administrative access protocols, see system interface on page 344. Note: For improved security, restrict all three trusted host addresses to the IP addresses of computers from which only this administrator will log in.	
type {local-user remote-user}	Select either: <code>local-user</code>—Authenticate this account locally, with the FortiWeb appliance itself. <code>remote-user</code>—Authenticate this account via a remote server such as an LDAP or RADIUS server. Also configure admin-usergroup "<remote-auth-group_name>" on page 227. If there is only one account configured on FortiWeb (i.e. the <code>admin</code> user), before setting it as a remote user, do make sure the remote authentication server is safe and stable. Once the remote authentication server is damaged and the account credentials are lost, FortiWeb can't recover it, which means the only one account that can log in to FortiWeb is lost. The configurations will be lost and you need to re-install FortiWeb image.	No default.
admin-usergroup "<remote-auth-group_name>"	Enter 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 63 characters. To display the list of existing groups, enter: <pre>edit ?</pre> For details about configuring remote authentication groups, see user admin-usergrp on page 394.	No default.
wildcard {enable disable}	Used when administrator accounts authenticate via a RADIUS query. This setting applies only if the value of type {local-user remote-user} on page 227 is <code>remote-user</code>.	No default.
sshkey "<sshkey_str>"	The public key used for connecting to the CLI using a public-private key pair.	No default.

Variable	Description	Default
	For more information on connecting to the CLI using a public-private key pair, see “Connecting to the CLI” in the <i>FortiWeb Administration Guide</i> : http://docs.fortinet.com/fortiweb/admin-guides	
force-password-change {enable disable}	Enable/disable force password change for next login. This field can be configured only when Password Policy is enabled in System > Admin > Settings .	Disable

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 (192.0.2.0/24), or from one of two specific IP addresses (192.0.2.15 and 192.0.2.50).

```
config system admin
  edit log-auditor
    set access-profile log_read_access
    set password P@ssw0rd
    set email-address log-admin@example.com
    set trusthost1 192.0.2.0 255.255.255.0
    set trusthost2 192.0.2.15 255.255.255.255
    set trusthost3 192.0.2.50 255.255.255.255
    set force-password-change enable
end
```



To display all dashboard status and widget settings, enter:

```
config system admin
  show
```

Related topics

- [system accprofile on page 220](#)
- [system global on page 307](#)
- [user admin-usergrp on page 394](#)

system admin-certificate ca

When FortiWeb's certificate-based Web UI login is applied. Besides the administrators' certificates information, the corresponding certificate authority (CA) certificates are required to be stored on the FortiWeb appliance. Certificate authorities validate and sign other certificates in order to indicate to third parties that those other certificates are

authentic and can be trusted. FortiWeb authorizes the administrator's login by verifying its certificate with the corresponding CA.

Use this command to show the names of the CA certificates that are relative to the administrators' certificates. You use the web UI to upload these certificates.

CA certificates are not used directly here (no set operations are defined), but they are required when you create a PKI user (an administrator that FortiWeb authorizes based on his certificate) on the FortiWeb. For details, see [user pki-user on page 406](#).

For information about certificate-based Web UI login, see the *FortiWeb Administration Guide*:

<http://docs.fortinet.com/fortiweb/admin-guides>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For details, see [Permissions on page 46](#).

Syntax

```
show system admin-certificate ca
```

Example

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

system admin-certificate intermediate-ca

If the certificate you are applying for HTTPS access to FortiWeb's GUI management is signed by several intermediate CAs, you need to import all the intermediate CA certificates of the certificate chain. FortiWeb will then send the intermediate CA certificates together with the server certificate when administrators access FortiWeb's GUI via HTTPS.

Intermediate CAs must belong to a group in order to be selected in a certificate verification rule. For how to add the intermediate certificates in a group, see [system admin-certificate intermediate-ca-group](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For details, see [system accprofile on page 220](#)

Syntax

```
config system admin-certificate intermediate-ca
  edit "<certificate_name>"
    set certificate "<certificate_str>"
  next
end
```

Variable	Description	Default
"<certificate_name>"	Enter the name of a certificate file. The maximum length is 63 characters.	No default.
certificate "<certificate_str>"	Set the certificate. Only certificates in PEM format may be set.	No default.

Example

This example adds a certificate to `Inter_Cert_1`

```
config system certificate intermediate-certificate
edit "Inter_Cert_1"
set certificate "-----BEGIN CERTIFICATE-----
MIIDKjCCAnoCCQCbXq6VYR1CiJANBgkqhkiG9w0BAQUFADCBiJELMAkGA1UEBhMC
SU4xEjAQBgNVBAgMCUthcm5hdGFrYTESMBAGA1UEBwwJQmFuZ2Fsb3JlMREwDwYD
VQQKDAhGb3J0aW5ldDEMAAoGA1UECwwdTEFECMQ0wCwYDVQQDDAR0ZXN0MSMwIQYJ
KoZIhvcNAQkBFhRzdXBwb3J0QGGZvcnRpbmV0LmNvbTAeFw0xMjEyMDUxMDE1NTla
Fw0xNDEyMDUxMDE1NTlaMIGKMQswCQYDVQQGEwJJTjESMBAGA1UECAwJS2FybmF0
YWthMRIwEAYDVQQHDA1CYW5nYWxvcnUxETAPBgNVBAoMCEZvcnRpbmV0MQwwCgYD
VQQLDANMQUIxDTALBgNVBAMMBHRlc3QxIzAhBgkqhkiG9w0BCQEFW1cHBvcnRA
Zm9ydGluZXQuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArvHH
eXZJilTr4TbH/505jFxKQ5dILr/561JOJ5UZWtgs9VhXSuCzmrs6FX35vyc7NR+9
tCbMr17qA68MxBMuu6phf2r77M9bsp3rOZE2nFR+lhjpWrXBk7/puFLBbI2yqh8d
7DB25m5pIOClmbdJ5GG1c/1wHULQhFQSYCMSVjc34esvaLE8oAVFWHAZX14dbAbj
gC4CMBayzJZaYefh/7suMwvdwS3sYjOwZYq6DFEF5ZPpKN+j9J+8EmAvaZS2m3M
fFdPff4eEAgSzmYasqxH7s4Ksc2zTm3cG5srRCqEsEddhobl1lJvmApoN2JiNiYJ
hYiEPyJdf2z+dAdwXwIDAQABMA0GCSqGSIb3DQEBBQUAA4IBAQCba8kKwVRPri/d
L8okLny6FygJ0auPbuRQCUGAWpfdKdXn6iyM1LuR066j82o2yrQ0ddgRcdaExt0I
RCoc2NqhzZvy8JJW2A+KTXutwdGGg8ckHQ5UVRtNo/1PZ6Quz8AsswzNk2Qx6OtF
FcTEBNxVTHKAbQR46ChIa3sG032WiuJ6Y2Rv77mTmmDRZnrY8QGZd2zMm3riAqUf
IGil0/yg0AhA+ZBt5rer3X+GTknhdAPJ+yU2WS1c8pPj3A3DI0+xwTOq/sNCqTmc
xb7Q1VM/1kioE9YaPasAJuQ7WHmnd8J0vHw1/e+whf/lsKxV0ClBNL/JdlyNAMvy
isnZYL58
-----END CERTIFICATE-----"
next
end
```

Related topics

- [system admin-certificate intermediate-ca-group](#)

system admin-certificate intermediate-ca-group

Use this command to group intermediate CA certificates for HTTPS access to FortiWeb's GUI management.

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 details, see [Permissions on page 46](#).

Syntax

```
config system admin-certificate intermediate-ca-group
edit "<admin_intermediate-ca-group_name>"
config members
edit <admin_intermediate-ca_index>
set name "<admin_intermediate_ca_name>"
next
end
next
end
```

Variable	Description	Default
"<admin_intermediate-ca-group_name>"	Enter the name of an admin intermediate certificate authority (CA) group. The maximum length is 63 characters.	No default.
<admin_intermediate-ca_index>	Enter the index number of an admin intermediate CA within its group. The valid range is 1–9,999,999,999,999,999.	No default.
name "<admin_intermediate_ca_name>"	Enter the name of a previously uploaded admin intermediate CA certificate. The maximum length is 63 characters. See system admin-certificate intermediate-ca .	No default.

Related topics

- [system admin-certificate intermediate-ca](#)

system admin-certificate local

The FortiWeb appliance presents its own HTTPS server certificate for secure connections (HTTPS) to its Web UI. By default, A Fortinet factory certificate is used as the certificate, which is named `defaultcert` in FortiWeb. You can also import other certifications to FortiWeb and replace the `defaultcert` with any of them for secure Web UI connections.

Use this command to edit the comment associated with the these FortiWeb's administration certificates that are stored locally on the FortiWeb appliance.

To replace the certificate that FortiWeb uses for the secure accesses to its Web UI, see .

For information on how to upload a certificate file to change FortiWeb's default certificate, see the *FortiWeb Administration Guide*:

<http://docs.fortinet.com/fortiweb/admin-guides>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system admin-certificate local
  edit "<certificate_name>"
    set comment "<comment_str>"
    set certificate "<certificate_str>"
    set passwd "<passwd_str>"
    set private-key "<private-key_str>"
    set flag 0
    set status ok
    set type certificate
  next
end
```

Variable	Description	Default
"<certificate_name>"	Enter the name of a certificate file. The maximum length is 63 characters.	No default.
comment "<comment_str>"	Enter 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.
certificate "<certificate_str>"	Enter the sequence number of the certificate file.	No default.
passwd "<passwd_str>"	When exporting the private key file from certificate factories, you can choose to enter a password to encrypt the file. Thus when you import the file into FortiWeb, you shall enter this password. This is optional.	No default.
private-key "<private-key_str>"	Enter the sequence number of the key file.	No default.
flag 0	Indicate if a password was saved. This is used by FortiWeb for backwards compatibility.	0
status ok	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, see . - pending—Indicates that the certificate request was generated, but must be downloaded, signed, and imported before it can be used as a local certificate.	ok
type certificate	Indicates whether the file is a certificate or a certificate signing request (CSR).	certificate

Example

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

```
config system admin-certificate local
  edit "certificate1"
    set comment "This is a certificate that FortiWeb uses for secure Web UI connections."
  next
end
```

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 details, see [Permissions on page 46](#).

Syntax

```
config system advanced
  set circulate-url-decode {enable | disable}
  set decoding-enhancement {enable | disable}
  set max-cache-size <cache_int>
  set max-dlp-cache-size <percentage_int>
  set max-dos-alert-interval <seconds_int>
  set share-ip {enable | disable}
  set anypktstream {enable | disable}
  set max-bot-alert-interval <interval_int> on page 234
  set ignore-undefined-query-param {enable | disable}
  set key-attr {enable | disable}
  set key-max-length <int>
  set key-printable {enable | disable}
  set owasp-top10-compliance {enable | disable}
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 <code>A</code> that is encoded as either <code>%41</code>, <code>%x41</code>, <code>%u0041</code>, or <code>\t41</code>.	enable

Variable	Description	Default
	Disable to decode only one level's worth of the URL, if encoded.	
decoding-enhancement {enable disable}	Enable to decode cookies and parameters using base64 or CSS for specified URLs. To configure decoding enhancement, see system decoding enhancement on page 277 .	disable
max-cache-size <cache_int>	Type the maximum size (in KB) of the body of the HTTP response from the web server that FortiWeb will cache per URL for body compression, decompression, rewriting, and XML detection. Increasing the body cache may decrease performance. Valid values range from 32 to 10240. The default value is 64. Increasing the body cache may decrease performance.	512
max-dlp-cache-size <percentage_int>	Type the maximum percentage of max-cache-size <cache_int> on page 234 —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
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, see system ip-detection on page 351 . Enabling this option is required for features that have a separate threshold for shared IP addresses. 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
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
max-bot-alert-interval <interval_int>	Type the maximum amount of interval time that FortiWeb will send an attack log during a bot attack. The valid range is 0-300 seconds.	60

Variable	Description	Default
ignore-undefined-query-param {enable disable}	Enable to bypass undefined query parameters in policies.	disable
key-attr {enable disable}	Requests with certain content types, such as PDF, tend to have extremely long parameter names or non-printable characters. While these characteristics are legitimate, they are prone to triggering signatures, resulting in unnecessary resource consumption and numerous false positives. To avoid such situations, you can enable <code>key-attr</code>. This feature allows requests with extremely long parameter names or non-printable characters to bypass scanning and be directly forwarded to the back-end server. However, it's important to note that in certain content types listed below, an unusually long parameter name or non-printable characters can actually be an indicator of attacks. In these cases, FortiWeb will conduct a security scan on requests with these content types, regardless of the <code>key-attr</code> settings. Additionally, if the <code>content-type</code> header is absent, the request will be treated as high-risk, prompting a security scan as well. • multipart • soap+xml • text/xml, application/xml,application/vnd.syncml+xml, application/vnd.ms-sync.wbxml • multipart/form-data (boundary is required) • text/html • application/x-www-form-urlencoded • text/plain • text/css • application/x-javascript • multipart/x-mixed-replace • application/javascript • text/javascript • application/rss+xml • message/HTTP • application/json, text/json • all other application/...xml	disable
key-max-length <int>	If the parameter name exceeds the max length value you have specified, FortiWeb will skip the security check and directly pass it on to the back-end server. The valid range is 1-1,024.	1024

Variable	Description	Default
key-printable {enable disable}	If this option is enabled, all the characters in the parameter name must be printable. Otherwise FortiWeb will skip the security check and directly pass it on to the back-end server. If this option is disabled, regardless whether the characters in the parameter name is printable or not, it should be proceeded for security check.	disable
owasp-top10-compliance {enable disable}	Enable this option so that the OWASP Top10 Compliance dashboard will display as one of the monitors in Dashboard. It provides visibility into the level of security your applications have in terms of protection from OWASP (Open Web Application Security Project) vulnerabilities.	disable

Related topics

- [server-policy policy on page 150](#)
- [system certificate local on page 258](#)
- [system ip-detection on page 351](#)
- [waf application-layer-dos-prevention on page 440](#)
- [waf HTTP-protocol-parameter-restriction on page 543](#)

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 details, see [Permissions on page 46](#).

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>
    set use-fsa {enable | disable}
end
```

Variable	Description	Default
default-db {basic extended}	Select which of the antivirus signature databases to use when scanning HTTP POST requests for viruses, either:	basic

Variable	Description	Default
	<code>basic</code>—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. <code>extended</code>—Select to use all signatures, regardless of whether the viruses or greyware are currently spreading.	
<code>scan-bzip2 {enable disable}</code>	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.	<code>enable</code>
<code>uncomp-size-limit <limit_int></code>	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. For details, see "waf file-uncompress-rule" on page 1. 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 waf HTTP-protocol-parameter-restriction on page 543. To be sure that it will not disrupt normal traffic, first configure <code>action</code> to be <code>alert</code>. If no problems occur, switch it to <code>alert_deny</code>. The maximum acceptable values are: 102400 KB: FortiWeb 100D, 100E, 100F, 400C, 400D, 400E, 400F, 600D, 600E, 600F, 1000C, 3000CFsx, 4000C 204800 KB: FortiWeb 1000D, 2000D, 3000D, 3000DFsx, 4000D, 1000E, 2000E, 3010E, 1000F, 2000F 358400 KB: FortiWeb 3000E, 4000E, 3000F, 4000F	5000
<code>uncomp-nest-limit <limit_int></code>	Type the maximum number of allowed levels of compression ("nesting") that FortiWeb will attempt to decompress.	12
<code>use-fsa {enable disable}</code>	Enable to use the Signature Database from FortiSandbox to supplement the AV Signature Database. If enabled, FortiWeb will download the malware package from FortiSandbox's Signature Database every minute.	<code>disable</code>

system automation-email

Use this command to configure the email notification settings in the Automation feature.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system automation-email
  edit <email_name>
    set subject <string>
    set body <string>
    set email-policy <email_policy_name>
  next
end
```

Variable	Description	Default
<email_name>	Enter the name of the email. You can reference it in a stitch.	No default.
subject <string>	Enter the subject of the email to be sent.	No default.
body <string>	Enter the email body. Simple string and two parameters are supported: 1. %%log%%: All fields from the log event triggering this stitch. 2. %%results%%: The complete result from previous action, such as CLI script.	No default.

Related topics

- [system automation-script on page 238](#)
- [system automation-trigger on page 239](#)
- [system automation-stitch on page 240](#)

system automation-script

Use this command to configure the CLI commands to be run in the Automation feature.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system automation-script
  edit <script_name>
    set script "<Cli_1>"
    set script "<Cli_2>"
```

```
next
end
```

Variable	Description	Default
<script_name>	Enable to override the default list of FDN servers, and connect to a specific server.	No default.
script "<cli>"	Enter the CLI commands to be run when certain trigger occurs. You can enter multiple CLI command lines.	No default.

Related topics

- [system automation-trigger on page 239](#)
- [system automation-stitch on page 240](#)
- [system automation-email on page 237](#)

system automation-trigger

Use this command to configure the triggers in the Automation feature.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system automation-trigger
  edit <trigger_name>
    set comments <string>
    set trigger-type event_based
    set event-type {high-cpu | event-log | reboot | HA}
    set logid <int>
    config fields
      edit <index>
        set name <string>
        set value <string>
      next
    end
  next
end
```

Variable	Description	Default
<trigger_name>	Enter a name for the trigger.	No default.

Variable	Description	Default
comments <string>	Enter a description for the trigger.	No default.
trigger-type event_based	Now we only support event_based trigger.	event_based
set event-type {high-cpu event-log reboot HA}	Select the type of the event for the trigger. FortiWeb will take action when the specified event occurs. - high-cpu: Available memory is less than 100 MB. - event-log: The system prints certain even logs. - reboot: The system reboots. - HA: HA fail-over occurs.	No default.
If the event-type is event-log, define the following parameters:		
logid	Enter the id of the event log.	No default.
<index>	Enter the index of the filter to filter out specific event logs.	No default.
name <string>	The name of the log field to be used to filter out certain logs.	No default.
value <string>	The value of the log field to be used to filter out certain logs.	No default.

Related topics

system automation-stitch

Use this command to configure the stitch in the Automation feature.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system automation-stitch
edit <stitch_name>
    set status {disable | enable}
    set action_interval <int>
    set comments <string>
    set trigger <trigger_name>
```



```

config actions
  edit "email"
    set type email
    set email-name <string>
    set delay 1
  next
  edit "script"
    set type script
    set script-name <string>
    set delay 0
  next
end
next
end

```

Variable	Description	Default
status {enable disable}	Select whether to enable or disable this stitch.	disable
action_interval <int>	Specify the interval time to execute each action.	3 (seconds)
comments <string>	Enter a description for the stitch.	No default.
trigger <trigger_name>	The name of the trigger you have defined by <code>config system automation-trigger</code> .	No default.
email-name <string>	The name of the email action you have defined by <code>config system automation-email</code> .	No default.
script-name <string>	The name of the script action you have defined by <code>config system automation-script</code> .	No default.

Related topics

- [system automation-email on page 237](#)
- [system automation-script on page 238](#)
- [system automation-trigger on page 239](#)

system autoupdate override

Use this command to override the default Fortiguard Distribution Server (FDS) and update FortiGuard services from the specified address.

If you cannot connect to the FortiGuard Distribution Network (FDN) or if your organization provides updates using their own FortiGuard server, you can specify the IP address of the FDS server 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 details, see [Permissions on page 46](#).

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>"}	Enter either the IP address or fully qualified domain name (FQDN) of the FDS override. If you connect with a FortiWeb device who is acting as an FDS proxy, you should enter port number 8989 after the IP address.	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

- [system autoupdate schedule on page 242](#)

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:

<http://docs.fortinet.com/fortiweb/admin-guides>

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 enter [system autoupdate override on page 241](#). If your FortiWeb appliance must connect through a web proxy, you must also enter [system autoupdate tunneling on page 244](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For details, see [Permissions on page 46](#).

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.	enable
frequency {daily every weekly}	Select the frequency with which the FortiWeb appliance will request signature updates.	every
time "<time_str>"	Enter the time at which the FortiWeb appliance will request signature updates. The time format is <code>hh:mm</code> , where: <code>hh</code> is the hour according to a 24-hour clock <code>mm</code> 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 <code>frequency</code> is <code>weekly</code> .	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

- [system autoupdate override on page 241](#)
- [system autoupdate tunneling on page 244](#)

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 (<http://tools.ietf.org/rfc/rfc2616.txt>).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

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>"}	Enter 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>	Enter the port number on which the web proxy listens for connections. The valid range is 0–65,535.	0
username "<proxy-user_str>"	If the proxy requires authentication, enter 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, enter 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

- [system autoupdate schedule on page 242](#)

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 [backup full-config on page 822](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system backup
edit "<backup_name>"
    set config-type {full-config | cli-config | waf-config}
    set ml-flag {disable | enable}
    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>"	Enter the name of the backup configuration. The maximum length is 59 characters. To display the list of existing backups, enter:	No default.

Variable	Description	Default
	edit ?	
config-type {full-config cli-config waf-config}	Select either: <code>full-config</code> — Include both the configuration file and other uploaded files, such as certificate and error page files, in the backup. <code>cli-config</code> — Include only the configuration file in the backup. <code>waf-config</code> — Include only the web protection profiles in the backup.	cli-config
ml-flag {disable enable}	Enable to include machine leaning data in the backup. This option takes effect only when the <code>config-type</code> is set to <code>full-config</code> .	disable
encryption {enable disable}	Enable to encrypt the backup file with a <code>.zip</code> extension. 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>"	Enter the password that will be used to encrypt the backup file. This field appears only if you enable encryption {enable disable} on page 246.	No default.
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>" on page 246 and ftp-passwd "<password_str>" on page 246. Disable for FTP servers that allow anonymous uploads.	disable
ftp-user "<user_str>"	Enter 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 {enable disable} on page 246 is <code>enable</code>.	No default.
ftp-passwd "<password_str>"	Enter 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 {enable disable} on page 246 is <code>enable</code>.	No default.
ftp-dir "<directory-path_str>"	Enter 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>"}	Enter 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: <code>now</code>—Use this to initiate the FTP backup immediately upon ending the command sequence. <code>days</code>—Enter this to allow you to set days and a time to run the backup automatically. You must also configure schedule_days {sun mon tue wed thu fri sat} on page 247 and schedule_time "<time_str>" on page 247	now
schedule_days {sun mon tue wed thu fri sat}	Enter 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, enter: <pre>set schedule_days mon, fri</pre> This command is available only if schedule_type {now days} on page 247 is <code>days</code> .	No default.
schedule_time "<time_str>"	Enter the time of day to run the backup. The time format is <code>hh:mm</code> , where: <code>hh</code> is the hour according to a 24-hour clock <code>mm</code> is the minute This command is available only if schedule_type {now days} on page 247 is <code>days</code> .	00:00

Related topics

- [restore config on page 848](#)
- [backup cli-config on page 821](#)

system captcha

Use this command to specify difficulty levels "easy/medium/hard" of CAPTCHA challenge.

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

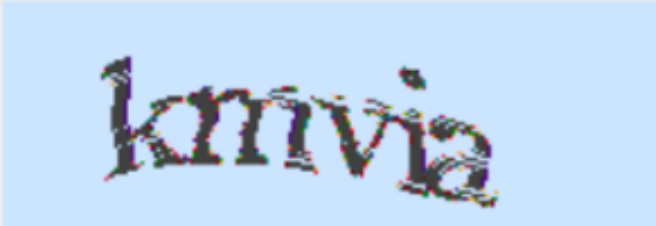
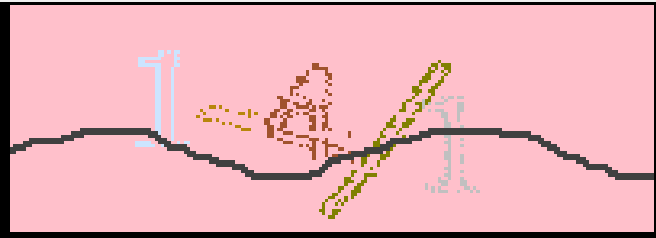
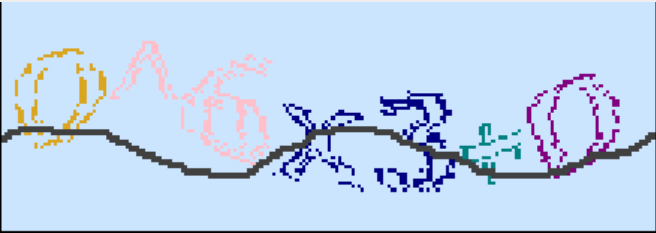
Syntax

```
config system captcha
```

```

set captcha-difficulty-level {easy | medium | hard}
end

```

Variable	Description	Default
captcha-difficulty-level {easy medium hard}	Specify different levels "easy/medium/hard" of CAPTCHA challenge. Below are examples of the easy/medium/hard level challenges. Easy (simple letters, no operators):  Medium (default mode) (3 operands, add/subtract/multiply/divide result between -100 ~ 100):  Hard (add/subtract/multiply/divide/power): 	medium

system central-management

Use this command to enable cross domain access feature for central management in the web UI and CLI.

Syntax

```

config system central management
set cm-access {enable | disable}
set system central-management
end

```


Variable	Description	Default
cm-access {enable disable}	Enable/disable the cross domain access feature for central management.	disable
system central-management	Enter the URL to access FortiWeb Manager.	disable

Example

This example shows enabling central management feature.

```
config system central-management
  set cm-access enable
  set allow-origin https://10.200.111.100
end
```

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 [system certificate ca-group on page 251](#).

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

<http://docs.fortinet.com/fortiweb/admin-guides>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For details, see [Permissions on page 46](#).

Syntax

```
show system certificate ca
config system certificate ca
  edit "<certificate_name>"
    set certificate "<certificate_str>"
  next
end
```

Variable	Description	Default
"<certificate_name>"	Enter the name of a certificate file. The maximum length is 63 characters.	No default.

Variable	Description	Default
certificate "<certificate_str>"	Set the certificate. Only certificates in PEM format may be set.	No default.

Example

This example creates two CA certificate items, CA_Cert_1 and CA_Cert_2.

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

This example adds a certificate to CA_Cert_1

```
config system certificate local
  edit "CA_Cert_1"
  set certificate "-----BEGIN CERTIFICATE-----
MIIDKjCCAnoCCQCbXq6VYRlCijANBgkqhkiG9w0BAQUFADCBIjELMAkGA1UEBhMC
SU4xEjAQBgNVBAgMCUthcm5hdGFrYTESMBAGA1UEBwwJQmFuZ2Fsb3JlMREwDwYD
VQQKDAhGb3J0aW5ldDEMMAoGA1UECwwdTEFCMQ0wCwYDVQQDDAR0ZXN0MSMwIQYJ
KoZlIhvcNAQkBFhRzdXBwb3J0QGZvcnRpbmV0LmNvbTAeFw0xMjEyMDUxMDE1NTla
Fw0xNDEyMDUxMDE1NTlaMIGKMQswCQYDVQQGEWJTTjESMBAGA1UECAwJS2FybmF0
YWthMRIwEAYDVQQHDA1CYW5nYWxvcmluXETAPBgNVBAoMCEZvcnRpbmV0MQwwCgYD
VQQLDANMQUIxDTALBgNVBAMMBHRlc3QxIzAhBgkqhkiG9w0BCQEFHFN1cHBvcnRA
Zm9ydGluZXQuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArvHH
eXZJilTr4TbH/5O5jFkKQ5dILr/561JOJ5UZWtgs9VhXSuCzmrs6FX35vyc7NR+9
tCbMr17qA68MxBMu6phf2r77M9bsp3rOZE2nFR+lhjpWrXBk7/puFLBbI2yqh8d
7DB25m5pIOClmbdJ5GGlc/1wHULQhFQSYCMSVjc34esvaLE8oAVFWHAZX14dbAbj
gC4CMBayzJZaYEfh/7suMwvdwS3sYjOwZYq6DFEF5ZPpKN+j9J+8EmAvaZS2m3M
fFdPFf4eEAgsHmYasqxH7s4Ksc2zTm3cG5srRCqEsEddhoblI1JvmApoN2JiNiYJ
hyiEPyJdf2z+dADwXwIDAQABMA0GCSqGSIB3DQEBBQUAA4IBAQCbA8kKwVRPri/d
L8okLny6FygJ0auPbuRQCUGAWpfdKdXn6iyMlLuR066j82o2yrQ0ddgRcdaExt0I
RCoc2NqhzZvy8JJW2A+KTXutwdGGg8ckHQ5UVRtNo/1PZ6Quz8AsswzNk2Qx6OtF
FcTEBNxVTHKabQR46ChIa3sG032WiuJ6Y2Rv77mTmmDRZnrY8QGZd2zMM3riAqUf
IGil0/yg0AhA+ZBt5rer3X+GTknhdAPJ+yU2WS1c8pPj3A3DI0+xwTOq/sNCqTmc
xb7Q1VM/1kiOE9YaPasAJuQ7WHmnd8J0vHw1/e+whf/lsKxV0ClBNL/JdlyNAMvy
isnZYL58
-----END CERTIFICATE-----"
  next
end
```

Related topics

- [system certificate ca-group on page 251](#)
- [system certificate verify on page 269](#)

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 details, see [Permissions on page 46](#).

Syntax

```
config system certificate ca-group
edit "<ca-group_name>"
    config members
    edit <ca_index>
        set type {CA | TSL}
        set publish-dn {enable | disable}
        set tsl "<tsl_name>"
        set name "<ca_name>"
        set trust-anchor {enable | disable}
    next
end
next
end
```

Variable	Description	Default
"<ca-group_name>"	Enter the name of a certificate authority (CA) group. The maximum length is 63 characters.	No default.
<ca_index>	Enter the index number of a CA within its group. The valid range is 1–999,999,999,999,999.	No default.
name "<ca_name>"	Enter the name of a previously uploaded CA certificate.	No default.
type {CA TSL}	Select to upload CA certificate or TSL.	CA
tsl "<tsl_name>"	Enter the name of a TSL.	No default.
publish-dn {enable disable}	Enable to list only certificates related to the specified CA Group. This is beneficial when a client installs many certificates in its browser or when apps don't list client certificates. If you enable this option, also enable the option in a certificate verification rule. For details, see system certificate verify on page 269 .	enable
trust-anchor {enable disable}	If <code>partial-chain</code> is enabled in <code>config system certificate verify</code> , you need to enable <code>trust anchor</code> for the system to perform partial chain verification.	disable

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

- [certificate ca on page 1](#)
- [system certificate local on page 258](#)
- [system certificate verify on page 269](#)

system certificate crt

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:

<http://docs.fortinet.com/fortiweb/admin-guides>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system certificate crt
  edit "<crl_name>"
    set certificate "<certificate_str>"
    set type {HTTP | local | scep}
    set url "<crl_str>"
  next
end
```

Variable	Description	Default
"<crl_name>"	Enter the name of a CRL. The maximum length is 63 characters.	No default.
certificate "<certificate_str>"	Set the certificate. Only certificates in PEM format may be set.	No default.
type {HTTP local scep}	Specify how you set the certificate. HTTP—query for the certificate from a HTTP server local—set the certificate through certificate <certificate_str_pem>. scep—query for the certificate from a SCEP server	local
url "<crl_str>"	If type {HTTP local scep} on page 253 is set as HTTP or scep, enter the URL of the certificate. The maximum length is 127 characters.	No default.

Related topics

- [certificate ca on page 1](#)
- [system certificate local on page 258](#)
- [system certificate crl-group on page 253](#)
- [system certificate verify on page 269](#)

system certificate crl-group

Use this command to create a group of CRLs that you have already uploaded to FortiWeb.

To ensure that FortiWeb validates only certificates that have not been revoked, you should periodically upload current certificate revocation lists (CRL) that may be provided by certificate authorities (CA). Once you've uploaded the CRL(s) you want to use, create CRL groups to include in your FortiWeb configuration.

For more information about CRLs and CRL groups, see the *FortiWeb Administration Guide*:

<http://docs.fortinet.com/fortiweb/admin-guides>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system certificate crl-group
  edit <crl_group_name>
    config members
      edit <entry_index>
        set <crl_name>
      next
    next
  end
```

```
next
end
```

Variable	Description	Default
<crl_group_name>	Type the name of the CRL group. You will use this name to select the CRL group in other parts of the configuration. The maximum length is 63 characters.	No default.
<entry_index>	Type the index number of the individual entry in the table.	No default.
<crl_name>	Type the name of a CRL that you want to include in the group. The maximum length is 63 characters. For details, see system certificate crl on page 252 .	No default.

Related topics

- [system certificate crl on page 252](#)
- [system certificate verify on page 269](#)

system certificate intermediate-certificate

Use this command to upload the names of uploaded intermediate CA certificate.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system certificate intermediate-certificate
edit "<certificate_name>"
    set certificate "<certificate_str>"
next
end
```

Variable	Description	Default
"<certificate_name>"	Enter the name of a certificate file. The maximum length is 63 characters.	No default.
certificate "<certificate_str>"	Set the certificate. Only certificates in PEM format may be set.	No default.

Example

This example creates three intermediate certificate items, Inter_Cert_1, Inter_Cert_2 and Inter_Cert_3.

```
config system certificate intermediate-certificate
  edit "Inter_Cert_1"
  next
  edit "Inter_Cert_2"
  next
  edit "Inter_Cert_3"
  next
end
```

This example adds a certificate to Inter_Cert_1

```
config system certificate local
  edit "Inter_Cert_1"
  set certificate "-----BEGIN CERTIFICATE-----
MIIDkjCCAnoCCQCbXq6VYR1CijANBgkqhkiG9w0BAQUFADCBiJELMAkGA1UEBhMC
SU4xEjAQBGNVBAGMCUthcm5hdGFrYTESMBAGA1UEBwwJQmFuZ2Fsb3JlMREwDwYD
VQKDAhG3J0aW5ldDEMAAoGA1UECwwdTEFECMQ0wCwYDVQDDAR0ZXN0MSMwIQYJ
KoZIhvcNAQkBFhRzdXBwb3J0QGGZvcnRpbmV0LmNvbTAeFw0xMjEyMDUxMDE1NTla
Fw0xNDEyMDUxMDE1NTlaMIGKMQswCQYDVQGEwJJTjESMBAGA1UECAwJS2FybmF0
YWthMRIwEAYDVQQHDA1CYW5nYWxvcmluZS5ETAPBgNVBAoMCEZvcnRpbmV0MQwwCgYD
VQQLDANMQUIxDTALBgNVBAMMBHRlc3QxIzAhBgkqhkiG9w0BCQEFwFHNlcHBvcnRA
Zm9ydGluZXQuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArvHH
eXZJilTr4TbH/505jFxBKQ5dILr/561JOJ5UZWtgs9VhXSuzCzmrs6FX35vyc7NR+9
tCbMr17qA68MxBMu6phf2r77M9bsp3rOZE2nFR+lhjpWrXBk7/puFLBbI2yqh8d
7DB25m5pI0ClmbdJ5GG1c/1wHULQhFQSYCMSVjc34esvaLE8oAVFWHAZX14dbAbj
gC4CMBayzJZaYEFh/7suMwvdwS3sYjOwZYq6DFEF5ZPpKN+jj9J+8EmAvaZS2m3M
fFdPFf4eEAgSzmYasqxH7s4Ksc2zTm3cG5srRCqEsEddhobl1lJvMApoN2JiNiYJ
hYiEPyJdf2z+dADwXwIDAQABMA0GCSqGSIb3DQEBAQUAA4IBAQCBA8kKwVRPri/d
L8okLny6FygJ0auPbuRQCUGAWpfdKdXn6iyM1LuR066j82o2yrQ0ddgRcdaExt0I
RCoc2NqhzZvy8JJW2A+KTXutwdGGg8ckHQ5UVRtNo/1PZ6Quz8AsswzNk2Qx6OtF
FcTEBNxVTHKABQR46ChIa3sG032WiuJ6Y2Rv77mTmmDRZnrY8QGZd2zmm3riaqUf
IGil0/yg0AhA+ZBt5rer3X+GTknhdAPJ+yU2WS1c8pPj3A3DI0+xwTOq/sNCqTmc
xb7Q1VM/1kioE9YaPasAJuQ7WHmnd8J0vHw1/e+whf/lsKxV0ClBNL/JdlyNAMvy
isnZYL58
-----END CERTIFICATE-----"
  next
end
```

Related topics

- [certificate inter-ca on page 1](#)
- [system certificate intermediate-certificate-group on page 255](#)
- [server-policy policy on page 150](#)

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 details, see [Permissions on page 46](#).

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>"	Enter the name of an intermediate certificate authority (CA) group. The maximum length is 63 characters.	No default.
<intermediate-ca_index>	Enter the index number of an intermediate CA within its group. The valid range is 1–9,999,999,999,999,999.	No default.
name "<ca_name>"	Enter the name of a previously uploaded intermediate CA certificate. The maximum length is 63 characters.	No default.

Related topics

- [certificate inter-ca on page 1](#)
- [system certificate intermediate-certificate on page 254](#)
- [server-policy policy on page 150](#)

system certificate letsencrypt

Instead of uploading CA certificate from your local directory, an easier way is to configure FortiWeb to obtain a CA certificate from Let's encrypt on behalf of you.

It's recommended to configure Let's Encrypt certificate through Web UI, where more functions are offered. Refer to "Let's Encrypt certificates" in *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 details, see [Permissions on page 46](#).

Syntax

```
config system certificate letsencrypt
```



```

edit "<certificate_name>"
  set domain "<application_domain_name>" on page 257
  set renewal-period <int>
  set validation-method {HTTP-01 | TLS-ALPN-01 | DNS-01}
  set key-type {RSA-2048 | RSA-3072 | RSA-4096}
  config subject-alternative-names
    edit <index>
      set san-dns <domain_name>
    end
  end
next
end

```

Variable	Description	Default
"<certificate_name>"	Enter the name of a certificate file. The maximum length is 63 characters.	No default.
domain "<application_domain_name>"	Enter the domain name of your application. FortiWeb will then retrieve the CA certificate for this domain from Let's encrypt. For Let's encrypt certificate, it's supported to add up to 11 domains. One of them should be root domain, while the rest 10 should all belong to the root domain. It's recommended to enter the root domain here, then add the rest domain items in <code>san-dns <domain_name></code>.	No default.
renewal-period <int>	Set how soon FortiWeb obtains the TLS certificate from Let's Encrypt. The valid range is 1-60 days.	30 (days)
validation-method {HTTP-01 TLS-ALPN-01 DNS-01}	• HTTP-01: Let's Encrypt will send HTTP request to FortiWeb for validation. When in RP mode, you must select HTTP service and uses port 80 for it in the server policy which uses the Let's Encrypt certificate. When in TTP mode, the back-end server which uses Letsencrypt certificate should have port 80 enabled. Redirect HTTP to HTTPS should not be enabled when the validation is in process. • TLS-ALPN-01: This method allows Let's Encrypt to send HTTPS requests to FortiWeb for validation. You must select HTTPS service in the server policy which uses the Let's Encrypt certificate. • DNS-01: This method allows Let's Encrypt to do validation through your DNS provider. FortiWeb will generate a TXT record, then you need to add this TXT record to the DNS record. Refer to "Fulfilling the DNS-01 challenge" in <i>FortiWeb Administration Guide</i>.	HTTP-01

Variable	Description	Default
key-type {RSA-2048 RSA-3072 RSA-4096}	Select Key Type. RSA algorithm with different key length can be implemented and accepted by the Let's Encrypt Server. Those key sizes are 2048, 3072, and 4096 bits. Please note that larger keys consume more computing resources, however, achieve better security.	RSA-2048
san-dns <domain_name>	Enter domain names. Up to 10 items can be added and they all should belong to the same domain.	No default.

Related topics

- [system certificate ca on page 249](#)
- [system certificate ca-group on page 251](#)
- [system certificate verify on page 269](#)

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 details about HSM integration, see [system hsm info on page 340](#) and the FortiWeb Administration Guide:

<http://docs.fortinet.com/fortiweb/admin-guides>

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's 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:

<http://docs.fortinet.com/fortiweb/admin-guides>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system certificate local
edit "<certificate_name>"
    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>"
    set certificate "<certificate_str>"
    set private-key "<private_key_str>"
    set passwd "<password>"
next
end
```

Variable	Description	Default
"<certificate_name>"	Enter the name of a certificate file. The maximum length is 63 characters.	No default.
comment "<comment_str>"	Enter 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}	Indicate the status of an imported certificate: <code>na</code>—Indicates that the certificate was successfully imported, and is currently selected for use by the FortiWeb appliance. <code>ok</code>—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. <code>pending</code>—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}	Indicate whether the file is a certificate or a certificate signing request (CSR).	No default.
flag {0 1}	Indicate if a password was saved. This is used by FortiWeb for backwards compatibility.	No default.
is-hsm {no yes}	Specify whether you configured the CSR for this certificate to work with an integrated HSM.	no

Variable	Description	Default
partition-number "<partition_name>"	Enter the name of the HSM partition you selected when you created the CSR for this certificate.	No default.
certificate "<certificate_str>"	Set the certificate. Only certificates in PEM format may be set.	No default.
private-key "<private_key_str>"	Set the private key for the certificate. Only private keys in PEM format may be set.	No default.
passwd "<password>"	Enter the password for the 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
```

This example adds a certificate named `certificate2`

```
config system certificate local
  edit "certificate2"
    set private-key "-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,82EAF556E3621A07
ZYqcytKrfYgksrp/6rFf4Ma3rIiW/63EiyxHFLS18NVOLFm+AWHYm5flnKJI4Ava
iZnv64Q1mLxTSDgU+/rS9XBADlg6DKoIDtDTlVvg99vU3I9TrU+LRMPaLCidVw/h
GMlKtvF8UGFACAM1HwTJ/zBejgaAN0ZKcmxDNX0RwGHQwTP1/dwXRae+uk9dK8Ya
kw9jcu5SM7aQuUKEFDvdKhI9fo8uMH81KwSViaDx50/BZfEQx5+cRHooS/AZfnnr
BjBlaAZA+zjuvp5mbDh76CO8+i+++09e4g5Kj83ZoRfVXkoUonfRug5FvAT7YFEi
lgnG+ChW5BrDtOq25Y4jQcPyqM9dL81kpMhfK+rayGWVyOfQAX0AtNNM0itbjb7U
m78N71RVjjz4We2QCKIBv5AibsPgJwq54M6VDZ3CIJ+f2QVvvyppN2UjVlepih6N
yS0RxVqwC2HOwbdbffvImJhla5AOSIFnEYHOAwAxIf3nlZWAf1HhW8Oc6IofqTuO
R5SeWnoYxFVFakhGcyMRw3sd/ekTp8tRoK8QbINn3L38AEMtp8HKSHWm+MWdIQeK
WNYW4AZsrKfmXIQpGzuaan50fh6y6eVevxB9zx/uVN2XxD/TmDs5KnLjw7A4ks7V
Ds0c8bSLOT8BE+qfb7I/mUjVbsbGxgX40ducmm/C7HR/bgbSV2u6PK92ieQ22q6q
7RATzFtvHuJ3OmJtrMKhlHGMHVSA01GhheL3m2JhHMKMoJfwhYLab1+UCV4n5GOi
MogQY9UQ022WRCTpTPes5S15IMVY/Oj1nP/QcUMK8a7iPtAZWPYN7HEPXDfU/Urm
52HbC0fSQ/eGG5gQ7kDy9N/aLZf9wDMGj5zjX2lmmMT/h1sD29+bUCoo4ODT2Kk1
i6HyZX+J6KNDYM5aNOdhyZabVZBZOu1GvtLMzzrd5pEugFs7Rzt0+NJ54d7jGgav
0QwKCKIDevSdZG0ZexLTVqONF9Pzo6i/E3uwIKuHFAnTatq6UrKveRLtWWXuSBim
AAifL8s23T0BJAa75C6b3+f5IUTC/K9e5vrUbBDWDsjSjsWgbkoPBD1EpWLI+Ogu
Th6nZeQx0U+gt1bC+bJTIKdVDbxgjVGXIEvmnzc7KU0cBHmMIQggqfQwdVTeSVUx
z9JefVD9accpoem6ghds/0xaQztbdvb5NAM9LX2o/HFECThcLWGke/jxgAKvFQX4
MZBFy1UukQeCgHfWJCIMw1D/tupKwAqzsvm351E0C8eTuC10WFvtkzQNoFkyD2vS
gWSFKz85nswSMkobWFNjxMmDuS1Q1AHUFuzpcVOJgrE6DmpdYE3DeKmsVMsLsNM/
17H3SlnvEptVf3fm5PpCxtOM60nqsQuveHEgkkm5gt8CLtE8bV81yv7JDvkXUFV2
5HlFRZ/RZAQgAeKiAS6REwHuE/dEhZKh7Jq2o02G0NXeAXR/WqeN0SWSw0dEVf39
TMARg27X27zx0Wg2g8pBC1nxAlzyzMfYI2OTwvFZFNpVenGCVUw1dFt8eolAOscO
LakQuCWrfRw7kiRQlXvK/o67fKTkBvt7zM5WjBEO3beGWe2TkRUWUg==
```

```

-----END RSA PRIVATE KEY-----"
set certificate "-----BEGIN CERTIFICATE-----
MIIDKjCCAnoCCQCbXq6VYR1CiJANBgkqhkiG9w0BAQUFADCBijELMAkGA1UEBhMC
SU4xEjAQBGNVBAGMCUthcm5hdGFrYTESMBAGA1UEBwwJQmFuZ2Fsb3JlMREwDwYD
VQQKDAhGb3J0aW5ldDEMAAoGA1UECwwdTEFECMQ0wCwYDVQQDDAR0ZXN0MSMwIQYJ
KoZihvcNAQkBFhRzdXBwb3J0QGZvcnRpbmV0LmNvbTAeFw0xMjEyMDUxMDE1NTla
Fw0xNDEyMDUxMDE1NTlaMIGKMQswCQYDVQQGEWJTTjESMBAGA1UECAwJS2FybmF0
YWthMRIwEAYDVQQHDA1CYW5nYWxvcmluZS5ETAPBgNVBAoMCEZvcnRpbmV0MQwwCgYD
VQQLDANMQUIxDTALBgNVBAMMBHRlc3QxIzAhBgkqhkiG9w0BCQEFH1cHBvcnRA
Zm9ydGluZXQuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEARvHH
eXZJilTr4TbH/5O5jFxBKQ5dILr/561JOJ5UZWTgs9VhXSuCzmrs6FX35vyc7NR+9
tCbMr17qA68MxBMuu6phf2r77M9bsp3rOZE2nFR+lhjpWrXBk7/puFLBbI2yqh8d
7DB25m5pI0ClmbdJ5GG1c/1wHULQhFQSYCMSVjc34esvaLE8oAVFWHAZX14dbAbj
gC4CMBayzJZaYEFh/7suMwvdwS3sYjOwZYq6DFEF5ZPpKN+ji9J+8EmAvaZS2m3M
fFdPFf4eEAgSbmYasqxH7s4Ksc2zTm3cG5srRCqEsEddhobli1JvMApoN2JiNiYJ
hYiEPyJdf2z+dADwXwIDAQABMA0GCSqGSIb3DQEBAQUAA4IBAQCBA8kKwVRPri/d
L8okLny6FygJ0auPbuRQCUGAWpfdKdXn6iyM1LuR066j82o2yrQ0ddgRcdaExt0I
RCoC2NqhzZvy8JJW2A+KTXutwdGGg8ckHQ5UVRtNo/1PZ6Quz8AsswzNk2Qx6OtF
FcTEBNxVTHKAbQR46ChIa3sG032WiuJ6Y2Rv77mTmmDRZnrY8QGZd2zMm3riAqUf
IGil0/yg0AhA+ZBt5rer3X+GTknhdAPJ+yU2WS1c8pPj3A3DI0+xwTOq/sNCqTmc
xb7Q1VM/1kiOE9YaPasAJuQ7WHmnd8J0vHw1/e+whf/lsKxV0ClBNL/JdlyNAMvy
isnZYL58
-----END CERTIFICATE-----"
next
end

```

Related topics

- [server-policy policy on page 150](#)
- [server-policy server-pool on page 182](#)

system certificate multi-local

Use this command to configure RSA, DSA, and ECDSA certificates into multi-certificate, and reference them in server policy in Reverse Proxy mode and pserver in TTP or WCCP mode.

Syntax

```

config system certificate multi-local
edit "<certificate-multi-local_name>" on page 262
    set comment "<comment_str>" on page 262
    set rsa-cert <rsa-cert_str> on page 262
    set dsa-cert <dsa-cert_str> on page 262
    set ecc-cert <ecc-cert_str> on page 262
next
end

```

Variable	Description	Default
"<certificate-multi-local_name>"	Enter the name of a multi-certificate file.	No default.
comment "<comment_str>"	Enter a description or other comment.	No default.
rsa-cert <rsa-cert_str>	Select the RSA certificate created in system certificate local (page 1).	No default.
dsa-cert <dsa-cert_str>	Select the DSA certificate created in system certificate local (page 1).	No default.
ecc-cert <ecc-cert_str>	Select the ECDSA certificate created in system certificate local (page 1).	No default.

Related topics

- [system certificate local on page 258](#)
- [server-policy policy on page 150](#)
- [server-policy server-pool on page 182](#)

system certificate ocsf-stapling

Use this command to configure an OCSP server.

Once an OCSP server is configured, OCSP stapling is enabled. When OCSP stapling is enabled, FortiWeb periodically fetches the revocation status of the specified certificate from the OCSP server and caches the response for a period if the revocation status is contained in the response.

For more information on OCSP stapling, see the *FortiWeb Administration Guide*:

<http://docs.fortinet.com/fortiweb/admin-guides>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system certificate ocsf-stapling
  edit "<ocsp_name>"
    set certificate "<certificate_name>"
    set local-cert "<certificate_name>"
    set comment "<comment_str>"
    set ocsf_url "<url>"
  next
end
```

Variable	Description	Default
"<ocsp_name>"	Enter the name of an OCSP group. The maximum length is 63 characters.	No default
certificate "<certificate_name>"	A CA certificate that has been imported in FortiWeb.	No default
local-cert "<certificate_name>"	The local certificate of the server certificate to be queried.	No default
comment "<comment_str>"	Optionally, enter a comment for the OCSP group.	No default
ocsp_url "<url>"	Enter URL of the OCSP server corresponding to the specified CA certificate.	No default

Related topics

- [system certificate local on page 258](#)
- [system certificate ca on page 249](#)
- [server-policy policy on page 150](#)
- [server-policy server-pool on page 182](#)

system certificate server-certificate-verify

Use this command to configure how the FortiWeb appliance will verify certificates presented by HTTP server.

Syntax

```
config system certificate server-certificate-verify
edit "<certificate_verificator_name>"
    set ca "<ca-group_name>"
    set crl "<crl-group_name>"
next
end
```

Variable	Description	Default
"<certificate_verificator_name>"	Enter the name of a certificate verifier. The maximum length is 63 characters.	No default.
ca "<ca-group_name>"	Enter the name of an existing CA Group that you want to use to authenticate client certificates.	No default.
crl "<crl-group_name>"	Enter the name of an existing CRL Group, if any, to use to verify the revocation status of client certificates.	No default.

Related topics

- [system certificate ca-group on page 251](#)
- [system certificate crt on page 252](#)

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 details, see [Permissions on page 46](#).

Syntax

```
config system certificate sni
  edit "<sni_name>"
    config members
      edit <entry_index>
        set domain-type {plain | regular}
        set domain "<server_fqdn>"
        set multi-local-cert {enable | disable}
        set multi-local-cert-group <multi-local-cert-group_name>
        set certificate-type {enable | disable}
        set lets-certificate <name>
        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>"	Enter the name of an Server Name Indication (SNI) configuration.	No default.
<entry_index>	Enter the index number of an SNI configuration entry. The valid range is 1–9,999,999,999,999,999.	No default.
domain-type {plain regular}	Specify <code>plain</code> to match a domain to certificates using a	<code>plain</code>

Variable	Description	Default
	literal domain specified in <code>domain</code> . Specify <code>regular</code> to match multiple domains to certificates using a regular expression specified in <code>domain</code> .	
<code>domain "<server_fqdn>"</code>	Enter the domain of the secure website (HTTPS) that uses the certificate specified by <code>local-cert "<local-cert_name>"</code> on page 265. Enter a literal domain if <code>domain-type {plain regular}</code> on page 264 is set to <code>plain</code> ; or enter a regular expression if <code>domain-type</code> is set to <code>regular</code> .	No default.
<code>multi-local-cert {enable disable}</code>	Enable this option to allow FortiWeb to use multiple local certificates.	<code>disable</code>
<code>multi-local-cert-group <multi-local-cert-group_name></code>	Select the multi-certificate you have created.	No default.
<code>certificate-type {enable disable}</code>	Enable allow FortiWeb to automatically retrieve CA certificates from Let's Encrypt.	<code>disable</code>
<code>lets-certificate <name></code>	Select the Letsencrypt certificate you have created. See system certificate letsencrypt .	No default.
<code>local-cert "<local-cert_name>"</code>	Enter the name of the server certificate that FortiWeb uses to encrypt or decrypt SSL-secured connections for the website specified by <code>domain "<server_fqdn>"</code> on page 265.	No default.
<code>inter-group "<intermediate-cagroup_name>"</code>	Enter 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 <code>local-cert "<local-cert_name>"</code> on page 265. If clients receive certificate warnings that an intermediary CA has signed the server certificate configured in <code>local-cert "<local-cert_name>"</code> on page 265, 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: http://docs.fortinet.com/fortiweb/admin-guides	No default.
<code>verify "<certificate_verificator_name>"</code>	Enter 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.	No default.

Variable	Description	Default
	Personal certificates, sometimes also called user certificates, establish the identity of the person connecting to the website (PKI authentication). You can require that clients present a certificate alternatively or in addition to HTTP authentication. For details, see waf HTTP-authen HTTP-authen-rule on page 529. To display the list of existing verifiers, enter: <pre>edit ?</pre> Note: The client must support TLS 1.0.	

Related topics

- [system certificate local on page 258](#)
- [system certificate intermediate-certificate-group on page 255](#)
- [system certificate verify on page 269](#)

system certificate xml-client-certificate

Use this command to show names of the uploaded XML client certificates that are stored locally on the FortiWeb appliance.

The XML client certificate is used for request verification or response encryption.

Syntax

```
config system certificate xml-client-certificate
  edit system certificate xml-client-certificate on page 266
    set certificate <certificate_str>
    set secret-key <secret-key_str>
  next
end
```

Variable	Description	Default
"<xml-client-certificate_name>"	Enter the name of an XML client certificate.	No default.
certificate <certificate_str>	Set the certificate. Only certificates in PEM format may be set.	No default.
secret-key <secret-key_str>	Enter the secret key string. This is optional, used only for HMAC-SHA-1 sign.	No default.

Related topics

- [waf ws security on page 718](#)
- [system certificate xml-client-certificate on page 266](#)

system certificate tsl-ca

Use this command to show the names of Trust Service Lists (TSL) for a certificate authority (CA). You use the web UI to upload the TSL.

For information on how to upload a TSL, see the FortiWeb Administration Guide:

<http://docs.fortinet.com/fortiweb/admin-guides>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system certificate tsl-ca
  edit "<tsl-ca_name>"
    set type {file | url}
    set distribute-url
  next
end
```

Variable	Description	Default
"<tsl-ca_name>"	Enter the name of a TSL.	No default
type {file url}	Select the way to upload a TSL.	No default
distribute-url	Enter the distribution URL of the TSL.	No default

Related topics

- [system certificate ca](#)
- [system certificate ca-group](#)

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.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For details, see [Permissions on page 46](#).

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>	Enter 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 <code>require</code> is <code>enable</code> , FortiWeb requires the client to present a private certificate.	No default.
require {enable disable}	Specify whether client requests with the URL specified by <code>url</code> are required to present a personal certificate. When you select <code>disable</code> , FortiWeb does not require client requests with the specified URL to present a personal certificate.	No default.

Related topics

- [server-policy policy on page 150](#)
- [server-policy server-pool on page 182](#)

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 [server-policy policy on page 150](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system certificate verify
  edit "<certificate_verificator_name>"
    set ca "<ca-group_name>"
    set crl "<crl-group_name>"
    set publish-dn {enable | disable}
    set strictly-need-cert {enable | disable}
    set partial-chain {enable | disable}
    set crl-allow-expired {enable | disable}
  next
end
```

Variable	Description	Default
"<certificate_verificator_name>"	Enter the name of a certificate verifier. The maximum length is 63 characters.	No default.
ca "<ca-group_name>"	Enter the name of an existing CA Group that you want to use to authenticate client certificates.	No default.
crl "<crl-group_name>"	Enter the name of an existing CRL Group, if any, to use to verify the revocation status of client certificates.	No default.
publish-dn {enable disable}	Enable to list only certificates related to the specified CA Group. This is beneficial when a client installs many certificates in its browser or when apps don't list client certificates. If you enable this option, also enable the option in a CA Group. For details, see system certificate ca-group on page 251 .	disable
strictly-need-cert {enable disable}	Enable to strictly require verifying the client certificate.	enable
partial-chain {enable disable}	Enable to do partial certificate chain validation. External clients can be validated by the Intermediate CA only. When this option is enabled, you also need to enable <code>partial-chain</code> in <code>config system certificate ca-group</code> .	disable

Variable	Description	Default
crl-allow-expired {enable disable}	Enable this option to allow the use of previously retrieved CRLs when the current CRL distribution point retrievals fail or are pending, or when you want to manually upload a CRL file. We highly recommend enabling it as a temporary solution only when the CRL has expired. Ideally, we strongly suggest using the most up-to-date CRL file at all times to ensure that the client with revoked certificates can be promptly blocked.	disable

Related topics

- [system certificate ca-group on page 251](#)
- [system certificate crl on page 252](#)
- [server-policy policy on page 150](#)
- [server-policy server-pool on page 182](#)

system certificate xml-client-certificate-group

Use this command to group XML client certificates.

Syntax

```
config system certificate xml-client-certificate-group
edit system certificate xml-client-certificate-group
    config members
        edit <entry_index>
            set client-name <name_str>
        next
    end
next
end
```

Variable	Description	Default
"<xml-client-certificate-group_name>"	Type the name of the XML client certificate group. You will use this name to select the client certificate group in other parts of the configuration.	No default.
<entry_index>	Type the index number of the individual entry in the table.	No default.
client-name <name_str>	Type the name of a client that you want to include in the group.	No default.

Related topics

- [system certificate xml-client-certificate on page 266](#)
- [waf ws security](#)

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 details, see [Permissions on page 1](#).

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>
  set auto-sync {enable | disable}
  set frequency {daily | every | weekly}
  set day {Friday | Monday | Saturday | Sunday | Thursday | Tuesday | Wednesday}
  set time "<hh:mm>"
end
```

Variable	Description	Default
ip "<remote-fortiweb_ipv4>"	Enter 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.
sync-type {full-sync partial-sync}	Select one of the synchronization types. For all operation modes except WCCP, <code>full-sync</code> 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	partial-sync

Variable	Description	Default
	future syncs) • Administrator accounts • Access profiles • HA settings For the WCCP operation mode, <code>full-sync</code> updates the entire configuration except for the following items: • <code>config system interface</code> • <code>config route static</code> • <code>config route policy</code> • <code>config system wccp</code> • Administrator accounts • Access profiles • HA settings For all operation modes, <code>partial-sync</code> 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 ...	
<code>server-port <port_int></code>	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 the command or the submitting operation will fail.	955
<code>auto-sync {enable disable}</code>	Enable to automatically synchronize the configurations hourly, daily, or weekly. Also configure the <code>frequency</code> , <code>day</code> , and <code>time</code> commands accordingly.	disable
<code>frequency {daily every weekly}</code>	Enter how often you want the configurations to synchronize: • <code>daily</code>—Synchronizes the configuration every day at a specified time. Also configure the <code>day</code> and <code>time</code> commands. For example, Selecting <code>10:30</code> will	No default.

Variable	Description	Default
	synchronize the configurations every day at 10:30. <code>every</code>—Synchronizes the configuration after an interval you set using the <code>time</code> command. For example, entering <code>05:00</code> for the <code>time</code> command will synchronize the configurations every five hours. <code>weekly</code>—Synchronizes the configuration on a specific day and time. For example, selecting <code>Sunday</code> for <code>day</code> and <code>5:15</code> for <code>time</code> will synchronize the configurations every Sunday at 5:15.	
<code>day {Friday Monday Saturday Sunday Thursday Tuesday Wednesday}</code>	If <code>auto-sync</code> is enabled and the <code>frequency</code> is set to <code>weekly</code> , enter the day of the week on which you want the configurations to synchronize.	No default.
<code>time "<hh:mm>"</code>	Enter the time of day or interval at which the configurations will be synchronized: <code>daily</code>—Sets the time of day at which the configurations will be synchronized. <code>every</code>—Sets the interval at which the configurations will be synchronized. <code>weekly</code>—Sets the time of day at which the configurations will be synchronized.	No default.

Related topics

- [system settings on page 372](#)

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 details, see [Permissions on page 46](#).

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: <code>more</code>—When displaying multiple pages' worth of output, pause after displaying each page's worth of text. When the display pauses, the last line displays <code>-More--</code>. You can then either: - Press the spacebar to display the next page. - Type <code>Q</code> to truncate the output and return to the command prompt. <code>standard</code>—Do not pause between pages' worth of output, and do not offer to truncate output.	standard
shell {cli sh}	Select either: <code>cli</code>—Command-line shell. <code>sh</code>—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

- [system admin on page 223](#)

system cpumem-monitor

Use this command to configure CPU and memory monitoring parameters, including capture intervals, utilization thresholds, and log retention limits. By adjusting these settings, you can fine-tune the frequency of resource checks, detect high usage conditions, and enable per-CPU monitoring for more granular analysis. Debugging and log retention controls allow for efficient troubleshooting and long-term data collection.

Syntax

```
config system cpumem-monitor
  set cpu-capture-interval <int>
```

```

set cpu-check-interval <int>
set cpu-high-threshold <int>
set cpumem-monitor {enable|disable}
set debug {enable|disable}
set max-files <int>
set mem-capture-interval <int>
set mem-change-threshold <int>
set mem-check-interval <int>
set mem-high-threshold <int>
set per-cpu-detect {enable|disable}

```

end

Variable	Description	Default
cpu-capture-interval <int>	Specify the minimum time (in seconds) between consecutive CPU usage captures. Valid range: 1–86400.	60
cpu-check-interval <int>	Specify the interval (in seconds) for checking CPU utilization. Valid range: 1–86400.	1
cpu-high-threshold <int>	Set the CPU utilization threshold (%) for high usage detection. Valid range: 10–100.	90
cpumem-monitor {enable disable}	Enable or disable monitoring of CPU and memory usage.	disable
debug {enable disable}	Enable or disable debug mode for the CPU and memory monitor.	disable
max-files <int>	Define the maximum number of retained monitoring log files. Valid range: 1–1000.	10
mem-capture-interval <int>	Specify the minimum time (in seconds) between consecutive memory usage captures. Valid range: 1–86400.	1800
mem-change-threshold <int>	Set the memory utilization change threshold (%) for anomaly detection. Valid range: 1–100.	10
mem-check-interval <int>	Specify the interval (in seconds) for checking memory utilization. Valid range: 1–86400.	300
mem-high-threshold <int>	Set the memory utilization threshold (%) for high usage detection. Valid range: 10–100.	90
per-cpu-detect {enable disable}	Enable or disable per-CPU usage detection.	disable

Example

```
config system cpumem-monitor
  set cpu-capture-interval 30
  set cpu-check-interval 1
  set cpu-high-threshold 90
  set cpumem-monitor enable
  set debug enable
  set max-files 10
  set mem-capture-interval 1800
  set mem-change-threshold 10
  set mem-check-interval 300
  set mem-high-threshold 90
  set per-cpu-detect enable
end
```

system csf

You can configure Fabric Connector to use Single Sign-On (SSO) to log in to FortiWeb with FortiGate's administrator accounts.

Use this command to configure the Fabric Connector on FortiWeb. Single sign-on with FortiGate requires configurations on FortiGate as well. For how to configure SSO with FortiGate, see [Fabric Connector: Single Sign On with FortiGate](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system csf
  set status {enable | disable}
  set configuration-sync {enable | disable}
  set upstream-ip <fortigate ip>
  set upstream-port <port for fabric>
  set management-ip <fortiweb mgmt ip>
  setmanagement-port <port for fortiweb mgmt>
end
```

Variable	Description	Default
status {enable disable}	Enable or disable the Fabric Connector.	disable
configuration-sync {enable disable}	Enable means when Fabric connection with FortiGate is established, the Single Sign-On mode would be enabled automatically and FortiGate would enable synchronizing SAML Single-Sign-On related settings to the FortiWeb device. Disable means when Fabric connection with the FortiGate is established, you need to manually enable Single Sign-On mode and manually configure the SAML Single-Sign-On settings. It's recommended to set it as <code>enable</code>.	Enable

Variable	Description	Default
upstream-ip <fortigate ip>	The FortiGate IP. If you have multiple FortiGate appliances and they are deployed as Fabric net, enter the IP address of the Fabric root. This IP would be the IP of the interface that is selected in the Allow other Security Fabric devices to join field on the FortiGate.	0.0.0.0
upstream-port <port for fabric>	Use the default 8013.	8013
management-ip <fortiweb mgmt ip>	Enter FortiWeb GUI management IP.	No default
management-port <port for fortiweb mgmt>	Enter FortiWeb GUI management HTTPS port. This must be the same as the setting of the HTTPS in System > Admin > Settings in FortiWeb	No default

Related topics

- [system saml](#)

system decoding enhancement

Use this command to configure decoding enhancement. You can decode cookies and parameters using base64 or CSS for specified URLs.

To configure decoding enhancement, you must first enable the feature. For details, see [system advanced on page 233](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system decoding-enhancement
  edit <entry_index>
    set url-type {plain | regular}
    set url-pattern "<url_string>"
    set b64arg enable
    config field-list
      edit <entry_index>
        set base64-decoding {enable | disable}
        set css-decoding {enable | disable}
        set field-name "<parameter_cookie_str>"
        set field-name-type {plain | regular}
        set field-type {parameter | cookie}
      next
    end
  next
end
```

Variable	Description	Default
<entry_index>	Enter the index number of the decoding rule that you want to create or modify.	No default.
url-type {plain regular}	Enter to select between: <code>plain</code>—A simple string; a string of text that contains a literal URL. <code>regular</code>—A regular expression; a string of text that defines a search pattern for a URL that may come in many variations.	No default.
url-pattern "<url_string>"	Enter the URL path for which you want the decoding rule to apply.	No default.
b64arg {enable disable}	When it's enabled, all the parameters in the URL will be decoded before being parsed. If you only want to decode certain parameters instead of all, you can disable this option and then enable the <code>base64-decoding</code> to apply the decoding for specified parameters.	enable
<entry_index>	Enter the index number of the field that you want to create or modify.	No default.
base64-decoding {enable disable}	Configure to enable Base64 decoding for the field.	disable
css-decoding {enable disable}	Configure to enable CSS decoding for the field.	disable
field-name "<parameter_cookie_str>"	Enter the parameter or cookie string for the field.	No default.
field-name-type {plain regular}	Enter to select between: <code>plain</code>—A simple string; a string of text that contains a literal URL. <code>regular</code>—A regular expression; a string of text that defines a search pattern for a URL that may come in many variations.	No default.
field-type {parameter cookie}	Enter to select between: <code>parameter</code>—Enter to set a parameter field for the field. <code>cookie</code>—Enter to set a cookie field for the field.	No default.

Example

This example enables decoding enhancement and creates a decoding rule with a parameter field type.

```
config system advanced
    set decoding-enhancement enable
end
```

```
config system decoding-enhancement
  edit 1
    set url-type plain
    set url-pattern "/decoding"
    config field-list
      edit 1
        set base64-decoding enable
        set css-decoding enable
        set field-type parameter
        set field-name-type plain
        set field-name key
      next
    end
  next
end
```

Related Topic(s)

- [system advanced on page 233](#)

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 details, see [Permissions on page 46](#).

Syntax

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

Variable	Description	Default
primary "<dns_ipv4>"	Enter the IP address of the primary DNS server.	8 . 8 . 8 . 8
secondary "<dns_ipv4>"	Enter the IP address of the secondary DNS server.	0 . 0 . 0 . 0
domain "<local-domain_str>"	Enter 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 <code>Host :</code> field of HTTP headers for client connections to protected web servers. Note: You can also configure the host name. For details, see .	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

- [log syslog-policy on page 93](#)
- [router static on page 101](#)
- [system interface on page 344](#)
- [server-policy policy on page 150](#)

system encryption-method

Use this command to use generate a random private encryption key and store it into the TPM (Trusted Platform Module). This key is used to encrypt and decrypt configuration passwords and certificates, ensuring that sensitive data remains protected. In HA deployments, the encryption key is automatically synchronized to the secondary node's TPM, preventing unauthorized access across different systems.



After enabling private encryption, it is recommended to generate a sample using `execute private-encryption-key sample` and record the output. If backup configurations fail to restore, the private key may have changed. Use `execute private-encryption-key verify` with the previously recorded sample to check if it matches the current private key. If verification fails, a new private key was generated, and the backup configuration must be re-encrypted. For details, see [private-encryption-key on page 844](#).

Syntax

```
config system encryption-method
    set private-encryption-key {enable|disable}
end
```

Variable	Description	Default
private-encryption-key {enable disable}	When enabled, FortiWeb generates a random encryption key and stores it in TPM.	disable

Related topic

[private-encryption-key on page 844](#)

system endpoint-control

Use this command to set a FortiClient EMS connector.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system endpoint-control fctems
    edit <ems_connector_name>
        set server <IP_address>
        set https-port <port>
        set server-verification {enable | disable}
        set ca-cert <cert_name>
        set source-ip <IP_address>
        set call-timeout <int>
        set preserve-ssl-session {enable | disable}
        set fingerprint <fingerprint>
        set EMS_SN <EMS_EN>
    next
end
```

Variable	Description	Default
<ems_connector_name>	Enter the name of the EMS connector.	No default.
server <IP_address>	Enter the EMS server IP address.	No default.
https-port <port>	Enter the HTTPS access port number.	443
server-verification {enable disable}	Enable this option to verify the FortiClient EMS certificate that is used for the HTTPS connection between FortiWeb and FortiClient EMS.	disable
ca-cert <cert_name>	Select the certificate for verifying FortiClient EMS server certificate that is used for the connection between FortiWeb and FortiClient EMS.	No default.
source-ip <IP_address>	Enter the allowed source IP addresses of the API calls.	0.0.0.0
call-timeout <int>	Enter the timeout value for the API calls from FortiWeb to EMS server.	15
preserve-ssl-session {enable disable}	Enable/disable preservation of EMS SSL session connection.	disable
fingerprint <fingerprint>	Enter the EMS server fingerprint.	automatically populated once EMS is verified.
EMS_SN <EMS_EN>	Enter the EMS server serial number.	automatically populated once EMS is verified.



It's highly recommended not to change the default value of the variables except <ems_connector_name>, server <IP_address>, and https-port <port>.

Related topics

- [system endpoint-control on page 799](#)
- [system endpoint-control on page 281](#)
- [server-policy ztna-profile on page 217](#)
- [server-policy ztna-rule on page 219](#)

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 details, see the *FortiWeb-VM Azure Install Guide*:

<https://docs.fortinet.com/fortiweb/hardware>

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 [log siem-policy on page 89](#)), FortiWeb also sends security logs to Azure Event Hub.

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 Azure Install Guide*:

<https://docs.fortinet.com/fortiweb/hardware>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

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 <code>enable</code> 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 <code>policy_name <policy-name_str></code>) 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 <code>servicebus_namespace <servicebus-namespace_str></code>).	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 on page 89](#)
- [log siem-message-policy on page 87](#)

system external-resource

Use this command to create IP address connectors which allow you to dynamically import an external block list from an HTTP/HTTPS server in the form of a plain text file, , or in STIX format from a TAXII server. Block lists can be used to enforce special security requirements, such as blocking access from certain IP addresses. The lists are dynamically imported, so that any changes are immediately imported by FortiWeb.

After you have imported your external block list through the IP Address connector, you can apply the IP External resource in **IP Protection > IP List**.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system external-resource
  edit <external-IP-name>
    set status {enable | disable}
    set protocol {http | https | taxii}
    set local-cert <cert-name>
    set verify-host-cert {enable | disable}
    set ca <ca_cert_name>
    set http-basic-authentication {enable | disable}
    set username <string> #HTTP basic authentication username
    set password <string> #HTTP basic authentication password
    set refresh-rate <int> #Time interval to refresh external resource (1 - 43200 min)
    set resource <string> #external-resource enable/disable
  next
end
```

Variable	Description	Default
<external-IP-name>	Specify the name of the IP Address connector. Valid characters are A-Z, a-z, 0-9, _, and -. No spaces.	No default
status {enable disable}	Enable the external IP connector.	disable
protocol {http https taxii}	Select the protocol used for the connections between FortiWeb and the IP External resource. Options include: • http — Downloads the blocklist over an unencrypted HTTP connection. Suitable for internal or non-sensitive sources. • https — Downloads the blocklist over a secure	https

Variable	Description	Default
	HTTPS connection. Recommended for most use cases to ensure data integrity. taxii — Uses the TAXII protocol to fetch STIX-formatted IP threat indicators from a TAXII server. This allows FortiWeb to integrate with structured threat intelligence platforms that publish IP-based indicators of compromise.	
local-cert <cert-name>	Select the TLS certificate used for the HTTPS connection between FortiWeb and the IP External resource. It should be uploaded in the Local tab in Sever Objects > Certificates > Local. Available only if <code>https</code> or <code>taxii</code> is selected for protocol.	No default
verify-host-cert {enable disable}	Enable this option to verify the IP External resource's URI is valid by checking the ownership of the CA certificate. Available only if <code>https</code> or <code>taxii</code> is selected for protocol.	disable
ca <ca_cert_name>	Select the CA certificate of the IP External resource's URI. It should be uploaded in the CA tab in Sever Objects > Certificates > CA. Available only if <code>https</code> or <code>taxii</code> is selected for protocol.	No default
username <string>	Specify the username to be used to access this IP address list. With username and password specified, the system will automatically enable HTTP Basic Authentication.	No default
password <string>	Specify the password to be used to access this IP address list. With username and password specified, the system will automatically enable HTTP Basic Authentication.	No default
refresh-rate <int>	Specify the refresh rate in minutes. (Default: 5. Range: 1-43200 minutes). FortiWeb will retrieve the data from the HTTP/HTTPS server periodically according to the refresh rate.	5
resource <string>	Specify the URI of the HTTP/HTTPS server where the IP address list is stored.	No default

Related topics

- [waf ip-list on page 561](#)

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**:

- when the operation mode is True Transparent Proxy, Transparent Inspection, or WCCP
- 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 600D: port1 + port2
 - FortiWeb 1000D: port3 + port4 or port5 + port6
 - FortiWeb 1000E: port3 + port4 + port5 + port6
 - FortiWeb 2000E: port1 + port2 or port3 + port4
 - FortiWeb3000E/4000E: port9 + port10, port11 + port12, port13 + port14, or port15 + port16
 - FortiWeb 3010E: port3 + port4, port9 + port10, port11 + port12, port13 + port14 or port15 + port16
 - FortiWeb 600F: port3 + port4
 - FortiWeb 1000F: port1 + port2, port3 + port4, port5 + port6 or port7 + port8
 - FortiWeb 2000F: port1 + port2 or port3 + port4
 - FortiWeb 3000F: port5 + port6, port11 + port12, port13 + port14, port15 + port16 or port17 + port18
 - FortiWeb 4000F: port1 + port2, port3 + port4, port13 + port14, port15 + port16, port17 + port18 or port19 + port20

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 details, see [Permissions on page 46](#).

Syntax

```
config system fail-open
    set port3-port4 {poweroff-bypass | poweroff-cutoff}
end
```

Variable	Description	Default
port3-port4 {poweroff-bypass poweroff-cutoff}	Select either: <code>poweroff-bypass</code>—Behave like a wire when powered off, allowing connections to pass directly through from one port to the other, bypassing policy and profile filtering. <code>poweroff-keep</code>—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

- [system ha on page 319](#)

system fds proxy

Use this command to configure the FortiWeb proxy to override the default list of FDN servers and update FortiGuard service packages from a new address.

Before using this command, you must configure FortiWeb to act as a proxy server. To do so, set `fds-proxy` to `enable`. See [system global](#) for how to enable `fds-proxy`.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system fds proxy override
    set override_switch {enable | disable}
    set address "<fds_IPv4>"
end

config system fds proxy schedule
    set status {enable | disable}
    set frequency {every | daily | weekly}
    set time
    set day {Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday}
end
```

Variable	Description	Default
override_switch {enable disable}	Enable to override the default list of FDN servers and connect to a specific server.	disable
address "<fds_IPv4>"	Enter either an IP address or fully qualified domain name (FQDN) of the FDS override, so that FortiWeb proxy will obtain FortiGuard service packages from this address.	No default.
status {enable disable}	Enable to schedule updating the database per certain frequency.	disable
frequency {every daily weekly}	Set the database update frequency.	No default.
time	Set the hour and minute ranges; hh: 0–23, mm 0–59 or 60=random.	No default.
day {Sunday Monday Tuesday Wednesday Thursday Friday Saturday}	Set the specific day during one week to update the database.	No default.

Example

This example enables FortiWeb to act as an FDS proxy and update FortiGuard service packages from 192.0.2.1.

```
config system global
    set fds-proxy enable
end

config system fds proxy
    set override_switch enable
    set address "192.0.2.1"
end
```

system feature-visibility

Use this command to enable or disable the ability to view configuration options for these features in the web UI and CLI:

1. System features
 - Traffic Mirror
 - Replacement Message for AJAX requests
 - Firewall
 - Debug
 - WCCP
 - reCAPTCHA
2. Security Features
 - FTP Security
 - Mobile Application Identification

- Signature Update Management
- FortiGate Integration
- Web Anti-Defacement
- Padding Oracle Protection
- Web Vulnerability Scan

3. Additional Features

- ADFS Policy
- Acceleration
- Web Cache
- API Gateway
- ICAP Server

When these features are disabled, options for configuring these features are hidden in the web UI and CLI. If you're planning to configure and implement these features in your FortiWeb configuration, you'll need to enable feature visibility for them first.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system feature-visibility
  set acceleration-policy {enable | disable}
  set adfs-policy {enable | disable}
  set api-gateway {enable | disable}
  set debug-log {enable | disable}
  set firewall {enable | disable}
  set recaptcha {enable | disable}
  set fortigate-integration {enable | disable}
  set ftp-security {enable | disable}
  set mobile-app-identification {enable | disable}
  set padding-oracle {enable | disable}
  set support-ajax-requests {enable | disable}
  set support-icap-server {enable | disable}
  set traffic-mirror {enable | disable}
  set wad {enable | disable}
  set wccp-mode {enable | disable}
  set web-cache {enable | disable}
  set wvs {enable | disable}
  set ztna {enable | disable}
end
```

Variable	Description	Default
acceleration-policy {enable disable}	Enable to display acceleration policy configuration options.	disable
adfs-policy {enable disable}	Enable to display ADFS policy and ADFS server pool options.	disable

Variable	Description	Default
api-gateway {enable disable}	Enable to display API users, API gateway rule and policy configuration options.	disable
debug-log {enable disable}	Enable to display debug log configurations.	disable
firewall {enable disable}	Enable to display firewall policy and NAT policy configuration options.	disable
recaptcha {enable disable}	Enable to display <code>user recaptcha-user</code> configurations.	disable
fortigate-integration {enable disable}	Enable to display FortiGate integration configuration options.	disable
ftp-security {enable disable}	Enable to display FTP security rule, profile, and policy configuration options.	disable
mobile-app-identification {enable disable}	Enable to display the JWT token secret and token header to verify a request from a mobile application.	disable
padding-oracle {enable disable}	Enable to display padding oracle rule configuration options.	disable
support-ajax-requests {enable disable}	Enable to display support AJAX requests options.	disable
support-icap-server {enable disable}	Enable to display ICAP server configuration options.	disable
traffic-mirror {enable disable}	Enable to display traffic mirror rule, profile, and policy configuration options.	disable
wad {enable disable}	Enable to display web anti-defacement configuration options.	disable
wccp-mode {enable disable}	Enable to display WCCP client configuration options.	disable
web-cache {enable disable}	Enable to display web cache policy and profile configuration options.	disable
wvs {enable disable}	Enable to display web vulnerability scan policy and profile configuration options.	disable
ztna {enable disable}	Enable to display Zero Trust Network Access (ZTNA) policy and profile configuration options.	

Related Topics

- [waf web-protection-profile inline-protection on page 696](#)
- [waf ftp-protection-profile on page 510](#)
- [waf ftp-command-restriction-rule on page 505](#)

- [waf ftp-file-security](#) on page 508
- [server-policy policy](#) on page 150
- [server-policy server-pool](#) on page 182
- [system replacemsg](#) on page 1

system fips-cc

Use this command to enable and configure Federal Information Processing Standards (FIPS) and Common Criteria (CC) compliant mode.

The following FortiWeb images don't support `fips-cc` mode:

- FWB_HYPERV
- FWB_XENAWS
- FWB_XENAWS_ONDEMAND
- FWB_AWSCLD
- FWB_VM_PAYG
- FWB_AZURE
- FWB_AZURE_ONDEMAND
- FWB_KVM
- FWB_KVM_PAYG
- FWB_GCP
- FWB_GCP_ONDEMAND
- FWB_OCI
- FWB_OCI_ONDEMAND
- FWB_ALI
- FWB_FTCLD
- FWB_GCPCLD
- FWB_OCICLD

The `fips-ciphers` mode is only supported by the following images:

- FWB_XENAWS
- FWB_XENAWS_ONDEMAND
- FWB_AZURE
- FWB_AZURE_ONDEMAND

Syntax

```
config system fips-cc
  set status {enable | disable | fips-ciphers}
  set entropy-token {dynamic | enable | disable}
  set reseed-interval <reseed-interval_int>
  set ssl-client-restrict {enable | disable}
end
```

Variable	Description	Default
status {enable disable fips-ciphers}	Select <code>enable</code> or <code>disable</code> to turn on and off the <code>fips-cc</code> operation mode. <code>fips-ciphers</code> is a special kind of FIPS mode. fips-ciphers mode The <code>fips-ciphers</code> mode is only supported by FortiWeb-VMs on AWS and Azure. In <code>fips-ciphers</code> mode, FortiWeb has the following limitations: - For the business traffic going through FortiWeb, both HTTP and HTTPS protocols are allowed, but TLS 1.0 and TLS 1.1 are not supported for HTTPS traffic. Only the following SSL ciphers are allowed: For TLS1.3 - TLS_AES_256_GCM_SHA384 - TLS_AES_128_GCM_SHA256 For TLS1.2 - ECDHE-ECDSA-AES256-GCM-SHA384 - ECDHE-RSA-AES256-GCM-SHA384 - DHE-RSA-AES256-GCM-SHA384 - ECDHE-ECDSA-AES128-GCM-SHA256 - ECDHE-RSA-AES128-GCM-SHA256 - DHE-RSA-AES128-GCM-SHA256 - For the traffic to FortiWeb's CLI and GUI, HTTP and Telnet are not allowed. Only HTTPS and SSH are allowed. The supported SSL ciphers for HTTPS traffic are the same as listed above. The supported ciphers for SSH traffic include: - diffie-hellman-group-exchange-sha256 - ssh-rsa - hmac-sha2-256 - hmac-sha2-512 - aes128-gcm@openssh.com - aes256-gcm@openssh.com	disable
entropy-token {dynamic enable disable}	Use the entropy token to seed the RNG in FIPS-CC mode. When the status is enabled, the entropy token is used to seed or reseed the RNG, and it must be inserted to FortiWeb.	disable

Variable	Description	Default
	- When the status is disabled, the entropy token is not used to seed or reseed the RNG, but the old method will be used to seed or reseed the RNG. - When the status is dynamic, it means when entropy token is present, the entropy token will be used to seed or reseed the RNG; if the token is not present, the old method will be used to seed or reseed the RNG.	
reseed-interval <reseed-interval_int>	Set the interval to reseed the RNG. The valid range is 0–1440 minutes.	1440
ssl-client-restrict {enable disable}	Enable/disable ciphers restriction.	disable

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. For details, see [system firewall firewall-policy on page 295](#).

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.
type {ip-netmask ip-range}	Select how this configuration specifies a firewall address or addresses: <code>ip-netmask</code>—A single IP address and netmask. <code>ip-range</code>—A single IP address or a range of IP addresses.	ip-range

Variable	Description	Default
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 {ip-netmask ip-range} on page 293 is ip-netmask.	No default.
ip-address-value "<firewall-address_ipv4>"	Enter a single IP address or a range of addresses. For example, 192.0.2.1, or 192.0.2.1-192.0.2.255. Available when type {ip-netmask ip-range} on page 293 is ip-range.	No default.

Related topics

- [system firewall firewall-policy on page 295](#)
- [system firewall service on page 294](#)

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. For details, see [system firewall firewall-policy on page 295](#).

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
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

Variable	Description	Default
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

- [system firewall address on page 293](#)
- [system firewall firewall-policy on page 295](#)

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. For details, see [system firewall address on page 293](#) and [system firewall service on page 294](#).

Syntax

```
config system firewall firewall-policy
  set default-action {deny | accept}
  config firewall-policy-match-list
    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}
      set vzone-enable {enable | disable}
      set vzone "<vzone_name>"
    end
  end
```

Variable	Description	Default
default-action {deny accept}	Select either: • 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	accept

Variable	Description	Default
	configured. <code>accept</code>—Firewall allows traffic that does not match a policy rule.	
<code><entry_index></code>	Enter the index number of the policy rule in the table.	No default.
<code>in-interface "<incoming_interface_name>"</code>	Enter the name of the interface (for example, <code>port1</code>) on which FortiWeb receives packets it applies this firewall policy rule to.	No default.
<code>out-interface "<outgoing_interface_name>"</code>	Enter the name of the interface (for example, <code>port2</code>) through which FortiWeb routes packets it applies this firewall policy rule to.	No default.
<code>src-address "<firewall-address_name>"</code>	Enter the name of the firewall address configuration that specifies the source IP address or addresses to which this policy applies. For details about creating firewall address configurations, see system firewall address on page 293.	No default.
<code>dest-address "<firewall-address_name>"</code>	Enter the name of the firewall address configuration that specifies the source IP address or addresses to which this policy rule applies. For details about creating firewall address configurations, see system firewall address on page 293.	No default.
<code>service "<firewall-service_name>"</code>	Enter the name of the firewall service configuration that specifies the protocols and ports to which this policy rule applies. For details about creating firewall address configurations, see system firewall address on page 293.	No default.
<code>action {deny accept}</code>	Enter either: <code>deny</code>—Firewall blocks traffic that matches this policy rule. However, administrative access is still allowed on network interfaces for which it has been configured. <code>accept</code>—Firewall allows traffic that matches this policy rule.	deny
<code>vzone-enable {enable disable}</code>	Select to enable a V-zone (bridge). If this option is enabled, select a V-zone to use. V-zones allow network connections to travel through FortiWeb's physical network ports without explicitly connecting to one of its IP addresses. This option is available only when the operation mode is True Transparent Proxy or Transparent Inspection mode.	disable
<code>vzone "<vzone_name>"</code>	Select a configured V-zone. For details about creating a V-zone, see system v-zone on page 388 .	No default.

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
  config firewall-policy-match-list
    edit 1
      set in-interface port1
      set out-interface port2
      set src-address site1
      set dest-address site1
      set service HTTP
      set action accept
    next
  end
end
```

Related topics

- [system firewall address on page 293](#)
- [system firewall service on page 294](#)

system firewall fwmark-policy

Use this command to mark the traffic coming in FortiWeb. Using it together with policy route, you can direct the marked traffic to go out of FortiWeb through a specified interface or/and to a specified next-hop gateway.

Syntax

```
config system firewall fwmark-policy
  edit "<fwmark-policy-name>" on page 298
    set from <firewall_source-address_name> on page 298
    set to <firewall_destination-address_name> on page 298
```

```

set in-interface <incoming_interface_name> on page 298
set service <firewall-service_name>" on page 298
set mark <mark_int> on page 298

```

```
end
```

Variable	Description	Default
"<fwmark-policy-name>"	The name of the fwmark policy.	No default.
from <firewall_source-address_name>	Enter the name of the firewall address configuration that specifies the source IP address or addresses to which this policy applies. For details about creating firewall address configurations, see system firewall address on page 293 .	No default.
to <firewall_destination-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 details about creating firewall address configurations, see system firewall address on page 293 .	No default.
in-interface <incoming_interface_name>	Enter the name of the interface (for example, <code>port1</code>) on which FortiWeb receives packets it applies this firewall policy rule to.	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 details about creating firewall address configurations, see system firewall address on page 293 .	No default.
mark <mark_int>	Enter a value to mark the traffic that matches with the conditions above. The valid range is 1-255.	No default.

Example

```

config system firewall fwmark-policy
edit "1"
    set from 1
    set to 2
    set in-interface port2
    set service ALL_TCP
    set mark 234
next
end

```

system firewall admin-policy

While security profiles control traffic flowing through the FortiWeb, admin policies (named as Firewall Admin Policy in GUI) control inbound traffic that is going to a FortiWeb interface.

Administrative access traffic (HTTPS, PING, SSH, and others) can be controlled by allowing or denying the service in the interface settings. Trusted hosts can be configured under an administrator to restrict the hosts that can access the administrative service.

To further restrict access, you can use admin policies to granularly define the source and destination addresses, interface, and services.

Traffic destined for the all the network interfaces of FortiWeb is subject to the admin firewall policy.

The firewall admin policy uses address and service configurations that you create separately. For details, see [system firewall address on page 293](#) and [system firewall service on page 294](#).

Syntax

```
config system firewall admin-policy
  config firewall-admin-policy-match-list
    edit <entry_index>
      set in-interface "<incoming_interface_name>"
      set src-address "<firewall-address_name>"
      set dest-address "<firewall-address_name>"
      set service "<firewall-service_name>"
      set action {deny | accept}
    end
  end
```

Variable	Description	Default
<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, <code>port1</code>) on which FortiWeb receives 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 details about creating firewall address configurations, see system firewall address on page 293 .	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 details about creating firewall address configurations, see system firewall address on page 293 .	No default.

Variable	Description	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 details about creating firewall address configurations, see system firewall address on page 293 .	No default.
action {deny accept}	Enter either: - deny—Firewall blocks traffic that matches this policy rule. - accept—Firewall allows traffic that matches this policy rule.	deny

Related topics

- [system firewall address on page 293](#)
- [system firewall service on page 294](#)

system firewall dnat policy

Use this command to configure a firewall DNAT policy. Firewall DNAT policies translate the destination IP address.

Firewall DNAT policies are available in Reverse Proxy, True Transparent Proxy, and Transparent Inspection operating modes.



FortiWeb applies a firewall DNAT policy only if IP forwarding is enabled. For details about IP forwarding, see [router setting on page 100](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system firewall dnat-policy
edit "<policy_name>" on page 301
    set external-start <external_ipv4> on page 301
    set mapped-start <mapped_ipv4> on page 301
    set mapped-end <mapped_ipv4> on page 301
    set ingress-interface <ingress_port> on page 301
    set protocol {tcp | udp | icmp} on page 301
    set port-forwarding {enable | disable} on page 301
    set external-port-start <external_port> on page 301
    set external-port-end <external_port> on page 301
    set mapped-port-start <mapped_port> on page 301
    set mapped-port-end <mapped_port> on page 301
```

```

next
end

```

Variable	Description	Default
"<policy_name>"	Enter a name that identifies the firewall DNAT policy. Don't use spaces or special characters. The maximum length is 63 characters.	No default.
external-start <external_ipv4>	Enter the first IP address of an IP range to match the destination IP address in the packet header that you want to translate. The external addresses must be one-to-one mapped to the translated addresses. For example, if the external IP range contains 10 addresses, the mapped IP range must also contain 10 addresses. After you configure the <code>mapped-start</code> and <code>mapped-end</code>, the system will calculate how many addresses are included in the range and automatically determine the last IP address of the external IP range. The IP address must be IPv4.	0.0.0.0
mapped-start <mapped_ipv4>	Enter the first IP address of an IP range that you want to translate the external IP to.	0.0.0.0
mapped-end <mapped_ipv4>	Enter the last IP address of an IP range that you want to translate the external IP to.	0.0.0.0
ingress-interface <ingress_port>	Enter the interface to match the network interface through which the packet comes in FortiWeb.	No default.
protocol {tcp udp icmp}	Select the protocol type of the packets that you want to translate.	No default.
port-forwarding {enable disable}	Enable to translate the port in destination IP address.	No default.
external-port-start <external_port>	Enter the first port in the port range to match the port in destination IP address. This option is available only when <code>port-forwarding</code> is enabled.	0
external-port-end <external_port>	Enter the last port in the port range to match the port in destination IP address. This option is available only when <code>port-forwarding</code> is enabled.	0
mapped-port-start <mapped_port>	Enter the first port in the port range to translate the external port range to. This option is available only when <code>port-forwarding</code> is enabled.	0
mapped-port-end <mapped_port>	Enter the last port in the port range to translate the external port range to.	0

Variable	Description	Default
	This option is available only when <code>port-forwarding</code> is enabled.	

Related Topic

- [router setting on page 100](#)
- [system firewall snat-policy on page 302](#)

system firewall snat-policy

Use this command to configure a firewall SNAT policy. Firewall SNAT policies translate a matching source IP address to a single IP address or an IP address in an address pool.

Firewall SNAT policies are available in Reverse Proxy, True Transparent Proxy, and Transparent Inspection operating modes.



FortiWeb applies a firewall SNAT policy only if IP forwarding is enabled. For details about IP forwarding, see [router setting on page 100](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system firewall snat-policy
edit "<policy_name>" on page 302
    set source-start <source_ipv4> on page 303
    set source-end <source_ipv4> on page 303
    set out-interface "<egress_port>" on page 303
    set destination-start <destination_ipv4> on page 303
    set destination-end <destination_ipv4> on page 303
    set trans-to-type {ip | pool | no-nat} on page 303
    set trans-to-ip "<translation_ipv4>" on page 303
    set trans-to-ip-start "<first_ipv4>" on page 303
    set trans-to-ip-end "<last_ipv4>" on page 303
next
end
```

Variable	Description	Default
"<policy_name>"	Enter a name that identifies the firewall SNAT policy. Don't use spaces or special characters. The maximum length is 63 characters.	No default.

Variable	Description	Default
source-start <source_ipv4>	Enter the first IP in the IP range to match the source IP address in the packet header that you want to translate. The IP address must be an IPv4 address.	0.0.0.0/0
source-end <source_ipv4>	Enter the last IP in the IP range to match the source IP address in the packet header that you want to translate. The IP address must be an IPv4 address.	
out-interface "<egress_port>"	Select the interface that FortiWeb will use to forward traffic that matches the source-start <source_ipv4> on page 303 .	No default.
destination-start <destination_ipv4>	Enter the first IP in the IP range to match the destination IP address in the packet header. The IP address must be an IPv4 address.	0.0.0.0/0
destination-end <destination_ipv4>	Enter the last IP in the IP range to match the destination IP address in the packet header. . The IP address must be an IPv4 address.	
trans-to-type {ip pool no-nat}	Select one of the following: <code>ip</code>—Select to translate the source IP to an IP address that you specify. <code>pool</code>—Select to translate the source IP to the next available IP address in an IP address pool that you specify. <code>no-nat</code>—Select to not perform SNAT for the matched traffic.	ip
trans-to-ip "<translation_ipv4>"	Enter the IP address that you want to translate the source IP to. An example IP address is 192.0.2.2. The IP address must be an IPv4 address. This option is available only when the trans-to-type {ip pool no-nat} on page 303 is set to <code>IP</code> .	0.0.0.0
trans-to-ip-start "<first_ipv4>"	Enter the first IP address in the SNAT pool. An example IP address is 192.0.2.3. The IP address must be an IPv4 address. This option is available only when the trans-to-type {ip pool no-nat} on page 303 is set to <code>pool</code> .	0.0.0.0
trans-to-ip-end "<last_ipv4>"	Enter the last IP address in the SNAT pool. An example IP address is 192.0.2.4. The IP address must be an IPv4 address. This option is available only when the trans-to-type {ip pool no-nat} on page 303 is set to <code>pool</code> .	0.0.0.0

Related Topic

- [router setting on page 100](#)
- [system firewall dn timer policy on page 300](#)

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. For details, see [waf web-protection-profile inline-protection on page 696](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system fortigate-integration
  set server "<domain_name_or_ipv4>"
  set port <port_int>
  set protocol {HTTP | HTTPS}
  set server-verification {enable | disable} on page 304
  set ca-cert <cert_name>
  set username "<username_str>"
  set password "<password_str>"
  set schedule-frequency <schedule-frequency_int>
  set flag {enable | disable}
end
```

Variable	Description	Default
server "<domain_name_or_ipv4>"	Enter the FortiGate IP address or domain name 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
server-verification {enable disable}	Enable this option to verify the TLS certificates used for the HTTPS connection between FortiWeb and FortiGate. Available only if HTTPS is selected for Protocol .	disable
ca-cert <cert_name>	Select the certificate for the HTTPS connection between FortiWeb and FortiGate. It should be uploaded in System > Admin > Certificates > Admin Cert CA .	No default.
username "<username_str>"	Enter the name of the administrator account that FortiWeb uses to connect to the FortiGate.	No default.

Variable	Description	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 per hour, for example, once or twice per hour. 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

- [waf file-upload-restriction-policy on page 497](#)
- [log reports on page 77](#)
- [system fortisandbox-statistics on page 862](#)

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 security 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 details, see [Permissions on page 46](#).

Syntax

```
config system fortisandbox
  set type {fsa | cloud}
  set server "<server_ipv4>"
  set cache-timeout <timeout_int>
  set email "<email_str>"
  set interval <interval_int>
  set elog {enable | disable}
  set region {Europe | Global | US | Japan}
end
```

Variable	Description	Default
type {fsa cloud}	Specify whether FortiWeb submits files that match the upload restriction rules to a FortiSandbox physical appliance (or FortiSandbox-VM) or to FortiWeb Cloud Sandbox. The FortiWeb Cloud Sandbox 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 <code>type</code> is <code>fsa</code> .	No default.
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. The valid range is 1–168. 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
eelog {enable disable}	Enter so that FortiWeb will report event logs when it successfully submits files to FortiSandbox.	disable
region {Europe Global US Japan}	Available only when the type is cloud (FortiWeb Cloud Sandbox). Datacenters are located in Canada, Germany, the United States, and Japan to ensure better performance. The default region is Global. Select a country or region from the list. FortiWeb will retrieve and establish a connection to the appropriate FortiSandbox Cloud server IP based on the selected region.	Global

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 email "admin@example.com"
```

end

Related topics

- [waf file-upload-restriction-policy](#) on page 497
- [log reports](#) on page 77
- [system fortisandbox-statistics](#) on page 862
- [forticloud-sandbox](#) on page 833

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 details, see [Permissions](#) on page 46.

Syntax

```
config system global
  set admin-port <port_int>
  set admin-sport <port_int>
  set admin-tls-v10 {enable | disable}
  set admin-tls-v11 {enable | disable}
  set admin-tls-v12 {enable | disable}
  set admin-tls-v13 {enable | disable}
  set admin-ssl-custom-cipher <cipher1 cipher2 ...>
  set admin-tls13-custom-cipher <cipher1 cipher2 ...>
  set admin-lockout-threshold <admin-lockout-threshold_int>
  set admin-lockout-duration <minutes_int>
  set admintimeout <minutes_int>
  set adom-admin {enable | disable}
  set auth-timeout <milliseconds_int>
  set cli-signature {enable | disable}
  set confsync-port <port_int>
  set debug-monitor-interval <int>
  set debug-memory-boundary <int>
  set dh-params {1024 | 1536 | 2048 | 3072 | 4096 | 6144 | 8192}
  set dst {enable | disable}
  set fds-proxy {enable | disable}
  set force-us-only {enable | disable}
  set hostname "<host_name>"
  set admin-HTTPS-pki-required {enable | disable}
  set HTTPS-certificate "<certificate_name>"
  set HTTPS-intermediate-certificate "<certificate_group_name>"
  set ie6workaround {enable | disable}
  set language {english | japanese | simch | trach}
  set multi-factor-authentication {optional | mandatory}
  set ntpserver {"<ntp_fqdn>" | "<ntp_ipv4>"}
  set ntpsync {enable | disable}
```

```

set pre-login-banner {enable | disable}
set record-cli-fail-cmd {enable | disable}
set refresh <seconds_int>
set syncinterval <minutes_int>
set timezone "<time-zone-code_str>"
set tftp {enable | disable}
set ssh-fips {enable | disable}
set cert-expire-check-time <cert-expire-check-time_int>
set ipv6-dad-ha {enable | disable} on page 316
set fortiguard-anycast {enable | disable} on page 316
set updated-debug-log {enable | disable}
set power-status {enable | disable}
set shell-access {enable | disable}
set shell-username <user_name>
set shell-password <password>
set shell-timeout <int>
set shell-history-size
set shell-trusthostv4
set shell-trusthostv6
set admin-forticloud-sso-login {enable | disable}
set advanced-bot-protection {enable | disable}
set advanced-bot-protection-portal-domain <fortiabp.forticloud.com>
set advanced-bot-protection-query-timeout <int>
set advanced-bot-protection-js-attribute-enable {enable | disable}
set advanced-bot-protection-js-attribute <string>
set sys-perf-log-interval <interval>

```

end

Variable	Description	Default
admin-port <port_int>	Enter the port number on which the FortiWeb appliance listens for HTTP access to the web UI. The valid range is 1–65,535.	80
admin-sport <port_int>	Enter the port number on which the FortiWeb appliance listens for HTTPS (SSL-secured) access to the web UI. The valid range is 1–65,535.	443
admin-tls-v10 {enable disable}	Enable to specify TLS 1.0 clients can use to connect securely to the FortiWeb appliance.	disable
admin-tls-v11 {enable disable}	Enable to specify TLS 1.1 clients can use to connect securely to the FortiWeb appliance.	disable
admin-tls-v12 {enable disable}	Enable to specify TLS 1.2 clients can use to connect securely to the FortiWeb appliance.	enable

Variable	Description	Default
<code>admin-tls-v13 {enable disable}</code>	Enable to specify TLS 1.3 clients can use to connect securely to the FortiWeb appliance.	<code>disable</code>
<code>admin-ssl-custom-cipher <cipher1 cipher2 ...></code>	Enter the ciphers that are supported for the TLS 1.0, 1.1, 1.2 connections.	no default
<code>admin-tls13-custom-cipher <cipher1 cipher2 ...></code>	Enter the ciphers that are supported for the TLS 1.3 connections. Only available when <code>admin-tls-v13</code> is enabled.	no default
<code>admin-lockout-threshold <admin-lockout-threshold_int></code>	Enter the number of invalid logon attempts before the account is locked out. The valid range is 1–10.	3
<code>admin-lockout-duration <minutes_int></code>	Set the length of time the account remains locked. The valid range is 1–2147483647 seconds.	60
<code>admintimeout <minutes_int></code>	Enter 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 1–480. To improve security, do not increase the idle timeout.	5
<code>adom-admin {enable disable}</code>	Enable to be able to restrict administrator accounts to specific administrative domains. See also <code>domains <adom_name> in config system admin</code> . Note: After you type <code>end</code> , 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 <code>root</code> ADOM. To continue by configuring additional ADOMs, log in again, then go to Defining ADOMs on page 57 .	<code>disable</code>

Variable	Description	Default
auth-timeout <milliseconds_int>	Enter the number of milliseconds that FortiWeb will wait for the remote authentication server to respond to its query. The valid range is 1–60,000. 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> on page 528 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>	Enter 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 1–65,535. Caution: The port number must be different than the port number set using config server-policy custom-application application-policy (page 1).	8333
debug-monitor-interval <int>	It controls the frequency in minutes for collecting debug information. The valid range is 1 - 65535.	5

Variable	Description	Default
debug-memory-boundary <int>	The configuration sets the memory usage threshold (boundary) for collecting debug information. If memory usage exceeds the defined boundary and the top 10 processes include proxyd or ml_daemon, then the system will enable jemalloc debugging to generate jeprof.out files. The valid range is 1 - 100 (%).	70
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
fds-proxy {enable disable}	Enable to configure FortiWeb to act as a proxy for the FDN. FortiWeb proxy will obtain FortiGuard service packages from the default list of FDN servers and distribute the packages to other FortiWeb devices. On FortiWeb proxy, port 8989 is used as the listening port for the package update requests from other FortiWeb devices, and the concurrent connection limit is 128. When FortiWeb proxy receives downloading requests from several devices at the same time, the requests will be queued and processed one by one. With this option enabled, you can configure system autoupdate override on other FortiWeb devices so that they can connect with this FortiWeb proxy to update FortiGuard service packages. If you want to override the default FDN servers and specify a new address for the FortiWeb proxy to obtain FortiGuard service packages, see system fds proxy.	disable

Variable	Description	Default
force-us-only {enable disable}	Enable so that FortiWeb will receive FortiGuard service updates from FortiGuard servers located only in the United States.	disable
hostname "<host_name>"	Enter the host name of this FortiWeb appliance. Host names may include US-ASCII letters, numbers, hyphens, and underscores. The maximum length is 63 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 config router all (page 1) CLI command. - It is used in the command prompt of the CLI. - It is used as the SNMP system name. For details about SNMP, see system snmp sysinfo on page 379. The System Information widget and the config router all (page 1) 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 system dns on page 279.	FortiWeb
admin-HTTPS-pki-required {enable disable}	Enable to use certificate-based Web UI login. Before enabling this, please make sure the related configurations are set correctly. For details, see system admin-certificate ca on page 228, user pki-user on page 406, and user admin-usergrp on page 394.	disable

Variable	Description	Default
HTTPS-certificate "<certificate_name>"	Specifies the certificate that FortiWeb uses for the accesses to its Web UI through HTTPS. This must be one of the certificates stored locally on the FortiWeb for administration. For details, see system admin-certificate local on page 231 .	defaultcert
HTTPS-intermediate-certificate "<certificate_group_name>"	Specifies the intermediate CA group if any. See system admin-certificate intermediate-ca-group .	No default
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
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 websites 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.	english

Variable	Description	Default
	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 50. Note: This setting does not affect the display of the CLI.	
multi-factor-authentication {optional mandatory}	Configure to set 2FA for admin account security. - optional: only when an admin user enters correct username and password, the Token Code window pops up to require the token code for account security. - mandatory: only when an admin user enters correct username and password as well as the token code, the authentication can succeed for login.	optional
ntpserver {"<ntp_fqdn>" "<ntp_ipv4>"}	Enter the IP address or fully qualified domain name (FQDN) of a Network Time Protocol (NTP) server or pool, such as <code>pool.ntp.org</code>, to query in order to synchronize the FortiWeb appliance's clock. The maximum length is 63 characters. For details about NTP and to find the IP address of an NTP server that you can use, go to: http://www.ntp.org/	pool.ntp.org
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>".	enable

Variable	Description	Default
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.	disable
record-cli-fail-cmd {enable disable}	Enable so that FortiWeb will generate an event log if a CLI command fails or is executed incorrectly.	disable
refresh <seconds_int>	Enter the automatic refresh interval (in seconds) for the web UI's System Status Monitor widget. The valid range is 0–9,223,372,036,854,775,807. To disable automatic refreshes, type 0.	80
syncinterval <minutes_int>	Enter how often (in minutes) the FortiWeb appliance should synchronize its time with the Network Time Protocol (NTP) server. The valid range is 1–1440. To disable time synchronization, type 0.	60
tftp {enable disable}	Specify whether FortiWeb can perform backups, restoration, firmware updates and other tasks using TFTP.	enable
timezone "<time-zone-code_str>"	Enter the two-digit code for the time zone in which the FortiWeb appliance is located. The valid range is from 00 to 75. To display a list of time zone codes, their associated the GMT time zone offset, and contained major cities, type <code>set timezone ?</code>.	04
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	disable

Variable	Description	Default
	information about this command.	
cert-expire-check-time <cert-expire-check-time _ int>	Set the notification time (the days) before the certificate expires. The valid value range is 0-365. When the value is 0, it means no certificate expiration will be checked. When the value is 100, it means notification will be sent 100 days before the certificate expires.	0
ipv6-dad-ha {enable disable}	Enable to perform IPv6 DAD detection on the primary appliance in Active-Passive and standard Active-Active HA groups.	disable
updated-debug-log {enable disable}	Disable it if too many FDS disconnection logs are generated.	enable
fortiguard-anycast {enable disable}	If enabled, FortiWeb will be upgraded from the Anycast server. The default domain is globalupdate.fortinet.net and the corresponding USG domain name is usupdate.fortinet.net. If disabled, FortiWeb will be upgraded from the original server, the default domain is update.fortiguard.net and the corresponding USG domain name is usupdate.fortiguard.net.	disable
power-status {enable disable}	Enable to show the power status.	disable
shell-access {enable disable}	Enable Shell access through SSH.	disable
shell-username <user_ name>	Enter the user name for Shell access.	N/A
shell-password <password>	Enter the password for Shell access.	N/A
shell-timeout <int>	Enter the time period after which the Shell access will be expired. The valid range is 1-1200 minutes.	10
shell-history-size	Specify the size of the command history file which is stored in "\$HOME/.ash_history".	1024

Variable	Description	Default
	Using <code>diag cli</code> command to view the history of the commands executed in Shell. The valid range is 1-4096 lines.	
shell-trusthostv4	Specify the IPv4 addresses or range of the trust-hosts who are allowed to access FortiWeb through Shell.	0.0.0.0/0
shell-trusthostv6	Specify the IPv6 addresses or range of the trust-hosts who are allowed to access FortiWeb through Shell.	::/0
admin-forticloud-sso-login {enable disable}	Enable this option to allow accounts created in FortiCloud Account Services to access FortiWeb. Once enabled, the following option will show on the FortiWeb Login page.  Sign in with FortiCloud The permission of these accounts in FortiWeb will be consistent with the ones in FortiCloud Account Services, either Read-Only or Read-Write for all the areas of configurations.	disable
advanced-bot-protection {enable disable}	Enable the bot detection service provided by FortiGuard Advanced Bot Protection. For more information on this service, see fortiabp.forticloud.com. For the whole process of the FortiGuard ABP integration configuration, refer to "Configuring Advanced Bot Protection policy" in <i>FortiWeb Administration Guide</i>.	disable
advanced-bot-protection-portal-domain <fortiabp.forticloud.com>	Enter the address of FortiGuard Advanced Bot Protection. This is a fixed address, which should be set as <code>us.mtls.fortiabp.forticloud.com</code> .	us.mtls.fortiabp.forticloud.com
advanced-bot-protection-query-timeout <int>	FortiWeb will stop connecting with FortiGuard Advanced Bot Protection if the query has been failed for the specified period. The valid range is 1-10.	6

Variable	Description	Default
advanced-bot-protection-js-attribute-enable {enable disable}	Enable to add js attribute to script tag.	enable
advanced-bot-protection-js-attribute <string>	Configure the js attribute to add. The default value is set to "async"	async
sys-perf-log-interval <interval>	FortiWeb generates system performance logs every 5 minutes. This data is sent to the connected FortiAnalyzer to display in its dashboard widget. You can run this command to change the log generation interval, measured in minutes. The default value is 5, and the valid range is 0-15. A value of 0 disables this feature.	5

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 08
    set ntpsync enable
    set ntpserver "pool.ntp.org"
    set syncinterval 30
end
```

For an example that includes a host name, see [system dns on page 279](#).

Related topics

- [system admin on page 223](#)
- [system autoupdate schedule on page 242](#)
- [system interface on page 344](#)
- [system dns on page 279](#)
- [system advanced on page 233](#)
- [router static on page 101](#)
- [date on page 828](#)
- [time on page 856](#)
- [system status on page 864](#)

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 and operate independently.

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



If you have multiple FortiWeb appliances but do **not** need failover, you can still synchronize the configuration. This can be useful for cloned network environments and externally load-balanced active-active HA. For details, see "[server-policy custom-application application-policy](#)" on page 1.

Unless specially stated, the configurations of `config system ha` can be automatically synchronized from primary to secondary appliances.

For more information on HA, including troubleshooting, failover behavior, synchronized data, and network topology, see the *FortiWeb high availability (HA)* section under *Key Concepts* chapter in *FortiWeb Administration Guide*:

<https://docs.fortinet.com/document/fortiweb>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system ha
  set mode {active-passive | active-active-standard | active-active-high-volume
    |standalone}
  set group-id <group_int>
  set group-name "<pair-name_str>"
  set sdn-connector <string>
  set lb-ocid <string>
  set priority <level_int>
  set override {enable | disable}
  set network-type {flat | udp-tunnel}
  set tunnel-local "<tunnel-local_str>"
  set tunnel-peer "<tunnel-peer_str>"
  set hbdev "<interface_name>"
  set hbdev-backup "<interface_name>"
  set lacp-ha-secondary {enable | disable}
  set link-failed-signal {enable | disable}
  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>"
```

```

set schedule {ip | leastconnection | round-robin}le {ip | leastconnection | round-
  robin}
set session-sync-broadcast {enable | disable}
set session-sync-dev {"<interface_name>" ...}
set session-warm-up <seconds_int>
set weight-1 <weight_int>
set weight-2 <weight_int>
set weight-3 <weight_int>
set weight-4 <weight_int>
set weight-5 <weight_int>
set weight-6 <weight_int>
set weight-7 <weight_int>
set weight-8 <weight_int>
set session-pickup {enable | disable}
set persistence-sync {enable | disable}
set hlck-sync {enable | disable}
set hlck-period-sync {enable | disable}
set hlck-period-timeout <integer>
set eip-addr <class_ip>
set eip-aid <eip-aid_str>
set ha-eth-type <ha-eth-type_str>
set hc-eth-type <hc-eth-type_str>
set hbcast-eth-type <hbcast-eth-type_str>
set l2ep-eth-type <l2ep-eth-type_str>
set l7-persistence-sync {enable | disable}
set server-policy-hlck {enable | disable}
set encryption {enable | disable}
set key <passwd>
end

```

Variable	Description	Default
mode {active-passive active-active-standard active-active-high-volume 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. - active-active-standard—The primary appliance in a standard active-active HA group plays the role as the central controller to receive traffic from clients and send the processed traffic to back-end web servers, and vice versa. The primary appliance distributes the traffic to all the HA members (including itself) according to the specified load-balancing algorithm so that each FortiWeb appliance performs the security services to protect the traffic. - active-active-high-volum—Unlike the standard active-active HA mode where the primary acts as a traffic distributor, the members in high volume active-active mode don't reply on the primary to distribute traffic, instead, they can directly	standalone

Variable	Description	Default
	receive traffic from the clients and process the traffic independently. It significantly increases the traffic throughput of the HA group. <code>standalone</code>—Operate each appliance independently. Note: To avoid connectivity issues, do not use <code>config system ha</code> to remove an appliance from an HA cluster. Instead, use ha disconnect on page 833, which removes the appliance from the cluster and changes the HA mode to standalone.	
<code>group-id <group_int></code>	Enter a number that identifies the HA pair. Both members of the HA pair must have the same group ID. If you have more than one HA pair on the same network, each HA pair must have a different group ID. Changing the group ID changes the cluster's virtual MAC address. The valid range is 0 to 63.	0
<code>group-name "<pair-name_str>"</code>	Enter 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 63 characters.	No default.
<code>sdn-connector <string></code>	Select the OCI SDN connector you have created. See system sdn-connector. Available only when FortiWeb-VM is deployed in active-passive mode on OCI.	No default.
<code>lb-ocid <string></code>	Enter the Load Balancer's OCID. To get the Load Balancer OCID: 1. Log in to OCI. 2. Go to Core Infrastructure > Networking > Load Balancers. 3. Click the load balancer used for the HA cluster. 4. Copy the OCID of this load balancer. Available only when FortiWeb-VM is deployed in active-passive mode on OCI.	No default.
<code>priority <level_int></code>	Enter 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 ha manage on page 835. This setting is optional. The smaller the number, the higher the priority. The valid range is 0 to 9.	5

Variable	Description	Default
	This setting can't be synchronized from primary to secondary appliances. You should configure it on each HA member. Note: - By default, unless you enable override {enable disable} on page 322, uptime is more important than this setting. - This setting can't be synchronized from primary to secondary appliances. You should configure it on each HA member. It's suggested to leave it with default value.	
override {enable disable}	Enable to make priority <level_int> on page 321 a more important factor than uptime when selecting the primary appliance.	disable
network-type {flat udp-tunnel}	Select the common HA mode flat or udp-tunnel mode on OpenStack platform.	flat
tunnel-local "<tunnel-local_ str>"	Set the local IP address on OpenStack platform. This filed can be configured only when the network type is upd-tunnel. Note: This setting can't be synchronized from primary to secondary appliances. You should configure it on each HA member. It's suggested to leave it with default value.	No default.
tunnel-peer "<tunnel-peer_ str>"	Set the peer IP address on OpenStack platform. This filed can be configured only when the network type is upd-tunnel. Note: This setting can't be synchronized from primary to secondary appliances. You should configure it on each HA member. It's suggested to leave it with default value.	No default.
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 <code>port3</code> for the primary heartbeat link, connect <code>port3</code> on this appliance to <code>port3</code> 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.	No default.

Variable	Description	Default
	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 page 323) 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.	
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>" on page 322. 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 <code>port4</code> for the secondary heartbeat link, connect <code>port4</code> on this appliance to <code>port4</code> 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.
lACP-ha-secondary {enable disable}	Enable to provide support for 2 LACP interfaces, also known as "bridges," "V-zones," or "aggregated links." For more information about configuring bridges, see the <i>FortiWeb Administration Guide</i>: http://docs.fortinet.com/fortiweb/admin-guides	disable
link-failed-signal {enable disable}	Enable to ensure that all equipment in the network detects the new primary unit in a cluster after a failover occurs.	disable

Variable	Description	Default
	When a failover occurs in an HA active-passive cluster, the new primary unit broadcasts gratuitous ARP packets so that switches will refresh their MAC forwarding tables and detect the new primary unit. However, sometimes switches will not immediately detect a failover and refresh MAC forwarding tables to recognize a new primary unit. This command shuts down each interface (except for the heartbeat interfaces and reserve management interfaces) of the former primary unit for about a second so that any remaining equipment that did not automatically detect the failover will refresh their MAC forwarding tables and recognize the new primary unit,	
arps <arp_int>	Enter the number of times that the FortiWeb appliance will broadcast address resolution protocol (ARP) packets (IPv4 environment) or Neighbor Solicitation (NS) packets (IPv6 environment) 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> on page 324. 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 1–16.	10
arp-interval <seconds_int>	Enter the number of seconds to wait between each broadcast of ARP/NS packets.	3

Variable	Description	Default
	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 1–20.	
hb-interval <milliseconds_int>	Enter 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 1–20 (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> on page 325 to prevent inadvertent failover from occurring before the initial synchronization.	1
hb-lost-threshold <seconds_int>	Enter 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.	3

Variable	Description	Default
	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 1–60. 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> on page 325 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 system snmp community on page 375.	
monitor { "<interface_name>" ... }	Enter 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>	Enter 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.	30

Variable	Description	Default
	The valid range is 1–100 seconds.	
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 can configure up to eight reserve management ports in each HA cluster. You cannot configure routing for the port you select.	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.
schedule {ip leastconnection round-robin}	Specifies the load-balancing algorithm used by the primary appliance (in an active-active HA cluster) to distribute received traffic over the available cluster members. • <code>ip</code>—Consistently distribute the traffic coming from a source to the same cluster member. • <code>leastconnection</code>—Dynamically distribute traffic to a cluster member who has the fewest connections processing. • <code>round-robin</code>—Distribute traffic among the available members in a circular order. Note that FortiWeb's Session Management is not supposed by the active-active HA deployment with the algorithm By connections or Round-robin being used for the load-balancing. Available only when <code>mode {active-passive active-active-standard active-active-high-volume standalone}</code> on page 320 is <code>active-active-standard</code> or <code>active-active-high-volume</code>.	ip
session-sync-broadcast {enable disable}	Specifies whether the primary appliance in an active-active HA cluster synchronizes sessions to others in broadcast. By default, session information is synchronized in unicast. Broadcast will be recommended if a active-active HA cluster contains many appliances.	disable

Variable	Description	Default
	Available only when <code>mode {active-passive active-active-standard active-active-high-volume standalone}</code> on page 320 is <code>active-active-standard</code> or <code>active-active-high-volume</code> .	
<code>session-sync-dev { "<interface_name>" ... }</code>	The primary appliance use the heartbeat interface (<code>hbdev "<interface_name>"</code> on page 322) to synchronize its session table to other appliances in an active-active HA cluster by default. However, you can use extra interfaces (up to four interfaces) for the session synchronization when the HA cluster is in heavy traffic. Specifies the network interface(s) of this FortiWeb appliance for session synchronizations. For example, typing <code>set session-sync-dev port3 port4 port5</code> for using port3, port4 and port5 to synchronize session information. Note: - Only the primary appliance in the active-active HA cluster is allowed to set <code>session-sync-dev</code>. The configuration here will be synchronized to all the secondary appliance in the cluster by the primary, and all the appliances send or receive session information with the same interface configuration. - The heartbeat interface will not participate in the session synchronization anymore if other interfaces are specified here. - It can not specify the heartbeat interface to <code>session-sync-dev</code>. - Available only when <code>mode {active-passive active-active-standard active-active-high-volume standalone}</code> on page 320 is <code>active-active-standard</code> or <code>active-active-high-volume</code>.	No default.
<code>session-warm-up <seconds_int></code>	Specifies the active-active HA warm-up time that the primary appliance will hold traffic distribution to wait for the active-active HA negotiation (determine the primary and secondary, and necessary synchronizations) completes (when every time the active-active HA starts). Available only when <code>mode {active-passive active-active-standard active-active-high-volume standalone}</code> on page 320 is <code>active-active-standard</code> or <code>active-active-high-volume</code>.	10
<code>weight-1 <weight_int></code>	When the <code>system ha</code> on page 319 algorithm is <code>ip</code> , sets the weight for the first unit in an active-active HA cluster.	1

Variable	Description	Default
	The primary unit performs weighted round-robin according to the specified weight to distribute the first packet coming from the source IP to cluster members. The weight of each unit can be set with a range of 0–256.	
weight-2 <weight_int>	When the <code>schedule</code> algorithm is <code>ip</code> , sets the weight for the second unit in an active-active HA cluster. The primary unit performs weighted round-robin according to the specified weight to distribute the first packet coming from the source IP to cluster members. The weight of each unit can be set with a range of 0–256.	1
weight-3 <weight_int>	When the system ha on page 319 algorithm is <code>ip</code> , sets the weight for the third unit in an active-active HA cluster. The primary unit performs weighted round-robin according to the specified weight to distribute the first packet coming from the source IP to cluster members. The weight of each unit can be set with a range of 0–256.	1
weight-4 <weight_int>	When the system ha on page 319 algorithm is <code>ip</code> , sets the weight for the fourth unit in an active-active HA cluster. The primary unit performs weighted round-robin according to the specified weight to distribute the first packet coming from the source IP to cluster members. The weight of each unit can be set with a range of 0–256.	1
weight-5 <weight_int>	When the system ha on page 319 algorithm is <code>ip</code> , sets the weight for the fifth unit in an active-active HA cluster. The primary unit performs weighted round-robin according to the specified weight to distribute the first packet coming from the source IP to cluster members. The weight of each unit can be set with a range of 0–256.	1
weight-6 <weight_int>	When the system ha on page 319 algorithm is <code>ip</code> , sets the weight for the sixth unit in an active-active HA cluster. The primary unit perform weighted round-robin according to the specified weight to distribute the first packet coming from the source IP to cluster members. The weight of each unit can be set with a range of 0–256.	1
weight-7 <weight_int>	When the system ha on page 319 algorithm is <code>ip</code> , sets the weight for the seventh unit in an active-active HA cluster. The primary unit performs weighted round-robin according to the specified weight to distribute the first packet coming from the source IP to cluster members.	1

Variable	Description	Default
	The weight of each unit can be set with a range of 0–256.	
weight-8 <weight_int>	When the system ha on page 319 algorithm is <code>ip</code>, sets the weight for the eighth unit in an active-active HA cluster. The primary unit performs weighted round-robin according to the specified weight to distribute the first packet coming from the source IP to cluster members. The weight of each unit can be set with a range of 0–256.	1
session-pickup {enable disable}	Enable so that the primary unit in the HA cluster synchronizes the session table with all cluster units. If a cluster unit fails, the HA session table information is available to the remaining cluster units which can use the session table to resume connections without interruption. Enable for session fail-over protection. If this is not required, disabling may reduce CPU usage and reduce HA heartbeat network bandwidth usage. Note: Only sessions that have been established for longer than 30 seconds will be synchronized.	disable
persistence-sync {enable disable}	Enable/disable the persistence synchronization.	disable
eip-addr <class_ip>	Enter the elastic IP address for HA on AWS.	No default.
eip-aid <eip-aid_str>	Enter the ID of the elastic IP for HA on AWS.	No default.
ha-eth-type <ha-eth-type_str>	HA heartbeat packet Ethertype (4-digit hex). The range is 0x8890–0x889F. Note: This setting can't be synchronized from primary to secondary appliances. You should configure it on each HA member. It's suggested to leave it with default value.	0x8890
hc-eth-type <hc-eth-type_str>	Tuple session HA heartbeat packet Ethertype (4-digit hex). The range is 0x8890–0x889F. Note: This setting can't be synchronized from primary to secondary appliances. You should configure it on each HA member. It's suggested to leave it with default value.	8891
hbcast-eth-type <hbcast-eth-type_str>	Broadcast HA heartbeat packet Ethertype (4-digit hex). The range is 0x8890–0x889F.	8893

Variable	Description	Default
l2ep-eth-type <l2ep-eth-type_ str>	Telnet session HA heartbeat packet Ethertype (4-digit hex). The range is 0x8890–0x889F. Note: This setting can't be synchronized from primary to secondary appliances. You should configure it on each HA member. It's suggested to leave it with default value.	8894
17-persistence- sync {enable disable}	When FortiWeb is operating in HA Active-Passive (AP) mode, you can enable Layer 7 Persistence Synchronization. This option enables session synchronization when there's a failover that causes the secondary appliance to take over as the new primary, and is useful for web applications that require sticky sessions.	disable
hlck-sync {enable disable}	Enable to synchronize the back-end servers' health check status from the primary to the secondary nodes. This ensures that when an HA fail-over occurs, the new primary FortiWeb appliance can immediately know the health status of the back-end servers, ensuring seamless traffic continuity during fail-over.	disable
hlck-period-sync {enable disable}	By default, the health check status is synchronized when there are changes in the back-end server health check status. Use this command if you prefer to synchronize it periodically instead.	disable
hlck-period- timeout <integer>	The interval of the health check status synchronization. The default interval is 3000 seconds. The valid range is 600-3000.	3,000
server-policy-hlck {enable disable}	Enable to check the server policy health. Server policy health check is only available if the operation mode is Reverse Proxy, and the HA mode is Active-Active.	disable
encryption {enable disable}	Enable to encrypt the heartbeat traffic between primary and secondary appliances. If you want to set an HA group, make sure the encryption status is the same across all members, otherwise the HA group can't successfully be built.	disable
key <passwd>	Enter the password to encrypt the heartbeat traffic between primary and secondary appliances when they are in Federal Information Processing Standards (FIPS) mode or in non-FIPS mode with <code>encryption</code> enabled.	ffffffffe12345678

Variable	Description	Default
	Note: This setting can't be synchronized from primary to secondary appliances. You should configure it on each HA member, and the password on all the members should be the same. It's suggested to leave it with default value.	

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

- [system interface on page 344](#)
- ["debug application hasync" on page 1](#)
- ["debug application hataalk" on page 1](#)
- [system ha status on page 808](#)
- [ha disconnect on page 833](#)
- [ha manage on page 835](#)
- [ha synchronize on page 836](#)
- [system status on page 864](#)

system ha-aa-server-policy-hlck

To check whether the server policies are running properly on the HA cluster, you can configure server policy health check. The configurations are synchronized to all members in the cluster. The system sends an HTTP or HTTPS request, and waits for a response that matches the values required by the health check rule. A timeout indicates that the

connection between the HA cluster member and the back-end server is not available. The system then generates event logs. The primary node will not distribute traffic to this HA member until the connection is recovered.

Server policy health check is only available if the operation mode is **Reverse Proxy**, and the HA mode is **Active-Active-Standard**.

You should first enable the **HA Health Check** option on the **HA** tab in **System > High Availability > Settings**, or enable it through the command `config system ha`, then configure a health check on the **HA Health Check** tab.

FortiWeb only supports checking the health of server policies in the root administrative domain.

To use this command, your administrator account's access control profile must have `rw` or `w` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system ha-aa-server-policy-hlck
  edit "<health-check_id>"
    set HTTPS {enable | disable}
    set client-cert <client-certificate-name>
    set relationship {and | or}
    config health-list
      edit <entry_index>
        set time-out <seconds_int>
        set retry-times <retries_int>
        set interval <seconds_int>
        set url-path "<request_str>"
        set method {get | head | post}
        set match-type {response-code | match-content | all}
        set response-code {response-code_int}
        set match-content "<match-content_str>"
      next
    end
  next
end
```

Variable	Description	Default
"<health-check_id>"	Enter the ID of the server policy health check. The maximum length is 63 characters. To display the list of existing server health checks, enter: <code>edit ?</code>	No default.
HTTPS {enable disable}	Enable to use the HTTPS protocol for the health check connections with the back-end server. The system uses HTTP protocol if this option is disabled. You can configure the client certificate for the connection.	
client-cert <client-certificate-name>	If HTTPS is enabled, you can specify a Client Certificate for the connection. This is optional.	

Variable	Description	Default
	The Client Certificate is imported on GUI in System > Certificates > Local or by CLI command <code>config system certificate local</code> .	
relationship {and or}	<code>and</code>—FortiWeb considers the server to be responsive when it passes all the tests in the list. <code>or</code>—FortiWeb considers the server to be responsive when it passes at least one of the tests in the list.	and
<entry_index>	Enter the index number of the individual rule in the table. The valid range is 1–16.	No default.
timeout <seconds_int>	Enter the number of seconds which must pass after the server health check to indicate a failed health check. The valid range is 1–10 .	3
retry-times <retries_int>	Enter 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 1–10.	3
interval <seconds_int>	Enter the number of seconds between each server health check. The valid range is from 1–10.	10
url-path "<request_str>"	Enter the URL, such as <code>/index.html</code> , 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 <code>match-content</code> , FortiWeb considers it to be responsive.	No default.
method {get head post}	Specify whether the health check uses the HEAD, GET, or POST method.	get
match-type {response-code match-content all}	<code>response-code</code>—If the web server successfully returns the URL specified by <code>url-path</code> and the code specified by <code>response-code</code>, FortiWeb considers the server to be responsive. <code>match-content</code>—If the web server successfully returns the URL specified by <code>url-path</code> and its content matches the <code>match-content</code> value, FortiWeb considers the server to be responsive. <code>all</code>—If the web server successfully returns the URL specified by <code>url-path</code> and its content matches the <code>match-content</code> value, and the code specified by <code>response-code</code>, FortiWeb considers the server to be responsive.	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 <code>match-type</code> is <code>response-code</code> or <code>all</code> .	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 <code>match-type</code> is <code>match-content</code> or <code>all</code> .	No default.

Example

This example configures a server policy health check that periodically requests the main page of the website, `/index`. If FortiWeb can't receive responses containing the required page (which contains the word "About") every 10 seconds (the default), and the check fails at least three times in a row, FortiWeb considers the connection between itself and the server being broken. The primary node will then stop distributing traffic to this HA member until the connection is recovered.

```
config config system ha-aa-server-policy-hlck
  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
```

system ha-mgmt-router-static

For a FortiWeb appliance in an HA group, the configurations set by `config router policy` and `config router static` are synchronized by all the group members, but the configurations set by HA Mgmt Static Route or HA Mgmt Policy route are applied only to this specific member.

Use this command to add or delete a static route that is used only by this HA member. It is useful when you want to connect this cluster member to back-end servers that are not in the server pool of the HA group.

To use this command, your administrator account's access control profile must have `rw` or `w` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).



Only one default route (the static route with destination as 0.0.0.0/0) is allowed on FortiWeb appliance. For example, if you have configured a default route in **Network > Route**, then it's not allowed to configure another default route in HA route settings.

Syntax

```
config system ha-mgmt-router-static
  edit <route_index>
    set device "<interface_name>"
    set dst "<destination_ip>"
    set gateway "<router_ip>"
  next
end
```

Variable	Description	Default
<route_index>	Enter 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 0–65,535.	No default.
device "<interface_name>"	Enter the name of the network interface, such as <code>port1</code> , through which traffic subject to this route will be outbound. The maximum length is 63 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 <code>0.0.0.0 0.0.0.0</code> or <code>::/0</code> .	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

system ha-mgmt-router-policy

For a FortiWeb appliance in an HA group, the configurations set by `config router policy` and `config router static` are synchronized by all the group members, but the configurations set by `HA Mgmt Static Route` or `HA Mgmt Policy route` are applied only to this specific member.

Use this command to add or delete a policy route that is used only by this HA member. It is useful when you want to connect this cluster member to back-end servers that are not in the server pool of the HA group.

To use this command, your administrator account's access control profile must have `rw` or `w` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system ha-mgmt-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 <priority_int>
next
end

```

Variable	Description	Default
<policy_index>	Enter the index number of the policy route. The valid range is 0–65,535.	No default.
"<incoming_interface_name>"	Enter the name of the interface, such as <code>port1</code> , 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
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 <code>port2</code> , 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. A gateway address is not required for the particular routing policies used as static routes in an one-arm topology. Leave this blank for a one-arm network topology.	0.0.0.0
priority <priority_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

system ha-node

For the high volume active-active mode, you should allocate appliances to the HA group.

Syntax

```

config system ha-node
  edit <HA_node_number>

```

```

        set <HA_node_device_SN>
    next
end

```

Variable	Description	Default
<HA_node_number>	The index number of the node to be selected as an HA group member.	N/A
<HA_node_device_SN>	The serial number of the node.	N/A

Example

```

config system ha-node
    edit 1
        set sn FV100XXXXXXXXXXXX
    next
end

```

system icapserver

Use this command to configure FortiWeb to submit all files that match your upload restriction rules to ICAP server.

ICAP server evaluates whether the file poses a threat and returns the result to FortiWeb. If ICAP determines that the file is malicious, FortiWeb performs the following tasks:

- Generates an attack log message that contains the result.
- Takes the action specified by the file security policy. During this time, it does not re-submit the file to ICAP server.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```

config system icapserver
    set server "<server_ipv4>"
    set cache-timeout <timeout_int>
    set port <port_int>
    set elog {enable | disable}
    set service-name <name_str>
    set ssl {enable | disable}
end

```

Variable	Description	Default
server "<server_ipv4>"	Enter the IP address or domain name of the ICAP server to send files to.	No default.

Variable	Description	Default
port <port_int>	Enter the port on which the ICAP server is listening. When ssl {enable disable} on page 339 is enable, the default port is 11344, while when ssl {enable disable} on page 339 is disable, the default port is 1344.	1344 or 11344
cache-timeout <timeout_int>	After it receives the ICAP results, FortiWeb takes the action specified by the file security policy. During this time, it does not re-submit the file to ICAP server. The valid range is 1-168 hours.	72
elog {enable disable}	Enter so that FortiWeb will report event logs when it successfully submits files to FortiSandbox.	disable
service-name <name_str>	The name of the ICAP service, which appears in the URL configured in the ICAP client. For example, <code>icap://<ip_address>/<name></code> .	No default
ssl {enable disable}	Enable to encrypt the transmission. The port varies depending on whether this option is enabled or not.	disable

Example

This example creates a connection to an ICAP server at `192.0.2.2` that retrieves statistics and sends a weekly report to `admin@example.com`.

```
config system icapserver
    set server "192.0.2.2"
    set ssl enable
    set cache-timeout 5
end
```

Related topics

- [waf file-upload-restriction-policy on page 497](#)
- [log reports on page 77](#)

system ha-traffic-distribution

The domain name of your application is paired with one or more IP addresses. These IP addresses are called Virtual IPs in FortiWeb. When your users visit your application, the destination of these requests are these virtual IP addresses. If you have deployed a FortiWeb HA cluster in your network, these requests will arrive first at FortiWeb cluster for threat detection, then be forwarded to the back-end servers. The traffic distribution controls which FortiWeb appliances in the cluster process the traffic destined to certain virtual IPs.

Syntax

```
config system ha-traffic-distribution
  edit <traffic-distribution_name>
    set node-order <the_index_of_node_with_highest_priority>
    set node-order <the_index_of_node_with_secondary_priority>
    set node-order <the_index_of_node_with_third_priority>
    ...
    set vip-list <vip_names>
  next
end
```

Variable	Description	Default
<traffic-distribution_name>	The name of the traffic distribution.	N/A
node-order <the_index_of_node_with_highest_priority>	The priority order of the nodes that process the traffic to the VIP.	N/A
node-order <the_index_of_node_with_secondary_priority>	The node with the highest priority processes the traffic to the specified VIPs. If this node is down, the secondary node takes over the traffic, and so on.	
node-order <the_index_of_node_with_third_priority>		
...		
vip-list <vip_names>	The name of the VIP. You can assign the same VIP to different traffic distributions.	N/A

Example

```
config system ha-traffic-distribution
  edit traffic1
    set node-order 2
    set node-order 3
    set node-order 1
    set vip-list vip1
  next
end
```

system hsm info

Use this command to edit the configuration so that FortiWeb will work with SafeNet Network HSM 7 (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*:

<https://docs.fortinet.com/document/fortiweb>

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 server-policy setting
    set high-compatibility-mode enable
    set hsm enable
end
```

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system hsm info
    set ip "<hsm_ipv4>"
    set port <port_int>
    set timeout <timeout_int>
    set filename "<filename_str>"
    set register-status {enable| disable}
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.
register-status {enable disable}	Enable to create FortiWeb as a client of the HSM.	disable

Related topics

- [system hsm partition on page 342](#)
- [system certificate local on page 258](#)

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 server-policy setting
    set hsm enable
```

For additional HSM integration settings, see [system hsm info on page 340](#).

For detailed information on integrating HSM with FortiWeb, see the *FortiWeb Administration Guide*:

<https://docs.fortinet.com/document/fortiweb>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

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

- [system hsm info on page 340](#)
- [system certificate local on page 258](#)

system icapserver

Use this command to configure FortiWeb to submit all files that match your upload restriction rules to ICAP server.

ICAP server evaluates whether the file poses a threat and returns the result to FortiWeb. If ICAP determines that the file is malicious, FortiWeb performs the following tasks:

- Generates an attack log message that contains the result.
- Takes the action specified by the file security policy. During this time, it does not re-submit the file to ICAP server.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system icapserver
  set server "<server_ipv4>"
  set cache-timeout <timeout_int>
  set port <port_int>
  set elog {enable | disable}
  set service-name <name_str>
  set ssl {enable | disable}
end
```

Variable	Description	Default
server "<server_ipv4>"	Enter the IP address or domain name of the ICAP server to send files to.	No default.
port <port_int>	Enter the port on which the ICAP server is listening. When <code>ssl {enable disable}</code> on page 343 is enable, the default port is 11344, while when <code>ssl {enable disable}</code> on page 343 is disable, the default port is 1344.	1344 or 11344
cache-timeout <timeout_int>	After it receives the ICAP results, FortiWeb takes the action specified by the file security policy. During this time, it does not re-submit the file to ICAP server. The valid range is 1-168 hours.	72
elog {enable disable}	Enter so that FortiWeb will report event logs when it successfully submits files to FortiSandbox.	disable
service-name <name_str>	The name of the ICAP service, which appears in the URL configured in the ICAP client. For example, <code>icap://<ip_address>/<name></code> .	No default
ssl {enable disable}	Enable to encrypt the transmission. The port varies depending on whether this option is enabled or not.	disable

Example

This example creates a connection to an ICAP server at 192.0.2.2 that retrieves statistics and sends a weekly report to admin@example.com.

```
config system icapserver
  set server "192.0.2.2"
  set ssl enable
  set cache-timeout 5
end
```

Related topics

- [waf file-upload-restriction-policy on page 497](#)
- [log reports on page 77](#)

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 [system admin on page 223](#).



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



The Link Aggregation Control Protocol (LACP) Interface and Redundant Interface are currently supported only when FortiWeb is deployed in Reverse Proxy or True Transparent Proxy mode. It can be applied to VLAN subinterfaces. It cannot be applied to ports that are used for the HA heartbeat, but it can be applied to monitor ports in an HA cluster. It is not supported in FortiWeb-VM.

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 [system snmp community on page 375](#).

To use this command, your administrator account's access control profile must have either `rw` permission to the `netgrp` area. For details, see [Permissions on page 46](#).

Syntax

```

config system interface
  edit "<interface_name>"
    set status {up | down}
    set type {aggregate | physical | vlan | redundant}
    set algorithm {layer2 | layer2_3 | layer3_4}
    set allowaccess {HTTP HTTPS ping snmp ssh FortiWeb-manager}
    set ip6-allowaccess {HTTP HTTPS ping snmp ssh FortiWeb-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 ip6-mode {static | dhcp}
    set vlanid <vlan-id_int>
    set vlanproto {8021q | 8021ad}
    set lacp-speed {fast | slow}
    set mtu <mtu_int>
    set system interface
    set system interface
    set system interface
    set system interface
  config secondaryip
    edit <entry_index>
      set ip {"<interface_ipv4mask>" | "<interface_ipv6mask>"}
    next
  end
next
end

```

Variable	Description	Default
"<interface_name>"	Enter the name of a network interface. The maximum length is 15 characters.	No default.
status {up down}	Enable (select <code>up</code>) 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 <code>config system interface</code> to configure <code>port1</code> with <code>set status up</code>, if the cable is physically unplugged, <code>diagnose hardware nic list port1</code> may indicate correctly that the link is down (Link detected: no).	up
algorithm {layer2 layer2_3 layer3_4}	Select the connectivity layers that will be considered when distributing frames among the aggregated physical ports. <code>layer2</code>—Consider only the MAC address. This results in the most even distribution of frames, but may be disruptive to TCP if packets frequently arrive	layer2

Variable	Description	Default
	out of order. <code>layer2_3</code>—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. <code>layer3_4</code>—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.	
<code>allowaccess {HTTP HTTPS ping snmp ssh FortiWeb-manager}</code>	Enter the IPv4 protocols that will be permitted for administrative connections to the network interface or VLAN sub-interface. Separate each protocol with a space. To remove from or add to the list of permitted administrative access protocols, retype the entire list. <code>ping</code>—Allow ICMP ping responses from this network interface. <code>HTTP</code>—Allow HTTP access to the web UI. The HTTP access to FortiWeb's GUI will be automatically redirected to HTTPS, so you can't enable HTTP alone, it should be enabled along with HTTPS. <code>HTTPS</code>—Allow secure HTTP (HTTPS) access to the web UI. <code>snmp</code>—Allow SNMP access. For details, see system snmp community on page 375. Note: This setting only configures which network interface will receive SNMP queries. To configure which network interface will send traffic, see system snmp community on page 375. <code>ssh</code>—Allow SSH access to the CLI. <code>FortiWeb-manager</code> — 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.	<code>ping</code> <code>HTTPS</code> <code>ssh</code>

Variable	Description	Default
ip6-allowaccess {HTTP HTTPS ping snmp ssh FortiWeb-manager}	Enter 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. • <code>ping</code>—Allow ICMP ping responses from this network interface. • <code>HTTP</code>—Allow HTTP access to the web UI. The HTTP access to FortiWeb's GUI will be automatically redirected to HTTPS, so you can't enable HTTP alone, it should be enabled along with HTTPS. • <code>HTTPS</code>—Allow secure HTTP (HTTPS) access to the web UI. • <code>snmp</code>—Allow SNMP access. For details, see system snmp community on page 375. Note: This setting only configures which network interface will receive SNMP queries. To configure which network interface will send traffic, see system snmp community on page 375. • <code>ssh</code>—Allow SSH access to the CLI. • <code>FortiWeb-manager</code> — 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>"	Enter 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.
interface "<interface_name>"	Enter the name of the network interface with which the VLAN subinterface will be associated. The maximum length is 15 characters.	No default.

Variable	Description	Default
	This field is available only if type {aggregate physical vlan redundant} on page 348 is <code>vlan</code> .	
<code>intf {"<port_name>" ...}</code>	Enter 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 {aggregate physical vlan redundant} on page 348 is <code>vlan</code> .	No default.
<code>ip "<interface_ipv4mask>"</code>	Enter 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 <code>192.168.1.99</code> with a netmask of <code>255.255.255.0</code> . Other ports have no default.	Varies by the interface.
<code>ip6 "<interface_ipv6mask>"</code>	Enter 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
<code>lacp-speed {fast slow}</code>	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
<code>type {aggregate physical vlan redundant}</code>	Indicates whether the interface is directly associated with a single physical network port, a group of redundant interfaces, 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 (<code>physical</code>) or creating a new subinterface/aggregate (<code>vlan</code> or <code>aggregate</code>).	Varies by the interface.
<code>mode {static dhcp}</code>	Specify whether the interface obtains its IPv4 address and netmask using DHCP.	static
<code>ip6-mode {static dhcp}</code>	Specify whether the interface obtains its IPv6 address and netmask using DHCP.	static

Variable	Description	Default
vlanid <vlan-id_int>	Enter 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 <i>FortiWeb Administration Guide</i>: https://docs.fortinet.com/document/fortiweb This field is available only when <code>type {aggregate physical vlan redundant}</code> on page 348 is <code>vlan</code>. 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
vlanproto {8021q 8021ad}	Select either the VLAN type 802.1Q or 802.1ad.	802.1Q
<entry_index>	Enter the index number of the individual entry in the table.	No default.
ip {"<interface_ipv4mask>" "<interface_ipv6mask>"}	Type an additional IPv4 or IPv6 address and netmask for the network interface. Available only when <code>ip-src-balance</code> or <code>ip6-src-balance</code> is enabled. For details, see system network-option on page 355.	No default.

Variable	Description	Default
mtu <mtu_int>	Enter the maximum transmission unit (MTU) that the interface supports. Valid values are 512–9216 (for IPv4) or 1280–9216 (for IPv6). You cannot specify an MTU for a VLAN interface that is larger than the MTU of the corresponding physical interface.	1500

Example

This example configures the network interface named port1, associated with the first physical network port, with the IP address and subnet mask 192.0.2.1/24. It also enables ICMP `ECHO` (ping) and HTTPS administrative access to that network interface, and enables it.

```
config system interface
  edit port1
    set ip 192.0.2.1 255.255.255.0
    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 192.0.2.1/24. It does not allow administrative access.

```
config system interface
  edit vlan_100
    set type vlan
    set ip 192.0.2.1 255.255.255.0
    set status up
    set vlanid 100
    set interface port1
  next
end
```

Related topics

- [system v-zone on page 388](#)
- [router static on page 101](#)
- [server-policy vserver on page 215](#)
- [system snmp community on page 375](#)
- [system admin on page 223](#)
- [system ha on page 319](#)
- [system network-option on page 355](#)
- [ping on page 838](#)

- [hardware nic on page 779](#)
- [network ip on page 786](#)
- [network sniffer on page 790](#)

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 details, see [Permissions on page 46](#).

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 an IP is shared by multiple clients.	low

Related topics

- [system advanced on page 233](#)

system manager-mode

The autoscaling options on FortiWeb are automatically configured after initial deployment. You can use this command to change the default configurations.

Syntax

```
config system manager
  set mode {server | client | standalone}
  set server-type {physical}
  set server-ip <server_ip_address>
  set server-port <integer>
  set config-sync-port <integer>
  set connection-interval <integer>
  set connection-lost-threshold <integer>
  set callback-url <string>
  set callback-interval <integer>
```

```

    set server-public-ip <server_public_ip_address>
  next
end

```

Variable	Description	Default
mode {server client standalone}	After the VMs in auto-scaling cluster are deployed, the function APP elects a server VM. You can use this command to change the role of the VM.	No default.
server-type {physical}	Currently we only support physical server. More types will be supported in future releases.	physical
server-ip <server_ip_address>	Enter port1's IP address of the server.	port1's IP address.
server-port	Enter a TCP port number. The clients use <code>server-ip: server-port</code> to communicate with the server, for example, register with the server to join, leave, etc.	996
config-sync-port <integer>	Enter the port that is used for configuration synchronization. The configurations of the server will be synchronized to all the clients in the cluster.	997
connection-interval <integer>	Enter the number of seconds between each server-client connection. The valid range is from 1–10.	10
connection-lost-threshold <integer>	Enter the number of seconds which must pass after the server confirmed that the client's connection is lost. The valid range is 1–10 .	3
callback-url <string>	The URL of the function APP. The VMs in the auto-scaling cluster uses this URL to communicate with the function APP. This URL is broadcasted to all the VMs in the cluster when they are deployed, so that they can communicate with the function APP. The function APP will then elect a server VM among all the available VMs.	function APP's IP address
callback-interval <integer>	Specify the interval time for FortiWeb-VM to send heartbeat request to callback URL. The valid range is 10-600 seconds.	30
server-public-ip	The public IP address of the Server. You can use this address to access the server's GUI and CLI.	server VM's IP address

system nethsm

Use this command to configure Securosys Primus HSM integration on FortiWeb. This step follows enabling HSM and specifying primus as the manufacturer in config server-policy setting.

Integrating with Securosys Primus HSM offloads cryptographic operations to a dedicated hardware security module, ensuring strong key protection and efficient processing. Once configured, FortiWeb utilizes the HSM for SSL/TLS key management, digital signatures, and secure encryption/decryption, leveraging hardware acceleration to enhance security and compliance with high-assurance standards.

Prerequisites

Before configuring Securosys Primus HSM on FortiWeb, ensure the following prerequisites are met. These credentials and files are required when setting up PKCS pin authentication on FortiWeb:

- Active account with HSM username, setup password, and PKCS#11 password.
- PKCS#11 API provider installed on the client machine.
- Primus HSM configuration file obtained and configured.
- Client registered to the HSM server and permanent secret retrieved.

Once you have configured and saved this configuration, FortiWeb will validate the configuration file and partition parameters. If all values match the expected HSM settings, the Primus HSM integration is established. At this point, cryptographic operations can be performed securely using the configured partition.

Next steps:

- Generate a Local CSR on FortiWeb — Create a CSR on FortiWeb with the Primus HSM enabled, selecting the appropriate HSM partition.
- Obtain a Signed Certificate — Download the CSR, submit it to a Certificate Authority (CA) for signing, and retrieve the signed certificate.
- Import the Signed Certificate into FortiWeb — Upload the signed certificate to FortiWeb for use in SSL/TLS encryption.
- Apply the Certificate in Server Policy — Assign the imported certificate to the relevant server policy to secure traffic with HSM-backed encryption.

For the complete configuration workflow of Securosys Primus HSM on FortiWeb, refer to the [FortiWeb Administration Guide](#).

Syntax

```
config system nethsm
  set status {enable|disable}
  set primus-cfg <cfg_content>
  set primus-cfg-version <version_number>
  config partitions
    edit <entry_index>
      set name <partition_name>
      set pkcs11-pin <pin>
      set secret <permanent_secret>
      set slot-id <slot_id>
    next
```

```
end
end
```

Variable	Description	Default
status {enable disable}	Enable the status to activate the Primus HSM integration.	disable
primus-cfg <cfg_content>	The primus configuration file content.	No default.
primus-cfg-version <version_number>	The version tracker of primus hsm configuration file.	No default.
config partitions		
<entry_index>	Enter the index number of the individual entry in the table. The valid range is from 1–9,999,999,999,999,999,999.	No default.
name <partition_name>	Define the partition name. This value must exactly match the <code>user_name</code> field in the uploaded Primus HSM configuration file to ensure authentication. For more information, see the Securosys documentation .	No default.
pkcs11-pin <pin>	Enter the PKCS#11 authentication PIN required to establish a secure session with the HSM. This PIN is used for cryptographic operations and must correspond to the PIN configured on the HSM.	No default.
secret <permanent_secret>	Provide the Permanent Secret associated with the partition. This secret serves as a cryptographic key to authenticate and encrypt communications between FortiWeb and the HSM.	No default.
slot-id <slot_id>	Specify the Slot ID corresponding to the HSM partition. This value must match the <code>id</code> defined in the uploaded configuration file. It corresponds to the PKCS#11 Slot ID assigned to the partition, serving as a unique identifier within the HSM. The correct Slot ID is required to establish secure access and ensure proper key management operations. For more information, see the Securosys documentation .	0

Related topics:

- [debug primuslog on page 769](#)
- [debug pkcs11providerlog on page 768](#)

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 details, see [Permissions on page 46](#).

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 | ultra}
  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}
  set route-priority {system | dhcp}
  set dns-priority {system | dhcp}
  set dns-cache-timeout <dns-cache-timeout_int>
  set tcp-mtu-probing {enable | disable}
  set ipfrag-high-thresh <ipfrag-high-thresh_int>
  set ipfrag-low-thresh <ipfrag-low-thresh_int>
  set ipfrag-timeout <ipfrag-timeout_int>
  set ip6frag-high-thresh <ip6frag-high-thresh_int>
  set ip6frag-low-thresh <ip6frag-low-thresh_int>
  set ip6frag-timeout <ip6frag-timeout_int>
  set tcp-usertimeout <integer>
  set ip-local-port-warning-threshold {high | normal | low | disable}
  set ip-local-port-assign-ex {enable | disable}
end
```

Variable	Description	Default
tcp-timestamp {enable disable}	Enable to: - Verify whether clients' TCP timestamps are sequential - Include TCP timestamps in packets from FortiWeb	enable

Variable	Description	Default
	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.	
tcp-tw-recycle {enable disable}	Enable to quickly recycle sockets that are ready to close (i.e. in the <code>TIME_WAIT</code> 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 system interface on page 344. 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 system interface on page 344.	disable
tcp-buffer {default high max ultra}	default: 64 KB high: 614 KB	max

Variable	Description	Default
	max: 1228 KB ultra: 3992 KB 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.	
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
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>	Enter only if no value is specified for tcp-usertimeout <tcp-usertimeout_int> on page 357. Fortinet recommends that you always specify a <code>tcp-usertimeout</code> 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
route-priority {system dhcp}	Configure the priority of route IP address obtained by the system and dhcp, whose route IP address has the priority.	No default
dns-priority {system dhcp}	Configure the priority of DNS obtained by the system and dhcp, whose DNS has the priority.	No default
dns-cache-timeout <dns-cache-timeout_int>	Configure how long the DNS proxy cache expires. The valid range is 0~60 (minutes). Only integers are supported. For example, if the value is set to 3, the DNS proxy queries the DNS records from the DNS server and renews the records in the cache every 3 minutes. Please note that if	0

Variable	Description	Default
	the DNS records in the DNS server are changed during the 3-minute interval, and a client requests for a connection to the domain at this point, the connection will fail because the DNS record stored in the DNS proxy cache is not valid anymore. To avoid this problem, you can set the <code>dns-cache-timeout</code> to a smaller value, so that the DNS proxy renews its cache more frequently. You can also set it to 0 (the default value), which means the DNS proxy doesn't cache the DNS records. It initiates query to the DNS server whenever there is a request to look up the DNS records.	
<code>tcp-mtu-probing {enable disable}</code>	Enable to negotiate with the upstream and downstream switches to get the maximum MTU value. Adjust the MTU accordingly for actual need.	disable
<code>ipfrag-high-thresh <ipfrag-high-thresh_int></code>	Enter the maximum threshold of the queued IP fragments memory that FortiWeb receives. The valid range is 0-4194304 bytes.	4194304
<code>ipfrag-low-thresh <ipfrag-low-thresh_int></code>	Enter the minimum threshold of the queued IP fragments memory that FortiWeb receives. The valid range is 0-3145728 bytes.	3145728
<code>ipfrag-timeout <ipfrag-timeout_int></code>	Type the number of seconds before the next IP fragment is received. The valid range is 0-30 seconds.	30
<code>ip6frag-high-thresh <ip6frag-high-thresh_int></code>	Enter the maximum threshold of the queued IP6 IP fragments memory that FortiWeb receives. The valid range is 0-4194304 bytes.	4194304
<code>ip6frag-low-thresh <ip6frag-low-thresh_int></code>	Enter the minimum threshold of the queued IP6 fragments memory that FortiWeb receives. The valid range is 0-3145728 bytes.	3145728
<code>ip6frag-timeout <ip6frag-timeout_int></code>	Type the number of seconds before the next IP6 fragment is received. The valid range is 0-30 seconds.	30
<code>tcp-usertimeout <integer></code>	When the health check is disabled and the back-end server is not responsive, FortiWeb will wait for the specified time until it sends the 503 error code. It's recommended to set a value smaller than 20 (seconds). This is to avoid too many times of retry being accumulated during the waiting time, which may cause the connection to be closed before FortiWeb has the chance to send the error code.	120

Variable	Description	Default
	This option is at the appliance level. It affects all the policies on the appliance. You can also set the <code>tcp-conn-timeout</code> under <code>config server-policy policy</code> which only affects a specific policy. If the timeout is configured both at the policy and the appliance level, FortiWeb will take the value whichever is smaller. Sometimes when there is a third device, such as a gateway, deployed between FortiWeb and the back-end server, FortiWeb will directly get the status code from the third device instead of waiting along the timeout period. The valid range for this option is 0-600 (seconds). 0 means FortiWeb will send the 503 error code as soon as it detects the back-end server is not responsive.	
<code>ip-local-port-warning-threshold {high normal low disable}</code>	FortiWeb allocates a different port number (ranging from 1024 to 65535) for each connection with the back-end server to distinguish these connections. When the port numbers are nearly exhausted, CPU usage will be high. It is suggested to create a new network interface for the back-end server connections when facing port exhaustion. It's important to stay informed about the port exhaustion situation so that you can take timely action to avoid CPU high usage. An efficient way to achieve this is by configuring FortiWeb to generate Port Exhaustion logs based on port usage levels: • High: The ports are almost fully utilized. • Normal: There are a few available ports, and the system is struggling to allocate ports to all current connections. It is highly likely that the ports will soon be exhausted. • Low: There are some available ports, and the system is functioning adequately. However, you should be prepared for the possibility that ports might be exhausted during a traffic spike. Another option is <code>disable</code>, which will disable generating the port exhaustion logs.	normal
<code>ip-local-port-assign-ex {enable disable}</code>	Enable this option to mitigate the port exhaustion situation. However, please note that this is a temporary solution and could impact system performance. Adding a new network interface for back-end server connections should be considered a high-priority solution when port exhaustion occurs.	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 192.0.2.71/24
        set allowaccess HTTPS ping ssh snmp HTTP telnet
        config secondaryip
            edit 1
                set ip 192.0.2.72/24
            next
            edit 2
                set ip 192.0.2.73/24
            next
        end
    next
end
```

Related topics

- [system interface on page 344](#)
- [ping on page 838](#)
- [network ip on page 786](#)
- [network sniffer on page 790](#)

system ntp

Use this command to manage the connection to an NTP server.

To use this command, your administrator account's access control profile must have `rw` permission to the `netgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system ntp
    set ntpsync {enable|disable}
    set syncinterval <integer>
    config ntp-server
        edit <no.>
            set server <server_name>
            set authentication {enable|disable}
            set key-type {aes128|aes256|sha1|sha256}
            set key <key>
```



```

        set key-id <key_id>
        set ip-type {v4|v6|both}
    next
end
end

```

Variable	Description	Default
ntpsync	Enable/disable use of NTP. When ntpsync is enabled , config ntp-server becomes configurable.	Enable
syncinterval	Specify how often the system synchronizes its time with the NTP server. The default is 60 minutes. The valid range is 1-1440.	60
config ntp-server		
server	Specify the IP address or domain name of an NTP server or pool, such as <code>pool.ntp.org</code> . To find an NTP server, go to http://www.ntp.org .	No default
authentication	Enable to apply authentication keys to secure the NTP server. This is disabled by default.	disable
key-type	The key-type option is available if authentication is enabled . Select the key type from the following: • aes128 • aes256 • sha1 • sha256 The default option is sha1.	sha1
key	The key option is available if authentication is enabled . Specify the Key in hexadecimal format. The maximum length is 127 digits or characters.	No default
key-id	The key-id option is available if authentication is enabled . Specify the Key ID. The valid range is 0-65536	No default
ip-type	Select the IP type from the following: • v4 • v6 • both The default option is v4.	v4

Example

```

config system time ntp
    set ntpsync enable
    set syncinterval 1
config ntp-server

```

```
edit 1
  set server 10.159.0.114
  set authentication enable
  set key-type aes256
  set key ENC
  set key-id 7
  set ip-type v4
next
end
end
```

system object-tagging

Use this command to create tags that can be attached to server policy. It helps in labeling server policy for future usage such as sorting, filtering and acknowledging policies.

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 object-tagging
  edit <string>
    set color <color-id>
  next
end
```

Variable	Description	Default
<string>	The name of the tag.	no default
<color-id>	Assign a color to this tag. The valid range is 0-32.	1

system password-policy

Use this command to configure a password policy for administrator accounts that set rules for password characteristics.

Syntax

```
config system password-policy
  set status {enable | disable}
  set min-length-option {enable | disable}
  set mini-length <mini-length_int>
  set single-admin-mode {enable | disable}
  set character-requirements {enable | disable}
  set min-upper-case-letter <min-upper-case-letter_int>
  set min-lower-case-letter <min-lower-case-letter_int>
```

```

set mini-number <mini_number_int>
set min-non-alphanumeric <min-non-alphanumeric_int>
set forbid-password-reuse {enable | disable}
set history-password-number <history-password-number_int>
set expire-status {enable | disable}
set expire-day <expire-day_int>

```

```
end
```

Variable	Description	Default
status {enable disable}	Enable to enforce password rules for administrator accounts. When you configure rules for the password policy, administrator accounts that don't adhere to the password policy will be prompted to update their password upon logging in. For some cloud platforms such as AWS, Azure, and GCP, etc., it is enabled by default.	disable
min-length-option {enable disable}	Enable/disable to set the minimum length for the password.	disable
mini-length <mini-length_int>	Enter the minimum password length. The valid range is 8–128.	8
single-admin-mode {enable disable}	Enable/disable to activate single admin user login.	disable
character-requirements {enable disable}	Enable/disable to set characters, upper/lower case, numbers (0–9), and special.	0
min-upper-case-letter <min-upper-case-letter_int>	Enter the number of upper case characters. The valid range is 0–128.	0
min-lower-case-letter <min-lower-case-letter_int>	Enter the number of lower case characters. The valid range is 0–128.	0
mini-number <mini_number_int>	Enter the number of number characters. The valid range is 0–128. Only numbers 0–9 are supported.	0
min-non-alphanumeric <min-non-alphanumeric_int>	Enter the number of special characters. The valid range is 0–128.	0
forbid-password-reuse {enable disable}	Enable forbidding password re-use.	disable
history-password-number <history-password-number_int>	Enter the number of history passwords that can not be re-used. The valid range is 1–10.	3

Variable	Description	Default
expire-status {enable disable}	Enable password expiration.	disable
expire-day <expire-day_int>	Enter the valid period for the password. The valid range 1–999 days	90

Example

This example enables configuration of the password policy.

```
config system password-policy
    set status enable
    set system password-policy
    set min-length 8
    set single-admin-mode enable
    set character-requirements enable
    set min-upper-case-letter 2
    set min-lower-case-letter 2
    set min-number 2
    set min-non-alphanumeric 3
    set forbid-password-reuse enable
    set history-password-number 2
    set expire-status enable
    set expire-day 100

end
```

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-1000E
- FortiWeb-1000F
- FortiWeb-2000E
- FortiWeb-3000C
- FortiWeb-3000D
- FortiWeb-3000E
- FortiWeb-4000C
- FortiWeb-4000D
- FortiWeb-4000E

Note: All supported platforms use hardware RAID, except for the FortiWeb-1000E and 1000F models, which implement software RAID.

RAID cannot be activated on older appliances that were upgraded to FortiWeb 4.0 MR1.



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 details, see [Permissions on page 46](#).

Syntax

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

Variable	Description	Default
level {raid1}	Enter 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

- [create-raid level on page 826](#)
- [create-raid rebuild on page 827](#)
- [hardware raid list on page 782](#)

system recaptcha-api

Use this command to specify the URL that FortiWeb will use to send API calls to Google reCAPTCHA service, and the timeout of the API request.

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 recaptcha-api
  set url <string>
  set timeout <int>
  set recaptcha-v3-score-threshold <string>
end
```

Variable	Description	Default
url <string>	Specify the URL of the Google reCAPTCHA service. FortiWeb sends API calls to this URL to verify client's response to the reCAPTCHA challenge. Currently the URL is https://www.google.com/recaptcha/api/siteverify . Please note this URL is subject to change by Google. Please refer to https://developers.google.com/recaptcha/docs/verify#api_request for the latest URL and make sure FortiWeb is configured with the latest URL.	https://www.google.com/recaptcha/api/siteverify
timeout <int>	If there isn't any result returned from Google reCAPTCHA service by the timeout period, the bot confirmation will be treated as failed.	10 (seconds)
recaptcha-v3-score-threshold <string>	reCAPTCHA v3 returns a score for each request. The score is based on interactions with your application. If the score surpasses the <code>recaptcha-v3-score-threshold</code> , FortiWeb will take corresponding actions. The valid range is 0-1.	0.5

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 details, see [Permissions on page 46](#).

Syntax

```
config system replacemsg-image
  edit "<image_name>"
    set image-type {gif | jpg | png | tiff}
    set image-base64 <image_code>
  end
```

Variable	Description	Default
"<image_name>"	Enter 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>	Enter 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 <code>image-type</code>	No default

system saml

You can configure Fabric Connector to use Single Sign-On (SSO) to log in to FortiWeb with FortiGate's administrator accounts.

Use this command to configure the single sign on options on FortiWeb. Before using this command, you need to first use `config system csf` to configure the Fabric Connector. For a complete guide, see [Fabric Connector: Single Sign On with FortiGate](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system saml
  set status {enable | disable}
  set default-login-page
  set default-profile
  set idp-entity-id
  set idp-single-sign-on-url
  set idp-single-logout-url
  set server-address
end
```

Variable	Description	Default
status {enable disable}	Enable or disable single sign on mode. When this is enabled, the Single Sign-On option will be available on the login page of FortiWeb.	disable
default-login-page	• <code>normal</code>: When accessing to FortiWeb GUI, the login page has both Single Sign-On and Non Single Sign-On login options. • <code>sso</code>: When accessing to FortiWeb GUI, it would redirect to the SAML Single Sign-On login page. Non Single Sign-On login is not available. User can only log in with	normal

Variable	Description	Default
FortiGate administrator accounts		
default-profile	Logging in to FortiWeb via FortiGate Fabric Single Sign-On does not share the same admin profile between FortiWeb and FortiGate. It requires specifying profiles to those FortiGate administrator accounts on FortiWeb. Choose the profiles you have created in <code>config system accprofile</code>. The selected profiles will be assigned to the FortiGate administrator accounts that are used to log in to FortiWeb via the SAML Single Sign-On. The following two default profiles are available as well as the customized profiles if any: <code>admin_no_access</code>: users will be assigned with none access privilege. <code>prof_admin</code>: this is FortiWeb's default profile for root admin.	No default
idp-entity-id	It's automatically synchronized from FortiGate if you have configured <code>set configuration-sync enable</code> in <code>config system csf</code> .	No default
idp-single-sign-on-url	It's automatically synchronized from FortiGate if you have configured <code>set configuration-sync enable</code> in <code>config system csf</code> .	No default
idp-single-logout-url	It's automatically synchronized from FortiGate if you have configured <code>set configuration-sync enable</code> in <code>config system csf</code> .	No default
server-address	It's automatically synchronized from FortiGate if you have configured <code>set configuration-sync enable</code> in <code>config system csf</code> .	No default

Related topics

- [system csf](#)

system sdn-connector

Use this command to create external connectors for Amazon Web Services (AWS), Microsoft Azure, and OCI.

The AWS and Azure connectors authorize FortiWeb to automatically retrieve the IP addresses of the back-end servers deployed on AWS or Azure.

OCI Connector is available only when FortiWeb-VM is deployed on OCI. It is used to obtain FortiWeb HA member information in Active-Passive mode.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system sdn-connector
edit <name>
    set status {enable | disable}
    set type {azure | aws | oci}
    set update-interval <int>
```



```

set access-key <string> on page 369
set secret-key <string> on page 369
set region <string>
set tenant-id <string>
set subscription-id <string>
set client-id <string>
set client-secret <string>
set resource-group <string>
set azure-region <string>
setserver-region-type {commercial | government}
set server-region <region-id>
set user-ocid <string>
set tenant-ocid <string>
set compartment-ocid <string>
set private-key <userdef>
end
end

```

Variable	Description	Default
<name>	Enter a name for the external connector object.	No default
status {enable disable}	Enable or disable the external connector object.	enable
type {azure aws oci}	Select the type of the connector.	No default
update- interval <int>	Specify the update interval for the connector to get AWS objects and dynamically populates the information in the server pool configuration.	60
AWS connector settings		
access-key <string>	Specify the access key ID. An access key on AWS grants programmatic access to your resources. If you have security considerations, it's recommended to create an IAM role specially for FortiWeb and grant read-only access. See this article for how to get access key ID and secret access key on AWS: https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html .	No default
secret-key <string>	Specify the secret access key.	No default
region <string>	Specify the region where your instances are deployed, for example, us-west-2.	No default

Variable	Description	Default
Azure connector settings You must create an Azure AD application to generate the Azure client ID and corresponding Azure client secret. This application must be a service principal. Otherwise, the Fabric connector cannot read the inventory. You can find the complete instructions at Use portal to create an Azure Active Directory application and service principal that can access resources . Keep the following in mind when you get to the part about making a new application registration: • The Application type has two options. Choose Web app/API. • The Sign-on URL has the asterisk commonly associated with a required field, but this is not applicable in this case. Put in any valid URL in the field to complete the form and enable the Create button.		
tenant-id <string>	See instructions above for how to find the Tenant ID.	No default
subscription-id <string>	The ID of the subscription where your application server is deployed.	No default
client-id <string>	See instructions above for how to find the Client ID.	No default
client-secret <string>	See instructions above for how to find the Client Secret.	No default
resource-group <string>	The name of the resource group where your application server is deployed. Make sure that the service principal (app registration) is granted for the network contributor and VM contributor roles for the target resource group.	No default
azure-region <string>	The region where your application server is deployed.	No default
OCI Connector settings you need to generate the RSA key that will be used for authentication when FortiWeb-VM connects to the load balancer. 1. Log in to a Linux system which has installed OpenSSL. 2. Open a SHELL terminal, enter the following commands: <pre>openssl genrsa -out ./oci_api.key 2048 openssl rsa -pubout -in ./oci_api.key -out ./oci_api_pub.key</pre> The file <code>oci_api.key</code> is the RSA private key file and the file <code>oci_api_pub.key</code> is its paired public key file. 3. Log in OCI. Go to Governance and Administration > Identity > User.		

Variable	Description	Default
4. Select the proper user you want to use. 5. Click Add Public Key, copy the text in <code>oci_api_pub.key</code> file, and then paste it into the PUBLIC KEY field on the Add Public Key window. 6. Click Add. For a complete guide on the OCI connector settings, see Configuring OCI Connector.		
server-region-type {commercial government}	If your OCI server region is either “US Federal Cloud with DISA Impact Level 5 Authorization Regions” or “US Government Cloud with FedRAMP Authorization Regions”, please select Government. Otherwise please select Commercial.	commercial
server-region <region-id>	Enter the Region Identifier of your load balancer. - For <code>Commercial</code> regions, please find the Region Identifier on this page: https://docs.cloud.oracle.com/en-us/iaas/Content/General/Concepts/regions.htm - For <code>Government</code> regions, please find the Region Identifier on the following pages: https://docs.cloud.oracle.com/en-us/iaas/Content/General/Concepts/govfeddod.htm https://docs.cloud.oracle.com/en-us/iaas/Content/General/Concepts/govfedramp.htm	No default
user-ocid <string>	To get the User OCID: - Log in to OCI. - Go to Governance and Administration > Identity > User. - Click the user you want to use. - Copy the OCID of this user.	No default
tenant-ocid <string>	To get the tenant OCID: - Log in to OCI. - Go to Governance and Administration > Administration > Tenancy Details. - Click the Tenancy you want to use. - Copy the OCID of this Tenancy.	No default
compartment-ocid <string>	To get the compartment OCID: - Log in to OCI. - Go to Governance and Administration > Identity > Compartments. - Click the compartment that your load balancer is located in. - Copy the OCID of this Tenancy. Note: If you don't have a compartment, you can leave this option empty.	No default
private-key <userdef>	Upload the private key file you have generated when system sdn-connector on page 368.	No default

To apply the external connector, you need to select it in the server pool configurations so that FortiWeb can use the connector to automatically retrieve the IP addresses of the back-end servers deployed on AWS or Azure.

Here is an example:

```
config server-policy server-pool
  edit pool
    config pserver-list
      edit 1
        set server-type sdn-connector
        set sdn-addr-type public
        set sdn aws
        set filter InstanceId=i-04d15747127e4f8fe
      next
    end
  next
end
```

Related topics

- [server-policy server-pool](#)

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 **Alert** cannot be guaranteed to be successful in Offline Protection mode. The FortiWeb appliance will attempt to block traffic that violates the policy by mimicking the client or server and requesting to reset the connection. However, the client or server may receive the reset request after it receives the other traffic due to possible differences in routing 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*:

<https://docs.fortinet.com/document/fortiweb>

You can use SNMP traps to notify you if the operation mode changes. For details, see [system snmp community on page 375](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

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 enable-debug-log {enable | disable}
set enable-machine-learning-debug {enable | disable}
set enable-file-upload {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 <i>FortiWeb Administration Guide</i>: https://docs.fortinet.com/document/fortiweb 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 <code>offline-protection</code>, 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> on page 154.	reverse-proxy
gateway "<router_ipv4>"	Type the IPv4 address of the default gateway. This setting is visible only if <code>opmode {offline-protection reverse-proxy transparent transparent-inspection wccp}</code> on page 374 is either True Transparent Proxy, Transparent Inspection, or WCCP. FortiWeb will use the <code>gateway</code> setting to create a corresponding static route under <code>router static</code> with the first available index number. Packets will egress through <code>port1</code> or <code>mgmt1</code>, 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. 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.	enable
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.	enable
enable-debug-log {enable disable}	Enable so that FortiWeb will record crash, daemon, kernel, netstat, and core dump logs.	enable
enable-machine-learning-debug {enable disable}	Enable so that FortiWeb will record machine learning debug.	enable

Variable	Description	Default
enable-file-upload {enable disable}	Enable to upload the debugging file.	disable

Related topics

- [server-policy policy on page 150](#)
- [server-policy vserver on page 215](#)

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 [system snmp user on page 381](#).

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 and add it as a member of at least one community. For details, see [system snmp sysinfo on page 379](#). You must also enable SNMP access on the network interface through which the SNMP manager will connect. For details, see [system interface on page 344](#).

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*:

<https://docs.fortinet.com/document/fortiweb>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

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-
  cluster-status-change | sys-ha-member-join | sys-ha-member-leave | sys-mode-
  change | waf-amethod-attack | waf-hidden-fields | waf-pvalid-attack | waf-
  signature-detection | power-supply-failure}
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>	Enter the index number of a community to which the FortiWeb appliance belongs. The valid range is 1–9,999,999,999,999,999.	No default.
status {enable disable}	Enable to activate the community. This setting takes effect only if the SNMP agent is enabled. For details, see system snmp sysinfo on page 379 .	disable
name "<community_str>"	Enter the name of the SNMP community to which the FortiWeb appliance and at least one SNMP manager belongs. The maximum length is 63 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-cluster-status-change sys-ha-member-join sys-ha-member-leave sys-mode-change waf-amethod-attack waf-hidden-fields waf-pvalid-attack waf-signature-detection power-supply-failure}	Enter 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. • <code>cpu-high</code>—CPU usage has exceeded 80%. • <code>intf-ip</code>—A network interface's IP address has changed. For details, see system interface on page 344. • <code>log-full</code>—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. For details, see log disk on page 66. • <code>mem-low</code>—Memory (RAM) usage has exceeded 80%. • <code>netlink-down-status</code>—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. • <code>netlink-up-status</code>—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. • <code>policy-start</code>—A policy was enabled. For details, see server-policy policy on page 150. • <code>policy-stop</code>—A policy was disabled. For details, see server-policy policy on page 150. • <code>pserver-failed</code>—A server health check has determined that a physical server that is a member of a server farm is now unavailable. For details, see server-policy policy on page 150 on page 1. • <code>sys-ha-cluster-status-change</code>—HA cluster status was changed. • <code>sys-ha-member-join</code>—HA member has joined. • <code>sys-ha-member-leave</code>—HA member has left. • <code>sys-mode-change</code>—The operation mode was changed. See system settings on page 372. • <code>waf-amethod-attack</code>—FortiWeb enforced an allowed methods restriction. For details, see waf web-protection-profile inline-protection on page 696, waf web-protection-profile offline-protection on page 706, and waf allow-method-exceptions on page 423. • <code>waf-hidden-fields</code>—FortiWeb detected a hidden fields attack. • <code>waf-pvalid-attack</code>—FortiWeb enforced an input/parameter validation rule. For details, see waf	No default.

Variable	Description	Default
	parameter-validation-rule on page 610. <code>waf-signature-detection</code>—FortiWeb enforced a signature rule. For details, see waf signature on page 612. <code>waf-url-access-attack</code>—FortiWeb enforced a URL access rule. See waf url-access url-access-rule on page 669. <code>power-supply-failure</code>—FortiWeb detects the power supply fails. It is only available for 2000E, 3000E, 3010E, and 4000E.	
<code>query-v1-port <port_int></code>	Enter 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 1–65,535.	161
<code>query-v1-status {enable disable}</code>	Enable to respond to queries using the SNMP v1 version of the SNMP protocol.	enable
<code>query-v2c-port <port_int></code>	Enter 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 1–65,535.	161
<code>query-v2c-status {enable disable}</code>	Enable to respond to queries using the SNMP v2c version of the SNMP protocol.	enable
<code>trap-v1-lport <port_int></code>	Enter the port number that will be the source (also called local) port number for SNMP v1 trap packets. The valid range is 1–65,535.	162
<code>trap-v1-rport <port_int></code>	Enter the port number that will be the destination (also called remote) port number for SNMP v1 trap packets. The valid range is 1–65,535.	162
<code>trap-v1-status {enable disable}</code>	Enable to send traps using the SNMP v1 version of the SNMP protocol.	enable
<code>trap-v2c-lport <port_int></code>	Enter the port number that will be the source (also called local) port number for SNMP v2c trap packets. The valid range is 1–65,535.	162
<code>trap-v2c-rport <port_int></code>	Enter the port number that will be the destination (also called remote) port number for SNMP v2c trap packets. The valid range is 1–65,535.	162
<code>trap-v2c-status {enable disable}</code>	Enable to send traps using the SNMP v2c version of the SNMP protocol.	enable
<code><snmp-manager_index></code>	Enter the index number of an SNMP manager for the community. The valid range is 1–9,999,999,999,999,999,999.	No default.

Variable	Description	Default
ip {"<manager_ipv4>" "<manager_ipv6>"}	Enter 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 [system snmp sysinfo on page 379](#).

Related topics

- [system snmp sysinfo on page 379](#)
- [system interface on page 344](#)
- [server-policy policy on page 150](#)

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. For details, see [system snmp community on page 375](#). You must also enable SNMP access on the network interface through which the SNMP manager will connect. For details, see [system interface on page 344](#).

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*:

<https://docs.fortinet.com/document/fortiweb>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system snmp sysinfo
  set contact-info "<contact_str>"
  set description "<description_str>"
```

```

set location "<location_str>"
set status {enable | disable}
set engine-id "<engine-id_str>"
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 63 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 63 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 63 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 system interface on page 344 .	disable
engine-id "<engine-id_str>"	Enter the SNMP engineID string. The maximum is 24 characters.	No default

Example1234

This example enables the SNMP agent, configures it to belong to a community named public whose SNMP manager is 192.0.2.20. 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-1000E"
    set location "Rack_2"
    set status enable
    set engine-id 246
end

config system snmp community

```

```
edit 1
    set status enable
    set name public
    set events cpu-high
    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 192.0.2.20
        next
    end
next
end
config system interface
    edit port3
        set allowaccess ping HTTPS ssh snmp
    next
end
```

Related topics

- [system snmp community on page 375](#)
- [system interface on page 344](#)
- [router static on page 101](#)

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 [system snmp community on page 375](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system snmp user
    edit name "<user_str>"
        set status {enable | disable}
        set security-level { noauthnopriv | authnopriv | authpriv >
        set auth-proto {sha1 | sha224 | sha256 | sha384 | sha512 | md5}
        set auth-pwd "<auth-password_str>"
```

```

set priv-proto {aes | des | aes256}
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 events {cpu-high | intf-ip | log-full | mem-low | netlink-down-status |
  netlink-up-status | policy-start | policy-stop | pserver-failed | sys-ha-
  cluster-status-change | sys-ha-member-join | sys-ha-member-leave | sys-mode-
  change | waf-amethod-attack | waf-hidden-fields | waf-pvalid-attack | waf-
  signature-detection | waf-url-access-attack | power-supply-failure}
set "<snmp-manager_index>"
config hosts
  edit "<snmp-manager_index>"
    set {"<manager_ipv4> | <manager_ipv6>"}
  next
end
next
end

```

Variable	Description	Default
name "<user_str>"	Enter the name of the SNMP user to which the FortiWeb appliance and at least one SNMP manager belongs. The maximum length is 63 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 system snmp sysinfo on page 379.	disable
security-level { noauthnopriv authnopriv authpriv >	Enter 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 <code>auth-proto</code> and <code>auth-pwd</code>. - authpriv—Adds both authentication and encryption. Also specify <code>auth-proto</code>, <code>auth-pwd</code>, <code>priv-proto</code>, and <code>priv-pwd</code>. Ensure that the SNMP manager and FortiWeb use the same protocols and passwords.	No default.
auth-proto {sha1 sha224 sha256 sha384 sha512 md5}	If the <code>security-level</code> option includes authentication, specify the authentication protocol.	sha1

Variable	Description	Default
auth-pwd "<auth-password_str>"	If the <code>security-level</code> option includes authentication, specify the authentication password.	No default.
priv-proto {aes des aes256}	If the <code>security-level</code> option is <code>authprivuser_name</code> , specify the encryption protocol.	aes
priv-pwd "<priv-password_str>"	If the <code>security-level</code> option is <code>authprivuser_name</code> , 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>	Enter the port number on which the FortiWeb appliance listens for SNMP v3 queries from the SNMP managers of the community. The valid range is 1–65,535.	161
trap-status {enable disable}	Enable to send traps using the SNMP v3 version of the SNMP protocol.	enable
trapport-local <port_int>	Enter the port number that is the source (also called local) port number for SNMP v3 trap packets. The valid range is 1–65,535.	162
trapport-remote <port_int>	Enter the port number that is the destination (also called remote) port number for SNMP v3 trap packets. The valid range is 1–65,535.	162
events {cpu-high intf-ip log-full mem-low netlink-down-status netlink-up-status policy-start policy-stop pserver-failed sys-ha-cluster-status-change sys-ha-member-join sys-ha-member-leave sys-mode-change waf-amethod-attack waf-hidden-fields waf-pvalid-attack waf-signature-detection waf-url-access-attack power-supply-failure}	Enter 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 <code>trap-status</code>. <code>cpu-high</code>—CPU usage has exceeded 80%. <code>intf-ip</code>—A network interface's IP address has changed. See system interface on page 344. <code>log-full</code>—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. For details, see log disk on page 66. <code>mem-low</code>—Memory (RAM) usage has exceeded 80%. <code>netlink-down-status</code>—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. <code>netlink-up-status</code>—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. <code>policy-start</code>—A policy was enabled. For details, see server-policy policy on page 150.	No default.

Variable	Description	Default
	• <code>policy-stop</code>—A policy was disabled. For details, see server-policy policy on page 150. • <code>pserver-failed</code>—A server health check has determined that a physical server that is a member of a server farm is now unavailable. For details, see server-policy policy on page 150. • <code>sys-ha-cluster-status-change</code>—HA cluster status was changed. • <code>sys-ha-member-join</code>—HA member has joined. • <code>sys-ha-member-leave</code>—HA member has left. • <code>sys-mode-change</code>—The operation mode was changed. For details, see system settings on page 372. • <code>power-supply-failure</code>—FortiWeb detects the power supply fails. It is only available for 2000E, 3000E, 3010E, and 4000E.	
	• <code>waf-amethod-attack</code>—FortiWeb enforced an allowed methods restriction. For details, see waf web-protection-profile inline-protection on page 696, waf web-protection-profile offline-protection on page 706, and waf allow-method-exceptions on page 423. • <code>waf-hidden-fields</code>—FortiWeb detected a hidden fields attack. • <code>waf-pvalid-attack</code>—FortiWeb enforced an input/parameter validation rule. For details, see waf parameter-validation-rule on page 610. • <code>waf-signature-detection</code>—FortiWeb enforced a signature rule. For details, see waf signature on page 612. • <code>waf-url-access-attack</code>—FortiWeb enforced a URL access rule. For details, see waf url-access url-access-rule on page 669. • <code>power-supply-failure</code>—FortiWeb detects the power supply failure. It is only available for 2000E, 3000E, 3010E, and 4000E.	
<code>"<snmp-manager_index>"</code>	Enter the index number of an SNMP manager for the community. The valid range is 1–9,999,999,999,999,999.	No default.
<code>{"<manager_ipv4> <manager_ipv6>"}</code>	Enter 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.	No default.

Variable	Description	Default
	To allow any IP address using this SNMP community name to query the FortiWeb appliance, enter 0.0.0.0 or : : . Note: Entering 0.0.0.0 or : : 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.	

Example

For an example, see [system snmp sysinfo on page 379](#).

Related topics

- [system snmp sysinfo on page 379](#)
- [system interface on page 344](#)
- [server-policy policy on page 150](#)

system sso-admin

With Single Sign-On Mode enabled, users will be redirected to FortiGate's Single Sign-On Provider page when they click **Single Sign-On** on FortiWeb's login page. They will be required to log in with FortiGate's administrator account.

Use this command to create a SSO admin account and grant permissions for this account.

For how to configure SSO with FortiGate, see [Fabric Connector: Single Sign On with FortiGate](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system sso-admin
  edit <name>
    set access-profile <profile name>
    set domains <adom name>
  end
end
```

Variable	Description	Default
<name>	Enter a name of the administrator account, such as <code>admin1</code> or <code>admin@example.com</code>, that can be referenced in other parts of the configuration. Do not use spaces or special characters except the 'at' symbol (<code>@</code>). The maximum length is 63 characters. To display the list of existing accounts, enter: <pre>edit ?</pre> Note: This is the user name that the administrator must provide when logging in to the CLI or web UI.	No default
access-profile <profile_name>	Enter the name of an access profile that gives the permissions for this administrator account. See also system accprofile on page 220. The maximum length is 63 characters. You can select prof_admin, a special access profile used by the <code>admin</code> administrator account. However, selecting this access profile will not confer all of the same permissions of the <code>admin</code> administrator. For example, the new administrator would not be able to reset lost administrator passwords. To display the list of existing profiles, enter: <pre>edit ?</pre>	No default
domains <adom_name>	Enter the name of an administrative domain (ADOM) to assign and restrict this administrative account to it.	root

Related topics

- [system admin](#)

system tcpdump

Use this command to configure capturing packets.

To use this command, your administrator account's access control profile must have `rw` permission to the `netgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config system tcpdump
edit file id
set "<filter_str>"
set {any | "<interface_str>"}
set "<max-packet-count_int>"
```

end

Variable	Description	Default
file id	Enter the packet capture file ID.	No default
"<max-packet-count_int>"	Specify the maximum packets you want to capture for the policy. Capture will stop automatically if the total captured packets hit the count.	4000
"<filter_str>"	Specify which protocols and port numbers that you do or do not want to capture, such as 'tcp and port 80 and host IP1 and (IP2 or IP3) ', or leave this field blank for no filters. Note that please use the same filter expression as <code>tcpdump</code> for this filter, you can refer to the Linux main page of TCPDUMP (http://www.tcpdump.org/manpages/tcpdump.1.html).	No default.
{any "<interface_str>"}	Select the network interface on which you want to capture packets, such as <code>port1</code> , or <code>any</code> for all interfaces.	any
"<max-packet-count_int>"	Specify the maximum packets you want to capture for the policy. Capture will stop automatically if the total captured packets hit the count.	4000

Related topics

- [debug on page 747](#)

system vip

The virtual IP addresses are the IP addresses that paired with the domain name of your application. When users visit your application, the destination of their requests are these IP addresses.

You can later attach one or more virtual IP addresses to a virtual server, and then reference the virtual server in a server policy. The web protection profile in the server policy will be applied to all the virtual IPs attached to this virtual server.

Only the global administrators can create, edit, and delete VIPs.

Syntax

```
config system vip
  edit <vip_name> on page 388
    set vip <ip&netmask> on page 388
    set vip6 <ip&netmask> on page 388
    set interface <interface_name> on page 388
    set index <the_index_number> on page 388
    set domains <a_dom_name>
  next
```

end

Variable	Description	Default
<vip_name>	Enter a unique name that can be referenced by other parts of the configuration. The maximum length is 63 characters.	No default
vip <ip&netmask>	Enter the IPv4 address and subnet of the virtual IP. If the FortiWeb appliance is operating in Offline Protection mode or either of the transparent modes, because FortiWeb ignores this IP address when it determines whether or not to apply a server policy to the connection, you can specify any IP address except the address of the web server. The virtual IP address cannot be the same with the IP address of any one of the interfaces.	0.0.0.0/0
vip6 <ip&netmask>	Enter the IPv6 address and subnet of the virtual IP. If the FortiWeb appliance is operating in Offline Protection mode or either of the transparent modes, because FortiWeb ignores this IP address when it determines whether or not to apply a server policy to the connection, you can specify any IP address except the address of the web server. The virtual IP address cannot be the same with the IP address of any one of the interfaces.	::/0
interface <interface_name>	Enter the name of the network interface or bridge the virtual IP is bound to and where traffic destined for the virtual IP arrives.	port1
index <the_index_number>	Enter the index number for this vip.	No default
domains <adom_name>	Enter the ADOM you want to create this virtual IP in.	No default

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.



For FortiWeb-VM, you must create vSwitches **before** you can configure a bridge.
For details, see the FortiWeb-VM Install Guide:
<https://docs.fortinet.com/fortiweb/hardware>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `netgrp` area. For details, see [Permissions on page 46](#).

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>" ...}
    set multicast-snooping {enable | disable}
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: <code>edit ?</code>	No 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 63 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 512–9216 (for IPv4) or 1280–9216 (for IPv6).	1500
multicast-snooping {enable disable}	Enable/disable multicast snooping.	No default
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	No default.

Variable	Description	Default
	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.	

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

- [system interface on page 344](#)
- [system settings on page 372](#)

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. For details, see [system settings on page 372](#).

For information on connecting and configuring your network devices for WCCP mode, see the *FortiWeb Administration Guide*:

<https://docs.fortinet.com/document/fortiweb>

For detailed information on configuring FortiGate and other Fortinet devices to act as a WCCP service group, see the FortiGate WCCP topic in the *Fortinet Variables Handbook*:

<https://docs.fortinet.com/fortigate/admin-guides>

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 51–256. Do not use 1–50, which are reserved by the WCCP standard.	51
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. For details, see system settings on page 372.	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 224.0.0.0–239.255.255.255.	No default.

Variable	Description	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 {enable disable} on page 392 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
ports <ports_int>	Enter the port numbers of the sessions that this client inspects. The valid range is 0–65535. 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 <code>assignment-weight</code> 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 <code>ports</code> and <code>protocol</code>, the WCCP server transmits all the traffic to the service group with the highest <code>priority</code> value.	0
protocol <priority_int>	Enter the protocol of the network traffic the WCCP service group transmits. For TCP sessions, enter 6.	6

Variable	Description	Default
	Valid values are 0–256.	
assignment-weight <assignment-weight_int>	Enter a value that the WCCP server uses in combination with <code>primary-hash</code> to direct traffic, when the WCCP service group has more than one WCCP client. The valid range is 0–256.	0
assignment-bucket-format {cisco-implementation wccp-v2}	Enter the hash table bucket format for the WCCP cache engine. <code>cisco-implementation</code>—Source IP address <code>wccp-v2</code>—Web Cache Communication Protocol version 2	cisco- 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 (192.0.2.100) and the WCCP server (192.0.2.1).

```
config system wccp
  edit service-id 52
    set cache-id "192.0.2.100"
    set router-list "192.0.2.1"
    set ports 80 443
    set primary-hash src-ip dst-ip
```

Related topics

- [system settings on page 372](#)
- [system interface on page 344](#)

system certificate xml-server-certificate

Use this command to show names of the uploaded XML server certificates that are stored locally on the FortiWeb appliance.

The XML server certificate is used for request decryption or response signature.

Syntax

```
config system certificate xml-server-certificate
  edit system certificate xml-server-certificate
```

```

    set certificate <certificate_str> on page 394
    set private-key <private-key_str>
    set passwd <passwd_str>
  next
end

```

Variable	Description	Default
"<xml-server-certificate_name>"	Enter the name of an XML server certificate.	No default.
certificate <certificate_str>	Set the certificate. Only certificates in PEM format may be set.	No default.
private-key <private-key_str>	Set the key file to upload.	No default.
passwd <passwd_str>	Type the password that is used to encrypt the file, enabling the FortiWeb appliance to decrypt and install the certificate.	No default.

Related topics

- [waf ws security on page 718](#)

user admin-usergrp

Use this command to configure LDAP/RADIUS/PKI/TACACS+ 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 LDAP, RADIUS, or TACACS+ accounts (see [user ldap-user on page 397](#) or "[server-policy custom-application application-policy](#)" on page 1), a PKI user (see [user pki-user on page 406](#)), or a TACACS+ user (see [user tacacs+ user on page 412](#)).

For information about certificate-based Web UI login, see the *FortiWeb Administration Guide*:

<https://docs.fortinet.com/document/fortiweb>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For details, see [Permissions on page 46](#).

Syntax

```

config user admin-usergrp
  edit "<group_name>"
    config members
      edit <entry_index>
        set type {ldap | radius | pki | tacacs+}
        set ldap-name "<query_name>"
        set radius-name "<query_name>"
        set tacacs+-name "<tacacs+_name>"
      next
    next
  next
end

```

```

    end
  next
end

```

Variable	Description	Default
"<group_name>"	Enter the name of the remote authentication group. The maximum length is 63 characters.	No default.
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999,999.	No default.
type {ldap radius pki tacacs+}	Select the protocol used for the query, LDAP, RADIUS, PKI or TACACS+.	ldap
ldap-name "<query_name>"	Enter the name of an existing LDAP account query. The maximum length is 63 characters. To display the list of existing queries, enter: edit ?	No default.
radius-name "<query_name>"	Enter the name of an existing RADIUS account query. The maximum length is 63 characters. To display the list of existing queries, enter: edit ?	No default.
pki-name "<pki_name>"	Enter the name of an existing PKI user. The maximum length is 63 characters. To display the list of existing queries, enter: edit ?	No default.
tacacs+-name "<tacacs+_name>"	Enter the name of an existing TACACS+. The maximum length is 63 characters. To display the list of existing queries, enter: 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

- [system admin on page 223](#)
- [user ldap-user on page 397](#)
- [user pki-user on page 406](#)
- [user radius-user on page 407](#)
- ["server-policy custom-application application-policy" on page 1](#)
- [user tacacs+ user on page 412](#)

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 details, see [waf site-publish-helper rule on page 626](#) and the *FortiWeb Administration Guide*:

<https://docs.fortinet.com/document/fortiweb>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config user kerberos-user
  edit "<kdc_name>"
    set realm "<realm_str>"
    set shortname <shortname_str>
    set status {enable | disable}
    config server-members
      edit "<entry_index>"
        set server <server_str>
        set port <port_int>
      next
    end
  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.

Variable	Description	Default
shortname <shortname_str>	Enter the shortname for the realm you specified (This is optional). A shortname is an alias of the delegated realm; it can be any set of characters except for symbols "@", "/" and "\". For example, the shortname can include the domain name of the realm that is not fully qualified. With a shortname being configured, the format of UPN can be username@shortname.	No default.
status {enable disable}	Specify whether the KDC configuration is enabled.	enable
server <server_str>	Enter the IP address of the KDC.	No default.
port <kdc-port_int>	Enter the port the KDC uses to listen for requests.	No default.
"<entry_index>"	Enter the index number of the server in the table.	No default.

Related topics

- [waf site-publish-helper rule on page 626](#)
- ["waf site-publish-helper keytab_file" on page 1](#)

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 [user user-group on page 413](#).

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 [user admin-usergrp on page 394](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For details, see [Permissions on page 46](#).

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_domain>"
set ssl-connection {enable | disable}
set ca-cert <ca_name>
set username "<bind-dn_str>"
next
end

```

Variable	Description	Default
"<ldap-query_name>"	Enter the name of the LDAP user query. The maximum length is 63 characters. To display the list of existing queries, enter: 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>" on page 398, distinguished-name "<search-dn_str>" on page 398, and the client-supplied user name. regular—Bind using a bind DN and password that you configure in username "<bind-dn_str>" on page 400 and password "<bind-password_str>" on page 399. anonymous—Do not provide a bind DN or password. Instead, perform the query without authenticating. Select this option only if the LDAP directory supports anonymous queries.	simple
common-name-id "<cn-attribute_str>"	Enter the identifier, often <code>cn</code> , 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>"	Enter the distinguished name (DN) such as <code>ou=People,dc=example,dc=com</code> , 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>"	Enter 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 {anonymous simple regular} on page 398 is <code>regular</code> .	No default.

Variable	Description	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} on page 399 and group_dn "<group-dn_str>" on page 399. This option is valid only when bind-type {anonymous simple regular} on page 398 is <code>regular</code>.	enable
group_dn "<group-dn_str>"	Enter the distinguished name of the LDAP user group, such as <code>ou=Groups,dc=example,dc=com</code>. The maximum length is 255 characters. This option is valid only when group_authentication {enable disable} on page 399 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 {enable disable} on page 399 is enabled.	open-ldap
password "<bind-password_str>"	Enter the password of the username "<bind-dn_str>" on page 400. 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 {anonymous simple regular} on page 398 is <code>anonymous</code> or <code>simple</code>.	No default.
port <port_int>	Enter the port number where the LDAP server listens. The valid range is 1–65535. The default port number varies by your selection in ssl-connection {enable disable} on page 400; 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 {enable disable} on page 400 is <code>enable</code>.	ldaps
server "<ldap_ipv4_domain>"	Type the server IP or domain address of the LDAP server.	0.0.0.0

Variable	Description	Default
ssl-connection {enable disable}	Enable to connect to the LDAP servers using an encrypted connection, then select the style of the encryption in protocol {ldaps starttls} on page 399.	enable
ca-cert <ca_name>	Enter the name of the certificate so the FortiWeb will only accept a certificate from the LDAP server that is signed by this CA. Only available when <code>ssl-connection</code> is enabled.	No default.
username "<bind-dn_str>"	Enter the bind DN, such as <code>cn=FortiWebA,dc=example,dc=com</code> , of an LDAP user account with permissions to query the distinguished-name "<search-dn_str>" on page 398. 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 {anonymous simple regular} on page 398 is <code>anonymous</code> or <code>simple</code> .	No default.

Example

This example configures an LDAP user query to the server at 192.0.2.100 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 "192.0.2.100"
    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

- [user user-group](#) on page 413
- [system admin](#) on page 223
- [user admin-usergrp](#) on page 394

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*:

<https://docs.fortinet.com/document/fortiweb>

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 [user user-group on page 413](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For details, see [Permissions on page 46](#).

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>"	Enter a name that can be referenced in other parts of the configuration. To display the list of existing accounts, enter: <code>edit ?</code> The maximum length is 63 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>"	Enter the user name that the client must provide when logging in, such as <code>user1</code> or <code>user1@example.com</code> . The maximum length is 63 characters.	No default.
password "<password_str>"	Enter 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

- [user user-group on page 413](#)

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*:

<https://docs.fortinet.com/document/fortiweb>

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 [user user-group on page 413](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For details, see [Permissions on page 46](#).

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>"	Enter the name of the NTLM user query. The maximum length is 63 characters. To display the list of existing queries, enter: <code>edit ?</code>	No default.
port <port_int>	Enter the port number where the NTLM server listens. The valid range is 1–65535.	445
server "<ntlm_ipv4>"	Enter the IP address of the NTLM server.	No default.

Example

This example configures an NTLM query connection to a server at `192.0.2.101` on port `445`.

```
config user ntlm-user
```

```
edit "ntlm-user1"
  set server "192.0.2.101"
  set port 445
next
end
```

Related topics

- [user user-group on page 413](#)

user oauth-user request

FortiWeb supports front-end authentication with third party authentication servers such as Google and Facebook.

Use this command to create OAuth requests. For more information about OAuth requests, refer to "OAuth authorization & OIDC authentication" in 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 details, see [Permissions on page 46](#).

Syntax

```
config user oauth-user request
  edit <oauth_request_name>
    set type {authz | token | refresh | validate | userinfo | jwks}
    set endpoint <string>
    set method {get | post}
    set ctype {urlencoded | json}
    set user-key <string>
    set tls-check {enable | disable}
    set tls-ca <ca_name>
    config custom-headers
      edit <index>
        set <custom-parameters_name>
        set <custom-parameters_value>
      next
    end
    config custom-parameters
      edit <index>
        set <custom-headers_name>
        set <custom-headers_value>
      next
    end
  next
end
```

Variable	Description	Default
<oauth_request_name>	Enter a name for the request.	No default
type {authz token refresh validate userinfo jwks}	Select the OAuth request types.	authz
endpoint <string>	Enter the OAuth request URL.	No default
method {get post}	Select the request method.	post
ctype {urlencoded json}	Select the request content type.	urlencoded
user-key <string>	Indicate username keyword in response.	No default
tls-check {enable disable}	Enable to do strict TLS verification even with a custom CA certificate to check the TLS traffic between FortiWeb and the third party OAuth authorization servers.	disable
tls-ca <ca_name>	Select the certificate to check the TLS traffic. It's uploaded in System > Admin > Certificates .	No default
<custom-headers_name>	Enter the name of the header to insert in the request.	No default
<custom-headers_value>	Enter the value of the header.	No default
<custom-parameters_name>	Enter the name of the parameter to insert into the request.	No default
<custom-parameters_value>	Enter the value of the parameter.	No default

Related topics

- [user oauth-user server](#)

user oauth-user server

FortiWeb supports front-end authentication with third party authentication servers such as Google and Facebook.

Use this command to add the third party authentication server information.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config user oauth-user server
  edit <server_name>
    set mode {client | resource-server | both}
```

```

set scope <string>
set oidc {enable | disable}
set client-id <string>
set client-secret <passwd>
set redirect-endpoint <string>
set authz-req <datasource>
set token-req <datasource>
set validate-req <datasource>
set validate-frequency {session | transaction | interval}
set validate-interval <integer>
set userinfo-req <datasource>
set jwks-req <datasource> on page 405

```

```

next

```

```

end

```

Variable	Description	Default
mode {client resource-server both}	Select whether FortiWeb works as an authorization client or a resource server, or both.	No default
scope <string>	Enter the scope field for OAuth.	No default
oidc {enable disable}	Enable to use OIDC authentication.	disable
client-id <string>	A client credential. Assigned by authorization server.	urlencoded
client-secret <passwd>	A client credential. Assigned by authorization server.	No default
redirect-endpoint <string>	Redirection URL back to FortiWeb.	disable
authz-req <datasource>	The authorization request created in <code>config user oauth-user request</code> .	No default
token-req <datasource>	The token request created in <code>config user oauth-user request</code> .	No default
refresh-req <datasource>	The refresh request created in <code>config user oauth-user request</code> .	No default
validate-req <datasource>	The valid request created in <code>config user oauth-user request</code> .	No default
validate-frequency {session transaction interval}	Whether to validate the request per session, transaction, or every several second.	No default
validate-interval <integer>	If the validate-frequency is interval, then enter the interval time.	No default
userinfo-req <datasource>	The user info request created in <code>config user oauth-user request</code> .	No default
jwks-req <datasource>	The JWKS request created in <code>config user oauth-user request</code> .	No default

Variable	Description	Default
	Available only if <code>oidc</code> is enabled.	

Related topics

- [user oauth-user request](#)

user pki-user

In FortiWeb's certificate-based Web UI login, a PKI user is the administrator that FortiWeb will authorize his Web UI access based on his PKI certificate. With this command, you can create a PKI user for FortiWeb to verify and authorize the Web UI accesses from the user.

Before creating a PKI user, you must import the CA certificate (through FortiWeb Web UI) associated with the user to the FortiWeb. For details, see [system admin-certificate ca on page 228](#).

After the PKI user is created, include it in an admin group through [user admin-usergrp on page 394](#).

For information about certificate-based Web UI login, see the *FortiWeb Administration Guide*:

<https://docs.fortinet.com/document/fortiweb>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config user pki-user
  edit "<pki-user_name>"
    set cacert "<cacert_str>"
    set subject "<subject_str>"
  next
end
```

Variable	Description	Default
"<pki-user_name>"	Enter the name of a PKI user. The maximum length is 63 characters.	No default.
cacert "<cacert_str>"	Specifies the CA certificate associated with the PKI user's certificate. It must be one of the CA certificates stored on the FortiWeb for administration. For details, see system admin-certificate ca on page 228 .	No default.
subject "<subject_str>"	Specifies the subject of the PKI user's certificate, such as <code>C = US, ST = Washington, O = yourorganization, CN = yourname</code> .	No default.

Example

This example adds a PKI user associated with the CA certificate CA_Cert_1.

```
config user pki-user
  edit "pki_user1"
    set cacert "CA_Cert_1"
    set subject "C = US, ST = Washington, O = organization, CN = Bradley Avery"
  next
end
```

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 (e.g., 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 "[server-policy custom-application application-policy](#)" on page 1.



For access profiles, FortiWeb appliances support RFC 2548 (<http://www.ietf.org/rfc/rfc2548.txt>) Microsoft Vendor-specific RADIUS Attributes. If you do not want to use them, you can configure them locally instead. For details, see [system accprofile on page 220](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config user radius-user
  edit "<radius-query_name>"
    set secret "<password_str>"
    set server {radius_ipv4 | radius_ipv6 | domain name}
    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 | domain name}
set secondary-server-port <port_int>
set fac-push {enable | disable}
next
end

```

Variable	Description	Default
"<radius-query_name>"	Enter a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 63 characters. To display the list of existing queries, enter: <pre>edit ?</pre> 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>" on page 224 or username "<user_str>" on page 401.	No default.
secret "<password_str>"	Enter the RADIUS server secret key for the primary RADIUS server. The primary server secret key should be a maximum of 16 characters in length, but is allowed to be up to 63 characters.	No default.
server {radius_ipv4 radius_ipv6 domain name}	Enter the IP address or domain name of the RADIUS server to query for users.	No default.
server-port <port_int>	Enter the port number where the RADIUS server listens. The valid range is 1–65535.	1812
auth-type {default chap ms_chap ms_chap_v2 pap}	Enter the authentication method. The <code>default</code> option uses PAP, MS-CHAP-V2, and CHAP, in that order.	default
nas-ip "<nas_ipv4>"	Enter the NAS IP address and called station ID. For details, see RFC 2548 (http://www.ietf.org/rfc/rfc2548.txt). 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>"	Enter the RADIUS server secret key for the secondary RADIUS server. The secondary server secret key should be a maximum of 16 characters in length, but is allowed to be up to 63 characters.	No default.
secondary-server {radius2_ipv4 domain name}	Enter the IP address or domain name of the secondary RADIUS server.	No default.
secondary-server-port <port_int>	Enter the port number where the secondary RADIUS server listens. The valid range is 1–65535.	1812

Variable	Description	Default
fac-push {enable disable}	If you are using FAC Radius server to authenticate clients, you can enable this option to send FortiToken mobile notification automatically to clients for extra token authentication.	disable

Related topics

- [user admin-usergrp on page 394](#)
- [user user-group on page 413](#)

user recaptcha-user

Use this command to create a reCAPTCHA server that FortiWeb uses to perform bot confirmation with Google reCAPTCHA service. This requires you to set the site key and secret key in the reCAPTCHA server configurations in FortiWeb so that it can communicate with the reCAPTCHA service on behalf of your application server.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For details, see [Permissions on page 46](#).

To use this command, you should enable `recaptcha` in `system feature-visibility`. See [system feature-visibility](#).

Syntax

```
config user recaptcha-user
  edit "<recaptcha_server_name>"
    set type {textbox | invisible | reCAPTCHA-V3}
    set site-key <str>
    set secret-key <str>
  next
end
```

Variable	Description	Default
type {textbox invisible reCAPTCHA-V3}	Select the type of the reCAPTCHA service you have registered in Google.	textbox
site-key <str>	Enter the site key	No default.
secret-key <str>	Enter the secret key.	No default.

user saml-user

Use this command to configure queries that can be used for remote authentication of either FortiWeb administrators or end users via a Security Assertion Markup Language (SAML) server.

To use a SAML server for client authentication, you need to first add this SAML server to a SAML server pool (for details, see [waf site-publish-helper saml-spool on page 639](#)), then select the server pool in a site publish rule (for details, see [waf site-publish-helper rule on page 626](#)).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config user saml-user
  edit "<saml_server_name>"
    set entityID "<server_URL>"
    set service-path "<server_URL_path>"
    set enforce-signing {enable | disable}
    set slo-bind {post | redirect}
    set slo-path "<slo_URL_path>"
    set sso-bind <post>
    set sso-path "<sso_URL_path>"
    config mapping-domains
      edit <index>
        set domain <domain_name>
      next
    end
  next
end
```

Variable	Description	Default
"<saml_server_name>"	Enter a name that can be referenced by other parts of the configuration. The maximum length is 63 characters.	No default.
entityID "<server_URL>"	Enter the URL for the SAML server. The communications protocol must be HTTPS.	No default.
service-path "<server_URL_path>"	Enter a path for the SAML server at the URL you specified in entityID "<server_URL>" on page 410 .	No default.
enforce-signing {enable disable}	Enable to enforce signing verification to digitally sign the SAML message, and then the Identity Provider will verify the signature to confirm its integrity.	disable
slo-bind {post redirect}	Select the binding that the server will use when the service provider initiates a single logout request: <code>POST</code>—SAML protocol messages are transported via the user's browser in an XHTML document using base64-encoding.	POST

Variable	Description	Default
	REDIRECT—SAML protocol messages will be carried in the URL of an HTTP <code>GET</code> request. Because the length of URLs is limited, this option is best for shorter messages. If the SAML message contains information that the IDP is not yet aware of, you can sign the message for security purposes.	
slo-path "<slo_URL_path>"	Enter a partial URL that the IDP will use to confirm with the service provider that a user has been logged out.	No default.
sso-bind <post>	Select the binding that the server will use to transport the SAML authentication request to the IDP.	POST
sso-path "<sso_URL_path>"	Enter a partial URL that the IDP will use to confirm with the service provider that a user has been authenticated.	No default.
<index>	Enter the index number for the domain name.	No default
domain <domain_name>	Add domain names for this server. When users log in with an email address suffixed with the specified domain name, the authentication request will be forwarded to this SAML server. For instance, if a user enters "xxx@example.com" in the Email field, FortiWeb will forward the request to the SAML server which is configured with the domain name "example.com".	No default

Authentication Required

Please choose a SAML IdP or provide the email address to continue

IdP

OR

Email

You can add multiple domain names for one SAML server. Similarly, it's allowed to associate multiple SAML server with the same domain name.

Example

This example configures a SAML server at `https://sp.example.com/samlsp`. We specify the Service Path, Assertion Consumer Service (ACS), and Single Logout Service (SLS). We use a `POST` binding for ACS and a `REDIRECT` binding for SLS.

```
config user saml-user
  edit "saml_example"
```

```

set entityID "https://sp.example.com/samlsp"
set service-path "/saml.sso"
set slo-bind redirect
set slo-path "/SLO/REDIRECT"
set sso-bind post
set sso-path "/SAML2/POST"
next
end

```

Related topic

- [waf site-publish-helper rule on page 626](#)

user tacacs+ user

Use this command to configure TACACS+ queries that can be used for authentication of administrators' access to the web UI or CLI.

To authenticate an administrator, the FortiWeb appliance sends the administrator's credentials to TACACS+ server for authentication. If the TACACS+ server replies to the query with a signal of successful authentication, the client is successfully authenticated with the FortiWeb appliance. If TACACS+ authentication fails or the query returns a negative result, the appliance refuses the connection.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For details, see "[Permissions](#)" on page 1.

Syntax

```

config user tacacs+-user
edit "<tacacs+-user_name>" on page 412
    set server {radius_ipv4 | domain name} on page 412
    set secret "<password_str>" on page 412
    set auth-type {auto | ms_chap | chap | pap | ascii} on page 412
next
end

```

Variable	Description	Default
"<tacacs+-user_name>"	Enter a unique name that can be referenced in other parts of the configuration. The maximum length is 63 characters.	No default.
server {radius_ipv4 domain name}	Enter the IP address or domain name of the TACACS+ server.	No default.
secret "<password_str>"	Enter the TACACS+ server secret key for the TACACS+ server.	No default.
auth-type {auto ms_chap chap pap ascii}	Select Auto to automatically assign an authentication type or select Specify to specify a type among MSCHAP, CHAP, PAP, and ASCII.	Auto

Related topics

- [user tacacs+ user on page 412](#)
- [user user-group on page 413](#)

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 [user local-user on page 401](#), [user ldap-user on page 397](#), ["server-policy custom-application application-policy" on page 1](#), or [user ntlm-user on page 402](#).

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 [waf HTTP-authen HTTP-authen-rule on page 529](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `authusergrp` area. For details, see [Permissions on page 46](#).

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>"	Enter the name of the user group. The maximum length is 63 characters. To display the list of existing groups, enter: <code>edit ?</code>	No default.
auth-type {basic digest NTLM}	Select one of the following authentication types: • <code>basic</code>—This is the original and most compatible	<code>basic</code>

Variable	Description	Default
	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.	
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999.	No default.
ldap-name "<query_name>"	Select the name of a LDAP user query. Available if the value of type {ldap local ntlm radius} on page 414 is <code>ldap</code>. The maximum length is 63 characters.	No default.
local-name "<query_name>"	Select the name of a local user account. Available if the value of type {ldap local ntlm radius} on page 414 is <code>local</code>. The maximum length is 63 characters.	No default.
ntlm-name "<query_name>"	Select the name of a NTLM user query. Available if the value of type {ldap local ntlm radius} on page 414 is <code>ntlm</code>. The maximum length is 63 characters.	No default.
radius-name "<query_name>"	Select the name of a RADIUS user query. Available if the value of type {ldap local ntlm radius} on page 414 is <code>radius</code>. The maximum length is 63 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 auth-type {basic digest NTLM} on page 413 does not support a given user type, all user accounts of that type will be ignored, effectively disabling them.	<code>local</code>

Example

For an example, see [waf HTTP-authen HTTP-authen-policy on page 527](#).

Related topics

- [user ldap-user on page 397](#)
- [user local-user on page 401](#)
- [user ntlm-user on page 402](#)
- [waf HTTP-authen HTTP-authen-rule on page 529](#)

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 details, see [Permissions on page 46](#).

Syntax

```
config wad file-filter
  edit "<wad-file-filter_name>"
    set filter-type {block-file-list | allow-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>"	Enter the name of the file filter you can reference in other parts of the configuration.	No default.
filter-type {block-file-list allow-file-list}	Specify the type of filter: • <code>block-file-list</code>—A list of files or folders that the anti-defacement feature does not monitor. • <code>allow-file-list</code>—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>	Enter 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: • <code>directory</code>—A folder or directory path. • <code>regular-file</code>—A file.	No default.

Variable	Description	Default
file-name "<file_str>"	Enter the name of the folder or file to add to the list. Ensure that the name exactly matches the folder or file that you want to specify. If <code>file-type {directory regular-file}</code> on page 415 is <code>directory</code>, include the / (forward slash). For example, if <code>file-type</code> is <code>directory</code> and you want to add a folder <code>abc</code> that is under the root folder of a website, enter <code>/abc</code>. You can restrict the filter condition to a specific file by including file path information in <code>file-name</code>. For example, a website contains many files with the name <code>123.txt</code>. To specify the instance located in the <code>abc</code> folder only, enter <code>/abc/123.txt</code>.	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 block-file-list
    edit 1
      set file-type directory
      set file-name "/abc"
    next
  end
```

Related topics

- [wad website on page 416](#)

wad website

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

The FortiWeb appliance monitors the website'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 website 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 (blocklist) or the specific files and folders you want it to monitor (allowlist). For details, see [wad file-filter on page 415](#).

FortiWeb automatically backs up website 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 website'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 website, 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. For details, see [backup-max-fsize <limit_int> on page 418](#) and [backup-skip-ftype "<extensions_str>" on page 418](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wadgrp` area. For details, see [Permissions on page 46](#).

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>	Enter the index number of the individual entry in the table. The valid range is 1–16.	No default.
alert-email "<email-policy_name>"	Enter the name of the email policy that specifies the email address that FortiWeb sends an email to when it detects that the website changed. (See log email-policy on page 68 .)The maximum length is 63 characters.	No default.
auto {disable restore acknowledge}	Enter the action that FortiWeb takes when it detects that the website has changed. • <code>disable</code>—FortiWeb takes no action. You can use the	<code>disable</code>

Variable	Description	Default
	web UI to manually restore all or some of the changed files. <code>restore</code>—Restore the website to the previous revision number. <code>acknowledge</code>—Accept changes to the website. Note: When you intentionally modify the website, type <code>acknowledge</code>. Otherwise, the FortiWeb appliance detects your changes as a defacement attempt and undoes them.	
<code>backup-max-fsize <limit_int></code>	Enter a file size limit in kilobytes (KB) to indicate which files will be included in the website backup. Files exceeding this size will not be backed up. The valid range is 1–1,048,576 kilobytes. Note: Backing up large files can impact performance.	10240
<code>backup-skip-ftype</code> <code>"<extensions_str>"</code>	Enter zero or more file extensions, such as <code>iso</code>, <code>avi</code>, to exclude from the website 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.
<code>connect-type {ftp smb ssh}</code>	Select which protocol to use when connecting to the website in order to monitor its contents and download website backups. For Microsoft Windows-style shares, enter <code>smb</code>.	<code>ftp</code>
<code>description "<comment_str>"</code>	Enter 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.
<code>hostname-ip {"<host_ipv4>" "<host_fqdn>"}</code>	Enter the IP address or fully qualified domain name (FQDN) of the physical server on which the website is hosted. This will be used when connecting by SSH or FTP to the website 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 <code>Host :</code> field of HTTP headers.	No default.
<code>interval-other <seconds_int></code>	Enter the amount of time (in seconds) between each monitoring connection from the FortiWeb appliance to the web server. During this connection, the FortiWeb appliance examines the website's subfolders to see if any files have been changed by comparing the files with the latest backup. The valid range is 1–86,400.	600

Variable	Description	Default
	If any file change is detected, the FortiWeb appliance will download a new backup revision. If you've enabled auto {disable restore acknowledge} on page 417, the FortiWeb appliance will revert the files to their previous version.	
interval-root <seconds_int>	Enter 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>" on page 420 (but not its subfolders) to see if any files have been changed by comparing the files with the latest backup. The valid range is 1–86,400. If any file change is detected, the FortiWeb appliance will download a new backup revision. If you've enabled auto {disable restore acknowledge} on page 417, the FortiWeb appliance will revert the files to their previous version.	60
monitor {enable disable}	Enable to monitor the website's files for changes, and to download backup revisions that can be used to revert the website to its previous revision if the FortiWeb appliance detects a change attempt.	enable
monitor-depth <folders_int>	Enter how many folder levels deep to monitor for changes to the website's files. Files in subfolders deeper than this level will not be backed up. The valid range is 1–10.	5
name "<name_str>"	Enter a name for the website. The maximum length is 63 characters. This name will not be used when monitoring the website, 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 website's FQDN or virtual host name.	No default.
password "<password_str>"	Enter the password for the user name you entered in user "<user_str>" on page 420. The maximum length is 63 characters.	No default.
port <port_int>	Enter the port number on which the website'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 {ftp smb ssh} on page 418 is <code>ftp</code> or <code>ssh</code> .	21
share-name "<share_str>"	Enter the name of the shared folder on the web server. The maximum length is 63 characters.	No default.

Variable	Description	Default
	This variable appears only if connect-type {ftp smb ssh} on page 418 is <code>smb</code> .	
<code>user "<user_str>"</code>	Enter the user name that the FortiWeb appliance will use to log in to the website's physical server. The maximum length is 63 characters.	No default.
<code>web-folder "<path_str>"</code>	Enter the path to the website's folder, such as <code>public_html</code> , on the physical server. The path is relative to the initial location when logging in with the user name that you specify in <code>user "<user_str>"</code> . The maximum length is 1,023 characters. Available only if the value of connect-type {ftp smb ssh} on page 418 is <code>ftp</code> or <code>ssh</code> .	No default.
<code>file-filter "wad-file-filter_name"></code>	Enter 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 "192.0.2.10"
    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

- [wad file-filter on page 415](#)
- [system interface on page 344](#)
- [router static on page 101](#)

waf advanced-bot-protection

FortiGuard Advanced Bot Protection is a SaaS (Software as a Service) solution designed to protect your online applications from malicious bots and automated attacks.

By incorporating FortiGuard Advanced Bot Protection (FortiGuard ABP) into FortiWeb's server policy, client traffic will be directed to the FortiGuard ABP service deployed on Google Cloud. It can analyze the traffic to identify any malicious bot behavior and suggest appropriate actions in response.

FortiGuard ABP builds up a machine learning model to protect against a wide range of threats, including Data harvesting, Credential stuffing attacks, Account takeover attempts, and DDoS attacks.

This topic introduces the FortiGuard ABP related CLI commands in FortiWeb. For the whole process of the FortiGuard ABP integration configuration, refer to "Configuring Advanced Bot Protection policy" in *FortiWeb Administration Guide*.

Syntax

```
config waf advanced-bot-protection
  edit waf advanced-bot-protection on page 420
    set application-id <string>
    set action {alert | deny_no_log | alert_deny | block-period | block-period-client}
    set severity {High | Medium | Low | Info}
    set trigger <trigger-policy_name>
    set exception {exception-policy-id}
    set bot-confirmation {enable | disable}
    set bot-recognition {captcha-enforcement | recaptcha-enforcement}
    set recaptcha <recaptcha_server_name>
    set validation-timeout <validation-timeout_int>
  next
end
```

Variable	Description	Default
"<advanced-bot-protection_name>"	Enter a name for the Advanced Bot Protection policy. You can reference it in the Web Protection Profile.	No default
application-id <string>	Enter the Application ID assigned to your FortiGuard ABP Application. The Application ID is used to bind this Advanced Bot Protection policy to the FortiGuard ABP Application. To obtain the ID, go to Application page of FortiGuard ABP, click the Settings icon in the Action column, then click Copy Application ID .	No default
action {alert deny_no_log alert_deny block-period block-period-client}	Select which action FortiWeb will take when FortiGuard ABP suggests a request is from a bot: • alert—Accept the connection and generate an alert email and/or log message. • alert_deny—Block the request (or reset the connection) and generate an alert and/or log message. • deny_no_log—Block the request (or reset the connection). • block-period—Block subsequent requests from the client for a number of seconds. • block-period-client—Block a malicious or suspicious client based on the FortiWeb	alert

Variable	Description	Default
	generated client ID. This is useful when the source IP of a certain client keeps changing. This option takes effect only when you enable Client Management in the Server Policy.	
block-period <content-scraping-block-period_int>	Enter the number of seconds that you want to block subsequent requests from an IP or client ID after FortiWeb detects content scraping activities. The valid range is 1–3,600 seconds. Available only if <code>action {alert deny_no_log alert_deny block-period block-period-client}</code> is set to <code>block-period</code> and <code>block-period-client</code> .	600
severity {High Medium Low Info}	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when FortiGuard ABP suggests a request is from a bot: • Informative • Low • Medium • High	Medium
trigger <trigger-policy_name>	Select the trigger, if any, that FortiWeb will use when it logs and/or sends an alert email when FortiGuard ABP suggests a request is from a bot. For details, see "Viewing log messages" on page 1.	No default.
exception {exception-policy-id}	Select the exception policy which specifies the elements to be exempted from the FortiGuard ABP scan.	No default
bot-confirmation {enable disable}	Enable to confirm if the client is indeed a bot. The system sends RBE (Real Browser Enforcement) JavaScript or CAPTCHA to the client to double check if it's a bot.	enable
bot-recognition {captcha-enforcement recaptcha-enforcement}	• <code>captcha-enforcement</code> — Requires the client to successfully fulfill a CAPTCHA request. CAPTCHA verification will not pop out for the bot confirmation again for the same user within 10 mins timeout. • <code>recaptcha-enforcement</code> — Requires the client to successfully fulfill a reCAPTCHA request.	captcha-enforcement
recaptcha <recaptcha_server_name>	Enter the reCAPTCHA server you have created through user recaptcha-user	No default.

Variable	Description	Default
bot-confirmation-max-attempt-times <int>	If <code>captcha-enforcement</code> is selected for bot-recognition, enter the maximum number of attempts that a client may attempt to fulfill a CAPTCHA request.	
validation-timeout <validation-timeout_int>	Enter the maximum amount of time (in seconds) that FortiWeb waits for results from the client.	20

Related topics

- [waf bot-deception on page 1](#)
- [waf biometrics-based-detection on page 442](#)
- [waf threshold-based-detection on page 658](#)
- [waf known-bots on page 571](#)

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 [waf web-protection-profile inline-protection on page 696](#) or [waf web-protection-profile offline-protection on page 706](#).

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 [server-policy allow-hosts on page 106](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf allow-method-exceptions
  edit "<method-exception_name>"
    config allow-method-exception-list
      edit <entry_index>
        set allow-request {get post head options trace connect delete put patch
          webdav rpc others}
        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>"	Enter the name of the allowed methods exception. The maximum length is 63 characters. To display a list of the existing exceptions, enter: <code>edit ?</code>	No default.
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999.	No default.
allow-request {get post head options trace connect delete put patch webdav rpc others}	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 applications such as Microsoft Exchange Server and Subversion, which may require HTTP methods not commonly used by web browsers, such as <code>PROPFIND</code> and <code>BCOPY</code> . For details, see RFC 4918 (http://tools.ietf.org/html/rfc4918). 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>"	Enter the name of a protected host that the <code>Host :</code> 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 <code>host-status {enable disable}</code> on page 424 is <code>enable</code> .	No default.
host-status {enable disable}	Enable to require that the <code>Host :</code> field of the HTTP request match a protected hosts entry in order to match the allowed method exception. Also configure <code>host "<protected-hosts_name>"</code> on page 424 .	disable
request-file "<url_str>"	Depending on your selection in <code>request-type {plain regular}</code> on page 425 , either: Enter the literal URL, such as <code>/index.php</code>, that is an exception to the generally allowed HTTP request methods. The URL must begin with a slash (/).	No default.

Variable	Description	Default
	Enter a regular expression, such as <code>^/*.php</code>, matching all and only the URLs which are exceptions to the generally allowed HTTP request methods. The pattern is not required to begin with a slash (<code>/</code>). However, it must at least match URLs that begin with a slash, such as <code>/index.cfm</code>. For example, if multiple URLs on a host have identical HTTP request method requirements, you would type a regular expression matching all of and only those URLs. Do not include the name of the web host, such as <code>www.example.com</code>, which is configured separately in host "<protected-hosts_name>" on page 424. The maximum length is 255 characters. Note: Regular expressions beginning with an exclamation point (<code>!</code>) are not supported. For information on language and regular expression matching, see the <i>FortiWeb Administration Guide</i>: https://docs.fortinet.com/document/fortiweb	
<code>request-type {plain regular}</code>	Indicate whether request-file "<url_str>" on page 424 is a literal URL (<code>plain</code>) or a regular expression (<code>regular</code>).	<code>plain</code>

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 `192.0.2.10`) 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

- [server-policy allow-hosts on page 106](#)
- [waf web-protection-profile inline-protection on page 696](#)

- [waf web-protection-profile offline-protection on page 706](#)

waf allow-method-policy

Use this command to allow only specific HTTP request methods.

To define specific exceptions to this policy, use [waf allow-method-exceptions on page 423](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf allow-method-policy
  edit "<allowed-methods_name>"
    set allow-method {get post head options trace connect delete put patch webdav rpc}
    set override-header {enable | disable}
    set override-parameter {enable | disable}
    set severity {High | Medium | Low | Info}
    set triggered-action "<trigger-policy_name>"
    set allow-method-exception "<method-exception_name>"
  next
end
```

Variable	Description	Default
"<allowed-methods_name>"	Enter 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 63 characters. To display a list of the existing policies, enter: <code>edit ?</code>	No default.
override-header {enable disable}	When Override Header or Override Parameter settings are enabled, FortiWeb should check methods from these headers or parameters as well as the HTTP method used in the actual request. If any of the methods are not in the allowed method list, FortiWeb should deny the request.	disable
override-parameter {enable disable}	When Override Header or Override Parameter settings are enabled, FortiWeb should check methods from these headers or parameters as well as the HTTP method used in the actual request. If any of the methods are not in the allowed method list, FortiWeb should deny the request.	disable
allow-method {get post head options trace connect delete put patch webdav rpc}	Select one or more HTTP request methods that you want to allow for this specific policy.	No default.

Variable	Description	Default
	Methods that you do not select will be denied, unless specifically allowed for a host and/or URL in analyzer-policy "<fortianalyzer-policy_name>" on page 97. The <code>others</code> option includes methods not specifically named in the other options. It often may be required by WebDAV applications such as Microsoft Exchange Server 2003 and Subversion, which may require HTTP methods not commonly used by web browsers, such as <code>PROPFIND</code> and <code>BCOPY</code>. For details, see RFC 2518 (http://tools.ietf.org/html/rfc4918). 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.	
severity {High Medium Low Info}	Select the severity level to use in logs and reports generated when a violation of the policy occurs.	High
triggered-action "<trigger-policy_name>"	Enter 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 63 characters. To display a list of the existing policies, enter: <pre>set triggered-action ?</pre>	No default.
allow-method-exception "<method-exception_name>"	Enter the name of an existing HTTP request method exception, if any, to apply to it. The maximum length is 63 characters. To display a list of the existing policy, enter: <pre>set allow-method-exception ?</pre>	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

- [waf allow-method-exceptions on page 423](#)

waf api-learning-policy

The machine learning based API Protection learns the REST API data structure from user traffic samples and then build a mathematical model to screen out malicious API requests.

It analyzes the method, URL, and endpoint data of the API request samples to generate an API data structure file for your application. This model describes the API data schema model of endpoint data. If the incoming API request violates the data structure, it will be detected as an attack.

Use this command to edit machine learning based API Protection policies.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf api-learning-policy
  edit <api-learning-policy_ID>
    set policy-id <index>
    set status {enable | disable}
    set ip-list-type {Trust | Black}
    set start-training-cnt <integer>
    set url-replacer-policy <string>
    set action-mlapi {alert | alert_deny | block-period | standby}
    set block-period-mlapi <integer>
    set severity-mlapi {High | Medium | Low | Info}
    set trigger-mlapi <datasource>
    set schema-property {maximum | minimum | maxLength | minLength | maxItems | minItems}
    set data-format {date-time | date | time | email | hostname | ipv4 | ipv6}
    set de-duplication-all {enable | disable}
    set de-duplication-count <integer>
    set schema-required-ratio <integer>
    set schema-ignored-ratio <integer>
    set svm-sensitivity-level {1 | 2 | 3 | 4}
  next
end
```

Variable	Description	Default
<api-learning-policy_ID>	Specify the API protection policy ID.	No default
policy-id <index>	Specify the server policy ID to associate this API protection policy with.	No default
status {enable disable}	Enable or disable API protection.	enable
ip-list-type {Trust Black}	Allow or deny sample collection from the Source IP	trust

Variable	Description	Default
	list.	
start-training-cnt <integer>	The system will start building API Protection machine learning model if the sample count reaches the <code>start-training-cnt</code> .	No default
url-replacer-policy <datasource>	Specify the URL replacer policy you want to use. If your applications have dynamic URLs or unusual parameter styles, you must use URL Replacer Policy to recognize them. See waf machine-learning url-replacer-rule/policy on page 590 for more information.	No default
action-mlapi {alert alert_deny block-period}	Choose the action FortiWeb takes when an API attack is detected. <code>alert</code> —Accepts the connection and generates an alert email and/or log message. <code>alert_deny</code> —Blocks the request (or resets the connection) and generates an alert and/or log message. <code>block-period</code> —Blocks the request for a certain period of time. <code>standby</code> —Selecting <code>standby</code> will activate the continuous learning mode. The system will continuously adjust the API learning models to adapt to changes in the API schema. This includes scenarios such as the introduction of new APIs, modifications to existing parameters, etc. It is important to note that blocking violations is not supported in continuous learning mode at present. However, you can go to API View to download the learned schema, then upload it to API Validation , which allows you to block malformed API requests.	alert_deny
block-period-mlapi <integer>	Enter the number of seconds that you want to block the requests. The valid range is 1–3,600 seconds. This option only takes effect when you choose Period Block in Action .	600
severity-mlapi {High Medium Low Info}	Select the severity level for this anomaly type. The severity level will be displayed in the alert email and/or log message.	High
trigger-mlapi <datasource>	Select a trigger policy that you have set in Log&Report > Log Policy > Trigger Policy . If an API attack is detected, it will trigger the system to send email and/or log messages according to the trigger policy.	No default

Variable	Description	Default
schema-property {maximum minimum maxLength minLength maxItems minItems}	In the learned model, it could include these properties and data formats under the string type. Specify the schema properties that will be learned by the API Protection machine learning model.	No default
data-format {date-time date time email hostname ipv4 ipv6}	Specify the data format that will be learned by the API Protection machine learning model.	No default
schema-required-ratio <integer>	The <code>schema-required-ratio</code> is the threshold for the required type. If the percentage of samples including a certain field is over the <code>schema-required-ratio</code> , this field will be treated as the required type and learned in the final model.	No default
schema-ignored-ratio <integer>	If the percentage of samples including a certain field is lower than the <code>schema-required-ratio</code> , this field will be discarded in the final model.	No default
svm-sensitivity-level {1 2 3 4}	Increasing the security level introduces more conditions that a request must meet to pass the scan. For example, a request that successfully passes at level 1 might be flagged as an anomaly at level 4 due to stricter criteria. While higher security levels enhance protection by enforcing more rigorous requirements, they also increase the risk of mistakenly blocking legitimate traffic.	1

waf api-learning-rule

Use this command to specify the domains to be protected by the ML based API protection model, and the API paths to be learned by the model.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf api-learning-rule
  edit <api-learning-rule_ID>
    set domain-name <index>
    config api-path-list
      edit api-path-list <id>
        set api-path-type {plain | regular}
        set api-path <string>
      next
    end
```

```

    next
end

```

Variable	Description	Default
<api-protection-rule_ID>	Specify the API protection policy ID.	No default
domain-name <string>	Enter the name of the domain to be protected.	No default
api-path-list <index>	Enter the API path list ID. The system by default learns API requests to all the URL paths of the domain. If you want to restrict the learning to certain API paths, specify the API paths that you want to system to learn.	No default
api-path-type {plain regular}	Specify whether the API pattern must contain a literal URL (plain), or a regular expression designed to match multiple URLs (regular).	plain
api-path <string>	- If the api-path-type is plain, then enter the the literal URL, such as <code>/folder1/index.htm</code> that the HTTP request must contain in order to match the rule, or use wildcards to match multiple URLs, such as <code>/folder1/*</code> or <code>/folder1/*/index.htm</code>. The URL must begin with a slash (/). - If the api-path-type is regular, then enter a regular expression, such as <code>^/*\.jsp\?uid\(.*\)</code>, matching all and only the URLs to which the rule should apply. The pattern does not require a slash (/); however, it must at least match URLs that begin with a slash, such as <code>/profile.cfm</code>.	No default

waf api-policy

Use this command to create API gateway policy.

Syntax

```

config waf api-policy
    edit <api-policy_name>
    config api-rule-list
        edit <api-rule-list_id>
            set api-rule-name <api-rule-name_str>
        next
    end
next

```

```
end
```

Variable	Description	Default
<api-policy_name>	Enter a name for the API gateway policy.	No default.
<api-rule-list_id>	The index number of the API gateway rule entry.	No default.
api-rule-name <api-rule-name_str>	Select the created API gateway rule.	No default.

Related topics

- [waf api-user-group on page 439](#)
- [waf api-rules on page 432](#)
- [waf api-users on page 437](#)

waf api-rules

To restrict API access, you can use this command to configure certain rules involving API key verification, API key carryover, API user grouping, sub-URL setting, and specified actions FortiWeb will take in case of any API call violation.

Syntax

```
config waf api-rules
edit <api-rules_name>
    set api-key-verification {enable | disable}
    set allow-user-group <allow-user-group_name>
    set api-key-location {HTTP-parameter | HTTP-header}
    set header-field-name <header-field-name_str>
    set parameter-name <parameter-name_str>
    set rate-limit-period <rate-limit-period_int>
    set rate-limit-requests <rate-limit-requests_int>
    set rate-limit-user-period <rate-limit-user-period_int>
    set rate-limit-user-requests <rate-limit-user-requests_int>
    set x-ratelimit-headers <enable|disable>
    set action {alert | deny_no_log | alert_deny | block-period}
    set block-period <block-period_int>
    set severity {High | Medium | Low | Info}
    set trigger-policy <trigger-policy_str>
    set host <host_str>
    set host-status {enable | disable}
    config attach-HTTP-header
        edit <attach-HTTP-header_id>
            set HTTP-header-item <HTTP-header-item_str>
        next
    end
    config match-url-prefixes
        edit <match-url-prefixes_id>
            set frontend-prefix <frontend-prefix_str>
```



```

        set backend-prefix <backend-prefix_str>
    next
end
config sub-url-setting
    edit <sub-url-setting_id>
        set HTTP-method {get | post | head | options | trace | connect | delete | put |
            patch | any}
        set type {plain | regular}
        set url-expression <url-expression_str>
        set api-key-verification {enable | disable}
        set api-key-location {HTTP-parameter | HTTP-header}
        set header-field-name <header-field-name_str>
        set parameter-name <parameter-name_str>
        set rate-limit-period <rate-limit-period_int>
        set rate-limit-requests <rate-limit-requests_int>
        set rate-limit-user-period <rate-limit-user-period_int>
        set rate-limit-user-requests <rate-limit-user-requests_int>
        set allow-user-group <allow-user-group_name>
        set api-key-inherit {enable | disable}
    next
end
next
end
end

```

Variable	Description	Default
<api-rules_name>	Type a unique name for the API gateway rule.	No default
api-key-verification {enable disable}	When an user makes an API request, the API key will be included in HTTP header or parameter, FortiWeb obtains the API key from the request. When this option is enabled, FortiWeb verifies the key to check whether the key belongs to an valid API user.	disable
allow-user-group <allow-user-group_str>	Select a user group created to define which users have the permission to access the API. Available only when waf api-rules is enable.	disable
api-key-location {HTTP-parameter HTTP-header}	Indicate where FortiWeb can find your API key in HTTP request: • HTTP-parameter • HTTP-header	HTTP-parameter
header-field-name <header-field-name_str>	Enter the header filed name in which FortiWeb can find the API key when api-key-location {HTTP-parameter HTTP-header} is HTTP Header.	No default.
parameter-name <parameter-name_str>	Enter the parameter name in which FortiWeb can find the API key when api-key-location {HTTP-parameter HTTP-header} is HTTP Parameter.	No default.
rate-limit-period <rate-limit-period_int>	Type the maximum number of API call requests allowed in a certain number of seconds .	No default.

Variable	Description	Default
rate-limit-requests <rate-limit-requests_ int>	Type the maximum number of API call requests allowed in a certain number of seconds.	No default.
rate-limit-user-period <rate-limit-user-period_ int>	Limit API requests by users. Type the maximum number of API call requests allowed per user in a certain number of seconds .	No default.
rate-limit-user-requests <rate-limit-user- requests_int>	Type the maximum number of API call requests allowed per user in a certain number of seconds.	No default.
x-ratelimit-headers {enable disable}	Enable to add X-RateLimit-* headers in the response packet if the user exceeds the rate limit. The following information can be displayed to users: the request limit, the remaining requests, and the minimum time to wait before the user is allowed to send the next request.	disable
action {alert deny_no_ log alert_deny block- period}	Select which action FortiWeb will take when it detects any API call violation: alert—Accept the connection and generate an alert email and/or log message. alert_deny—Block the request (or reset the connection) and generate an alert and/or log message. deny_no_log—Block the request (or reset the connection). block-period—Block subsequent requests from the client for a number of seconds. Also configure waf api-rules.	alert
block-period <block- period_int>	Enter the number of seconds that you want to block subsequent requests from a client after FortiWeb detects any API call violation. The valid range is 1–10,000 seconds. Available only if waf api-rules is set to block-period .	600
severity {High Medium Low Info}	When policy violations are recorded in the attack log, each log message contains a Severity Level (severity_level) field. Select which severity level FortiWeb will use when it logs any API call violation: - Informative - Low - Medium - High	Low
trigger-policy <trigger- policy_str>	Select the trigger, if any, that FortiWeb will use when it logs and/or sends an alert email about any API call violation. For details, see " Viewing log messages " on page 1.	No default.
host <host_str>	Select the name of a protected host that the Host: field of an HTTP request must be in to match the API gateway rule.	No default.

Variable	Description	Default
	This option is available only if waf api-rules is enable.	
host-status {enable disable}	Enable to apply this rule only to HTTP requests for specific web hosts. Also configure waf api-rules .	disable
<attach-HTTP-header_id>	Enter the sequence number of the HTTP header.	No default.
HTTP-header-item <HTTP-header-item_str>	Enter the HTTP header item.	No default.
<match-url-prefixes_id>	The sequence number of the match URL prefixes.	No default.
frontend-prefix <frontend-prefix_str>	Enter the Frontend Prefix; the frontend prefix is the URL path in a client call, for example, /fortiweb/, the URL is like this <code>https://172.22.14.244/fortiweb/example.json?param=value</code> .	No default.
backend-prefix <backend-prefix_str>	Enter the Backend Prefix; the backend prefix is the path which the client request will be replaced with, for example, /api/v1.0/System/Status/. After the URL rewriting, the URL is like this <code>https://10.200.3.183:90/api/v1.0/System/Status/example.json?param=value</code> .	No default.
<sub-url-setting_id>	Enter the sequence number of the sub-URL.	No default.
HTTP-method {get post head options trace connect delete put patch any}	Select the HTTP method from the drop down list.	GET
type {plain regular}	Select whether the url-expression <url-expression_str> field must contain either: - plain—The field is a string that the request URL must exactly. - regular—The field is a regular expression that defines a set of matching URLs.	plain
url-expression <url-expression_str>	Depending on your selection in type {plain regular} , enter 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 backslash (/). - A regular expression, such as ^/*.php, matching all and only the URLs to which the input rule should apply. The pattern does not require a slash (/); however, it must at least match URLs that begin with a slash, such as /index.cfm.	No default.

Variable	Description	Default
api-key-verification {enable disable}	When an user makes an API request, the API key will be included in HTTP header or parameter, FortiWeb obtains the API key from the request. When this option is enabled, FortiWeb verifies the key to check whether the key belongs to an valid API user.	disable
api-key-location {HTTP-parameter HTTP-header}	Indicate where FortiWeb can find your API key in HTTP request: - HTTP-parameter - HTTP-header Available only when api-key-verification {enable disable} is enable.	HTTP-parameter
header-field-name <header-field-name_str>	Enter the header filed name in which FortiWeb can find the API key when api-key-location {HTTP-parameter HTTP-header} is HTTP-header.	No default.
parameter-name <parameter-name_str>	Enter the parameter name in which FortiWeb can find the API key when api-key-location {HTTP-parameter HTTP-header} is HTTP-parameter.	No default.
rate-limit-period <rate-limit-period_int>	Type the maximum number of API call requests allowed in a certain number of seconds .	No default.
rate-limit-requests <rate-limit-requests_int>	Type the maximum number of API call requests allowed in a certain number of seconds.	No default.
rate-limit-user-period <rate-limit-user-period_int>	Limit API requests by users. Type the maximum number of API call requests allowed per user in a certain number of seconds .	No default.
rate-limit-user-requests <rate-limit-user-requests_int>	Type the maximum number of API call requests allowed per user in a certain number of seconds.	No default.
allow-user-group <allow-user-group_name>	Select a user group created to define which users have the permission to access the API. Available only when api-key-verification {enable disable} is enable.	No default.
api-key-inherit {enable disable}	When an user makes an API request, the API key will be included in HTTP header or parameter of sub URL, FortiWeb obtains the API key from the request. When this option is enabled, FortiWeb verifies the key to check whether the key belongs to an valid API user.	disable

Related topics

- [waf api-user-group on page 439](#)
- [waf api-policy on page 431](#)

- [waf api-users on page 437](#)

waf api-users

Use this command to define API users to restrict access to APIs based on API keys.

Syntax

```
config waf api-users
  edit <api-user_name>
    set email <email_str>
    set comments <comments_str>
    set uuid <uuid_str>
    set api-key <api-key_str>
    set create-time <create-time_str>
    set key-mode {dynamic | jwt | standard}
    set url <jwt_url>
    set headers <jwt_headers>
    set params <jwt_parameters>
    set phantom-token-name <token_name>
    set token-name <token_name>
    set header-verification <string>
    set payload-validation <string>
    set rsa-key
  config ip-access-list
    edit <ip-access-list_id>
      set ip <ip_str>
    next
  end
  config http-referer-list
    edit <http-referer-list_id>
      set http-referer <http-referer_str>
    next
  end
next
end
```

Variable	Description	Default
<api-user_name>	Enter a name that identifies the user.	No default.
email <email_str>	Type the email address of the user that is used for contact purpose.	No default.
comments <comments_str>	Optionally, enter a description or comments for the user.	No default.
uuid <uuid_str>	Enter a unique identifier for the requesting user.	No default.
api-key <api-key_str>	Specify an API key for the API user; the minimum length is 40 characters.	No default.

Variable	Description	Default
key-mode {dynamic jwt standard}	Standard Once the API user is created successfully, an API key and UUID are automatically assigned to this user by FortiWeb. Dynamic FortiWeb adopts RSA algorithm to generate token. It uses public key to encode, and private key to decode a random string with minimum length 64. You need to enter the RSA key for dynamic key. JWT JSON Web Token (JWT) is an open standard (RFC 7519) that defines a way for transmitting information –like authentication and authorization facts– between two parties: an issuer and an audience. For the JWT key, you need to enter the value for the following fields so that FortiWeb can communicate with the JWT server to validate the key.	Standard
url <jwt_url>	The URL that FortiWeb uses to communicate with the JWT server.	No default.
headers <jwt_headers>	The headers append to the URL.	No default.
params <jwt_parameters>	The parameters append to the URL.	No default.
phantom-token-name <token_name>	The name of the phantom token used for JWT key.	No default.
token-name <token_name>	The name of the token used for JWT key.	No default.
header-verification <string>	The header verification used for JWT key.	No default.
payload-validation <string>	The payload verification used for JWT key.	No default.
rsa-key	The RSA key used for Dynamic key or JWT key.	No default.
create-time <create-time_str>	Specify the API user creation time.	No default.
<ip-access-list_id>	The index number of the IP entry.	No default.
<ip_str>	Specify the IP addresses from which the API key can only be used.	No default.
<http-referer-list_id>	The index number of the referer HTTP header entry.	No default.

Variable	Description	Default
http-referer <http-referer_str>	Specify the referer HTTP header in which the specified URLs are present.	No default.

Related topics

- [waf api-policy on page 431](#)
- [waf api-rules on page 432](#)
- [waf api-user-group on page 439](#)

waf api-user-group

Use this command to create API user group which defines specific permissions of the group users can perform.

Syntax

```
config waf api-user-group
  edit <api-user-group_name>
    config user-list
      edit <user-list_id>
        set api-user-name <api-user-name_str>
      next
    end
  next
end
```

Variable	Description	Default
<api-user-group_name>	Enter a name for the API user group.	No default.
<user-list_id>	The index number of the API user entry.	No default.
api-user-name <api-user-name_str>	Select the created API user name.	No default.

Related topics

- [waf api-policy on page 431](#)
- [waf api-rules on page 432](#)
- [waf api-users on page 437](#)

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 details, see [Permissions on page 46](#).

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>"
    set layer3-fragment-protection {enable | disable}
next
end
```

Variable	Description	Default
"<app-dos-policy_name>"	Enter the name of a new or existing rule. The maximum length is 63 characters. To display the list of existing rules, enter: 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>" on page 440 and HTTP-request-flood-prevention-rule "<rule_name>" on page 440 .	disable
HTTP-connection-flood-check-rule "<rule_name>"	Enter the name of an existing rule that sets the maximum number of HTTP requests per second to a specific URL. The maximum length is 63 characters. To display a list of the existing rules, enter: set HTTP-connection-flood-check-rule ? This setting applies only if enable-HTTP-session-based-prevention {enable disable} on page 440 is enabled.	No default.
HTTP-request-flood-prevention-rule "<rule_name>"	Enter the name of an existing rule that limits TCP connections from the same client. The maximum length is 63 characters. To display a list of the existing rules, enter: set HTTP-request-flood-prevention-rule ? This setting applies only if enable-HTTP-session-based-prevention {enable disable} on page 440 is enabled.	No default.

Variable	Description	Default
enable-layer4-dos-prevention {enable disable}	Enable to use DoS protection that is not based on session cookies. Also configure layer4-access-limit-rule "<rule_name>" on page 441 and layer4-connection-flood-check-rule "<rule_name>" on page 441 .	disable
layer4-access-limit-rule "<rule_name>"	Enter the name of a rule that limits the number of HTTP requests per second from any source IP address. The maximum length is 63 characters. To display a list of the existing rules, enter: set layer4-access-limit-rule ? This setting applies only if enable-layer4-dos-prevention {enable disable} on page 441 is enabled.	No default.
layer4-connection-flood-check-rule "<rule_name>"	Enter the name of an existing rule that limits the number of TCP connections from the same source IP address. The maximum length is 63 characters. To display a list of the existing rules, enter: set layer4-connection-flood-check-rule ? This setting applies only if enable-layer4-dos-prevention {enable disable} on page 441 is enabled.	No default.
layer3-fragment-protection {enable disable}	Enable to prevent attacks of fragmented packets.	disable

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

- [waf HTTP-connection-flood-check-rule on page 532](#)
- [waf HTTP-request-flood-prevention-rule on page 547](#)
- [waf layer4-access-limit-rule on page 582](#)
- [waf layer4-connection-flood-check-rule on page 586](#)
- [system advanced on page 233](#)

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 details, see [Permissions on page 46](#).

Syntax

```
config waf base-signature-disable
  edit "<signature-ID_name>"
  next
end
```

Variable	Description	Default
"<signature-ID_name>"	Enter the name of an individual signature or signature category ID. The maximum length is 63 characters. For example, to disable the first cross-site scripting attack signature everywhere it is currently selected, you would enter: 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

- [waf signature on page 612](#)

waf biometrics-based-detection

By checking the client events such as mouse movement, keyboard, screen touch, and scroll, etc in specified period, FortiWeb judges whether the request comes from a human or from a bot. You can use this command to configure the biometrics based detection rule to define the client event, collection period, and the request URL, etc.

Syntax

```

config waf biometrics-based-detection
  edit <biometrics-based-detection-name_str>
    set mouse-movement {enable | disable}
    set page-focus {enable | disable}
    set click {enable | disable}
    set screen-touch {enable | disable}
    set keyboard {enable | disable}
    set scroll {enable | disable}
    set bot-traits {enable | disable}
    set bot-traits-num <int>
    set event-collection-time <time_int>
    set bot-effective-time <time_int>
    set action {alert | alert_deny | | deny_no_log}
    set severity {high | medium | low | Info}
    set trigger <trigger_policy>
    set bot-access-rate <int>
  config url-list
    edit <url-list_id>
      set host <host_str>
      set host-status {enable | disable}
      set type {simple-string | regex-expression}
      set url <url_str>
    next
  end
next
end

```

Variable	Description	Default
<biometrics-based-detection-name_str>	Type a unique name that can be referenced in other parts of the configuration.	No default.
mouse-movement {enable disable}	Enable to monitor the mouse movement event.	enable
page-focus {enable disable}	Enable to monitor how long the user stays on the page.	disable
keyboard {enable disable}	Enable to monitor the keyboard event.	enable
click {enable disable}	Enable to monitor the click event.	enable
screen-touch {enable disable}	Enable to monitor the screen touch event.	disable
scroll {enable disable}	Enable to monitor the scroll event.	disable
bot-traits {enable disable}	For the requests passing the Monitor Client Events check, you can enable <code>bot-traits</code> to implement an additional layer of detection to check whether the requests are generated by bots.	disable

Variable	Description	Default
	<code>bot-traits</code> looks at the properties of the client's browser for values commonly used by bots. By examining these characteristics, it becomes possible to effectively identify and filter out malicious events that are artificially simulated by scripts. This is particularly useful in detecting web crawlers that leverage headless browsing techniques to simulate browser behaviors in order to bypass conventional bot detection methods.	
<code>bot-traits-num <int></code>	Specify how many bot traits should be detected to identify a client as a bot. The valid range is 2-10.	5
<code>event-collection-time <time_int></code>	Specify how long the events will be collected from the client.	15
<code>bot-effective-time <time_int></code>	For the identified bot, choose the time period before FortiWeb tests and verifies the bot again.	5
<code>action {alert alert_deny deny_no_log}</code>	Select which action FortiWeb will take when it detects a violation of the policy: • Alert—Accept the connection and generate an alert email and/or log message. • Alert & Deny—Block the request (or reset the connection) and generate an alert and/or log message. • Deny (no log)—Block the request (or reset the connection). The default value is Alert.	Alert
<code>severity {high medium low Info}</code>	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs a violation of the policy: • Informative • Low • Medium • High	Low

Variable	Description	Default
trigger <trigger_policy>	Select the trigger, if any, that FortiWeb will use when it logs and/or sends an alert email about a violation of the policy. For details, see "Viewing log messages" on page 1.	No default.
bot-access-rate <int>	Specify the bot-access-rate to define the maximum bot JS requests per second per IP. The detection threshold is calculated using the formula: $\text{bot-access-rate} \times (\text{report\_waiting\_time} + \text{event\_collection\_time})$ Clients exceeding this value are identified as bots. The valid range is 1 to 100, with a default of 5.	5
<url-list_id>	Enter the sequence number of the URL.	No default.
host <host_str>	Select the name of a protected host that the <code>Host: field</code> of an HTTP request must be in to match the bot deception policy. This option is available only if waf biometrics-based-detection on page 442 is enabled.	No default.
host-status {enable disable}	Enable to apply this rule only to HTTP requests for specific web hosts. Also configure host <host_str> .	disable
type {simple-string regex-expression}	Select whether the url <url_str> field must contain either: simple-string—The field is a string that the request URL must exactly. regex-expression—The field is a regular expression that defines a set of matching URLs.	simple-string
url <url_str>	Depending on your selection in type {simple-string regex-expression} , enter either: The literal URL, such as <code>/index.php</code>, that the HTTP request must contain in order to match the input rule. The URL must begin with a backslash (<code>/</code>).	No default.

Variable	Description	Default
	A regular expression, such as <code>^/*\.php</code>, matching all and only the URLs to which the input rule should apply. The pattern does not require a slash (<code>/</code>); however, it must at least match URLs that begin with a slash, such as <code>/index.cfm</code>. When you have finished typing the regular expression, click the <code>>></code> (test) icon. This opens the Regular Expression Validator window where you can finetune the expression. For details, see Appendix D: Regular expressions.	

Related topics

[waf bot-mitigation-policy on page 459](#)

waf bot-detection-policy

Use this command to edit bot detection policies.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf bot-detection-policy
edit <bot-detection-policy_ID>
    set policy-id <server-policy-id>
    set model-status {enable | disable}
    set advanced-mode {enable | disable}
    set client-identification-method {IP | IP-and-User-Agent | Cookie}
    set sampling-count <integer>
    set sampling-count-per-client <integer>
    set sampling-time-per-vector <integer>
    set training-accuracy <percentage>
    set cross-validation <percentage>
    set testing-accuracy <percentage>
    set selected-model {Strict | Loose}
    set anomaly-count <integer>
    set bot-confirmation {enable | disable}
```

```

set verification-method {Disable | Real-Browser-Enforcement | Captcha-Enforcement
    | reCaptcha-Enforcement}
set recaptcha <recaptcha_server_name>
set validation-timeout <integer>
set max-attempt-times <integer>
set mobile-verification-method {Disable | Mobile-Token-Validation} on page 452
set auto-refresh {enable | disable}
set refresh-factor <value-from-0-to-one>
set minimum-vector-number <integer>
set action {alert | deny_no_log | alert_deny | block-period}
set block-period <integer>
set severity {High | Medium | Low | Info}
set trigger <trigger_policy_name>
config allow-source-ip
    edit <allow-source-ip-list-id>
        set ip <ip-address>
    next
end
config bot-detection-exception-list
    edit <bot-detection-exception-list-id>
        set host <string>
        set host-status {enable | disable}
        set url-type {plain | regular}
        set url-pattern <string>
    next
end
next
end

```

Variable	Description	Default
policy-id <server-policy-id>	Associate this bot detection policy with the specified server policy.	No default
model-status {enable disable}	Enable or disable bot detection.	enable
advanced-mode {enable disable}	Enable or disable the advanced settings in the bot detection policy	disable
client-identification-method {IP IP-and-User-Agent Cookie}	The data collected in one sample should be from the same user. The system uses IP, IP and User-Agent, or Cookie to identify a user. IP: The traffic data in one sample should come from the same source IP. IP and User-Agent: The traffic data in one sample should come from the same source IP and User-Agent (the browser). Cookie: The traffic data in one sample should have the same cookie value.	IP-and-User-Agent
sampling-count <integer>	This controls how many samples should be collected during the sample collection period.	1000

Variable	Description	Default
	More samples mean the model will be more accurate; but at the same time, it costs longer time to complete the sample collection. Not all traffic data will be collected as samples. The system abandons traffic data if it meets one of the following criteria: • The system sends Javascript challenge to user clients before collecting samples from them. If a client doesn't pass the challenge, the system will not collect sample data from it. • The traffic is from malicious IPs reported by the IP Intelligence feature, or is recognized as a bot by the system. • The traffic is from Known Engines, such as Google and Bing. The system also skips the known engine traffic when executing bot detection. Using these criteria is to exclude malicious traffic and the traffic from known engines that act like a bot, thus to make sure the bot detection model is built upon valid data collected from regular users.	
<code>sampling-count-per-client <integer></code>	This controls how many samples FortiWeb will collect from each client (user) in an hour. For example, if the value is set to 3, and a client generates 10 samples in an hour, the system only collects the first 3 samples from this client in an hour. If the client generates more samples in the second hour, the system continues collecting samples from this client until the sample count reaches 3. This option prevents the system from continuously collecting samples from one client, thus to avoid the interference of the bot traffic in the sampling stage.	3
<code>sampling-time-per-vector <integer></code>	Each vector (also called sample) records a certain user's behaviors in a certain time range. This option defines how long the time range is. For example, if the Sample Time Per Vector is 5 minutes, the system will record a certain user's behaviors in 5 minutes and count it as one sample.	5

Variable	Description	Default
training-accuracy <userdef>	The training accuracy is calculated by this formula: The number of the regular samples in the training sample set/the total number of training samples * 100%. As we have introduced in the Basic Concepts section, multiple models are built based on multiple parameter combinations in the SVM algorithm. The system uses each model to detect anomalies in the sample set, and calculates the training accuracy for each model. For example, if there are 100 training samples, and 90 of them are treated as regular samples by a model, then the training accuracy for this model is 90%. The default value for the training accuracy is 95%, which means only the models whose training accuracy equals to or higher than 95% will be selected as qualified models.	95%
cross-validation <userdef>	The system divides the training sample sets evenly into three parts, let's say, Part A, B and C. The system executes three rounds of bot detection: • First, the system observes the samples in Part A and B to build up a mathematical model, then uses this model to detect anomalies in Part C. • Then, the system observes the samples in Part B and C to build up a mathematical model, then uses this model to detect anomalies in Part A. • At last, the system observes the samples in Part A and C to build up a mathematical model, then uses this model to detect anomalies in Part B. The cross-validation value is calculated by this formula: The total number of the regular samples/the total number of samples * 100%. For example, if there are 100 samples, and 10 anomalies are detected in the three rounds, then the cross-validation value for this model is: $(100-10)/100 * 100\% = 90\%$.	90%

Variable	Description	Default
	The default value for the training accuracy is 90%, which means only the models whose Cross-Validation Value equals to or higher than 90% will be selected as qualified models.	
testing-accuracy <userdef>	Three quarters of the samples are divided into training sample set, and one quarter of the samples are divided into testing sample set. The system uses the models built for the training sample set to detect anomalies in the testing sample set. If the training accuracy and testing accuracy for a model vary greatly, it may indicate the model is not invalid. The testing accuracy is calculated by this formula: The number of the regular samples in the testing sample set/the number of the testing samples * 100%. For example, if there are 100 testing samples, and 95 of them are treated as regular samples by a model, then the testing accuracy for this model is 95%. The default value for the training accuracy is 95%, which means only the models whose testing accuracy equals to or higher than 95% will be selected as qualified models.	95%
selected-model {Strict Loose}	Multiple models are built during the model building stage. The system uses training accuracy, cross-validation value, and testing accuracy to select qualified models. The Model Type is used to select the one final model out of all the qualified models. - If you configure the Model Type to Loose, the system chooses the model which has the highest training accuracy among all the qualified models. - If you configure the Model Type to Strict, the system chooses the model which has the lowest training accuracy among all the qualified models. The Strict Model detects more anomalies, but there are chances that regular users are false positively detected as bots.	loose

Variable	Description	Default
	The Moderate Model is comparatively loose. It's less likely to conduct false positive detection, but there are risks that real bots might be escaped from detection. There isn't a perfect option for every situation. Whichever model type you choose, you can always leverage the other commands to mitigate the side effects, for example, using <code>bot-confirmation enable</code> to avoid false positive detections.	
<code>anomaly-count</code> <code><integer></code>	If the system detects certain times of anomalies from a user, it takes actions such as sending alerting emails or blocking the traffic from this user. Anomaly Count controls how many times of anomalies are allowed for each user. For example, the Anomaly Count is set to 4, and the system has detected 3 anomalies in the last 6 vectors. If the 7th vector is detected again as an anomaly, the system will take actions. Please note that if no valid traffic is collected for the 7th vector (for example, the user leaves your application), the system will clear the anomaly count and the user information. If the user revisits your application, he/she will be treated as new users and the system starts anomaly counting afresh. Since this option allows certain times of anomalies from a user, it might be a good choice if you want to avoid false positive detections.	3
<code>bot-confirmation</code> <code>{enable </code> <code>disable}</code>	If the number of anomalies from a user has reached the Anomaly Count, the system executes Bot Confirmation before taking actions. The Bot Confirmation is to confirm if the user is indeed a bot. The system sends RBE (Real Browser Enforcement) JavaScript or CAPTCHA to the client to double check if it's a real bot.	enable

Variable	Description	Default
<pre>verification-method {Disable Real- Browser- Enforcement Captcha- Enforcement reCaptcha- Enforcement}</pre>	Disable: Do not execute browser verification. Real Browser Enforcement: The system sends a JavaScript to the client to verify whether it is a web browser. CAPTCHA Enforcement: The system requires clients to successfully fulfill a CAPTCHA request. CAPTCHA verification will not pop out for the bot confirmation again for the same user within 10 mins timeout. reCAPTCHA Enforcement: The system requires the client to successfully fulfill a reCAPTCHA request. It will trigger the action policy if the traffic is not from web browser.	Real-Browser-Enforcement
<pre>recaptcha <recaptcha_ server_name></pre>	Enter the reCAPTCHA server you have created through user recaptcha-user	No default.
<pre>validation-timeout <integer></pre>	Enter the maximum amount of time (in seconds) that FortiWeb waits for results from the client for Bot Confirmation. The default value is 20. The valid range is 5–30.	20
<pre>max-attempt-times <integer></pre>	The maximum number of the CAPTCHA enforcement validation attempts. If the client fails the validation for the specified time, the system will trigger the action policy. This is only available if the verification-method is set to CAPTCHA-Enforcement	3
<pre>mobile-verification- method {Disable Mobile-Token- Validation}</pre>	Disable: Disable the system to verify whether the sample traffic is from mobile devices. Mobile-Token-Validation: The system verifies the mobile token to confirm if the traffic is from mobile devices.	disable
<pre>auto-refresh {enable disable}</pre>	If this is enabled, FortiWeb detects if the current model is applicable. If not, FortiWeb will refresh the current model automatically.	enable
<pre>refresh-factor <userdef></pre>	Auto Refresh Factor controls the timing to trigger the model refreshment when a certain number of false positive vectors are detected.	0.7

Variable	Description	Default																								
	FortiWeb makes statistics for the bot detection in the past 24 hours. It counts the number of the following vectors: • All vectors in the past 24 hours (A), • Anomaly vectors (B), and • The anomaly vectors that are confirmed as bots (C) If $(B - C)/(A - C) > 1 - \text{Auto Refresh Factor} * \text{training accuracy}$, the model will be refreshed. • $(B - C)$ is the false positive vectors, and $(A - C)$ is the regular vectors. $(B - C)/(A - C)$ represents the false positive rate. • $(1 - \text{Auto Refresh Factor} * \text{training accuracy})$ is an adjusted anomaly vector rate. You can consider it as an auto refresh threshold. If the false positive rate $(B - C)/(A - C)$ becomes greater than the auto refresh threshold $(1 - \text{Auto Refresh Factor} * \text{training accuracy})$, the system determines the current model is not applicable and automatically refreshes the model. The following table calculates the value of the auto refresh threshold when the Auto Refresh Factor is set to 0-1 (assuming the training accuracy is the default value 95%). For example, if the Auto Refresh Factor is set to 0.8, the auto refresh threshold will be $1 - 0.8 * 95\% = 0.24$, which means the system automatically refreshes the model when the false positive rate is greater than 0.24 (e.g. 24 false positive vectors and 100 regular vectors). You can use this table to quickly decide a value for the Auto Refresh Factor that is suitable for your situation.																									
	<table><tr><th>Auto Refresh Factor</th><th>Auto Refresh Threshold 1 - Auto Refresh Factor * training accuracy *Assuming the training accuracy is the default value 95%.</th></tr><tr><td>0</td><td>1</td></tr><tr><td>0.1</td><td>0.905</td></tr><tr><td>0.2</td><td>0.81</td></tr><tr><td>0.3</td><td>0.715</td></tr><tr><td>0.4</td><td>0.62</td></tr><tr><td>0.5</td><td>0.525</td></tr><tr><td>0.6</td><td>0.43</td></tr><tr><td>0.7</td><td>0.335</td></tr><tr><td>0.8</td><td>0.24</td></tr><tr><td>0.9</td><td>0.145</td></tr><tr><td>1</td><td>0.05</td></tr></table>	Auto Refresh Factor	Auto Refresh Threshold 1 - Auto Refresh Factor * training accuracy *Assuming the training accuracy is the default value 95%.	0	1	0.1	0.905	0.2	0.81	0.3	0.715	0.4	0.62	0.5	0.525	0.6	0.43	0.7	0.335	0.8	0.24	0.9	0.145	1	0.05	
Auto Refresh Factor	Auto Refresh Threshold 1 - Auto Refresh Factor * training accuracy *Assuming the training accuracy is the default value 95%.																									
0	1																									
0.1	0.905																									
0.2	0.81																									
0.3	0.715																									
0.4	0.62																									
0.5	0.525																									
0.6	0.43																									
0.7	0.335																									
0.8	0.24																									
0.9	0.145																									
1	0.05																									

Variable	Description	Default
<code>minimum-vector-number</code> <code><integer></code>	As we mentioned above, the system decides whether to update the bot detection model based on the statistics in the past 24 hours. If very few vectors are detected in the past 24 hours, it may interfere the rightness of the model refreshment decision. Set a value for the Minimum Vector Number, so that the system won't update the model if the number of the vectors hasn't reached this value. If the value is set to 0, the system will use the value of the Sample Count as the Minimum Vector Number.	0
<code>action {alert deny_</code> <code>no_log alert_</code> <code>deny block-</code> <code>period}</code>	The action FortiWeb takes when a user client is confirmed as a bot: • alert—Accepts the connection and generates an alert email and/or log message. • deny_no_log—Blocks the request. No logs will be generated. • alert_deny—Blocks the request (or resets the connection) and generates an alert and/or log message. • block-period—Blocks the request for a certain period of time.	alert
<code>block-period <integer></code>	Enter the number of seconds that you want to block the requests. The valid range is 1–3,600 seconds. This option only takes effect when you choose Period Block in Action.	600
<code>severity {High </code> <code>Medium Low </code> <code>Info}</code>	Select the severity level for this anomaly type. The severity level will be displayed in the alert email and/or log message.	High
<code>trigger <trigger-</code> <code>policy-name></code>	Select a trigger policy. If an anomaly is detected, it will trigger the system to send email and/or log messages according to the trigger policy.	No default
<code><ip-address></code>	If specified, the system will collect sample data only from the these IP addresses.	No default
<code>host <string></code>	The system collects samples from any IP address except the specified IP address or FQDN of a protected host.	No default

Variable	Description	Default
<code>host-status {enable disable}</code>	Enable or disable comparing the URLs to the <code>Host :</code> field in the HTTP header.	enable
<code>url-type {plain regular}</code>	Specify whether the Exception URLs must contain either: plain—The field is a string that the Exception URL must match exactly. regular—The field is a regular expression that defines a set of matching URLs.	No default
<code>url-pattern <string></code>	Depending on the <code>url-type</code> , enter either: plain—The literal URL, such as <code>/index.php</code>, that the HTTP request must contain in order to match the rule. The URL must begin with a slash (<code>/</code>). regular—A regular expression, such as <code>^/*\.php</code>, matching the URLs to which the rule should apply. The pattern does not require a slash (<code>/</code>), but it must match URLs that begin with a slash, such as <code>/index.cfm</code>. Do not include the domain name, such as <code>www.example.com</code> , which is configured separately in <code>[bot-detection-exception-list] <No.> host <string></code> .	No default

waf bot-mitigation-exception

You can use this command to create exception policy to omit bot mitigation attack scans when you know that some parameters or URLs may trigger positives during normal use. The exception policy can be applied in Bot Mitigation policy, Biometrics Based Detection, Threshold Based Detection, and Bot Deception.

Syntax

```
config waf bot-mitigate-exception
edit edit "<bot_excetpion_policy-name>"
config exception-element-list
edit <index>
    set match-target CLIENT_IP
    set operator {EQ |NE}
    set ip-range <IP_range>
    set concatenate-type {AND | OR}
next
edit <index>
    set match-target host
```

```

        set operator {STRING_MATCH | REGEXP_MATCH}
        set value <string>
        set concatenate-type {AND | OR}
    next
    edit <index>
        set match-target URI
        set operator {STRING_MATCH | REGEXP_MATCH}
        set value <string>
        set concatenate-type {AND | OR}
    next
    edit <index>
        set match-target FULL_URL
        set operator {STRING_MATCH | REGEXP_MATCH}
        set value <string>
        set concatenate-type {AND | OR}
    next
    edit <index>
        set match-target PARAMETER
        set operator {STRING_MATCH | REGEXP_MATCH}
        set value-name <string>
        set value-check {enable | disable}
        set value <string>
        set concatenate-type {AND | OR}
    next
    edit <index>
        set match-target COOKIE
        set operator {STRING_MATCH | REGEXP_MATCH}
        set value-name <string>
        set value-check {enable | disable}
        set value <string>
        set concatenate-type {AND | OR}
    next
end
next
end

```

Variable	Description	Default
<bot_excetpion_policy-name>	Enter the name of the bot mitigation exception policy.	No default
<index>	Enter the index number of the exception element.	No default
match-target CLIENT_IP		
operator {EQ NE}	- EQ—Equal. FortiWeb does not perform a bot mitigation attack scan for requests with a client IP address or IP range that matches the value of ip-range. - NE—Not Equal. FortiWeb only performs a bot mitigation attack scan for requests with a client IP address or IP range that matches the value of ip-range.	EQ
CLIENT_IP <ip>	Specify the client IP addres that FortiWeb uses to determine whether or not to perform a bot mitigation attack	No default

Variable	Description	Default
	scan for the request.	
ip-range <IP_range>	Specify the client IP address or IP range that FortiWeb uses to determine whether or not to perform a bot mitigation attack scan for the request.	No default
match-target host		
operator {STRING_MATCH REGEXP_MATCH}	- STRING_MATCH—Value is a literal host name. - REGEXP_MATCH—Value is a regular expression that matches all and only the host name that the exception applies to.	REGEXP_MATCH
value <string>	Specifies the Host : field value to match.	No default
match-target URI		
operator {STRING_MATCH REGEXP_MATCH}	- STRING_MATCH—Value is a literal URL, such as <code>/folder1/index.htm</code> that the HTTP request must contain in order to match the rule, or use wildcards to match multiple URLs, such as <code>/folder1/*</code> or <code>/folder1/*/index.htm</code>. - REGEXP_MATCH—Value is a regular expression that matches all and only the URIs that the exception applies to.	REGEXP_MATCH
value <string>	Specifies a URL value to match. You can use up to 2048 characters in regex configuration for signature. The value does not include parameters. For example, <code>/testpage.php</code>, which match requests for <code>http://www.test.com/testpage.php?a=1&b=2</code>. If operator is STRING_MATCH, ensure the value starts with a forward slash (<code>/</code>) (for example, <code>/causes-false-positives.php</code>). If operator is REGEXP_MATCH, the value does not require a forward slash (<code>/</code>). However, ensure that it can match values that contain a forward slash. Do not include a domain name or parameters. To match a domain name, use the Host element type. To match a URL that includes parameters, use the Full URL type.	No default
match-target FULL_URL		
operator {STRING_MATCH REGEXP_MATCH}	STRING_MATCH—Value is a literal URL, such as <code>/folder1/index.htm</code> that the HTTP request must contain in order to match the rule, or use wildcards to match multiple URLs, such as <code>/folder1/*</code> or <code>/folder1/*/index.htm</code>.	REGEXP_MATCH

Variable	Description	Default
	REGEXP_MATCH—Value is a regular expression that matches all and only the URLs that the exception applies to.	
value <string>	Specifies a URL value that includes parameters to match. For example, /testpage.php?a=1&b=2, which match requests for http://www.test.com/testpage.php?a=1&b=2. If operator is STRING_MATCH, ensure the value starts with a forward slash (/) (for example, /testpage.php?a=1&b=2). If operator is REGEXP_MATCH, the value does not require a forward slash (/). However, ensure that it can match values that contain a forward slash. Do not include a domain name. To match a domain name, use the Host element type. To match a URL that does not include parameters, use the URI type.	No default
match-target PARAMETER		
operator {STRING_MATCH REGEXP_MATCH}	STRING_MATCH—Name is the literal name of a parameter. REGEXP_MATCH—Name is a regular expression that matches all and only the name of the parameter that the exception applies to.	REGEXP_MATCH
value-name <string>	Specifies the name of the parameter to match.	No default
value-check {enable disable}	Enable to specify a parameter value to match in addition to the parameter name.	disable
value <string>	Specifies the parameter value to match.	No default
match-target COOKIE		
operator {STRING_MATCH REGEXP_MATCH}	STRING_MATCH—Name is the literal name of a cookie. REGEXP_MATCH—Name is a regular expression that matches all and only the name of the cookie that the exception applies to.	REGEXP_MATCH
value-name <string>	Specifies the name of the cookie to match.	No default
value-check {enable disable}	Select to specify a cookie value to match in addition to the cookie name.	disable
value <string>	Specifies the cookie value to match.	No default

Variable	Description	Default
concatenate-type {and or}	- And—A matching request matches this entry in addition to other entries in the exemption list. - Or—A matching request matches this entry instead of other entries in the exemption list. Later, you can use the exception list options to adjust the matching sequence for entries. The lower the index number, the earlier it will be processed.	and

Related topics

- [waf bot-deception on page 1](#)
- [waf biometrics-based-detection on page 442](#)
- [waf threshold-based-detection on page 658](#)
- [waf known-bots on page 571](#)

waf bot-mitigation-policy

You can use this command to integrate the bot deception policy, the biometrics based detection rule, and threshold based detection rule, and apply the policy in the web protection profile for bot mitigation.

Syntax

```
config waf bot-mitigate-policy
  edit bot-deception <bot-deception_str>
    set bot-deception <bot-deception_str>
    set biometrics-based-detection <biometrics-based-detection_str>
    set threshold-based-detection <threshold-based-detection_str>
    set known-bots <known-bots_str>
  next
end
```

Variable	Description	Default
"<bot-mitigate-policy_ name>"	Enter a name for the bot mitigation policy.	No default
bot-deception <bot- deception_str>	Select a bot deception policy from the created policy list.	No default
biometrics-based-detection <biometrics-based- detection_str>	Select a biometrics based detection rule from the created rule list.	No default
threshold-based-detection	Select a threshold based detection rule from the created rule	No default

Variable	Description	Default
<threshold-based-detection_str>	list.	
known-bots <known-bots_str>	Select a known bots rule from the created rule list.	No default

Related topics

- [waf bot-deception on page 1](#)
- [waf biometrics-based-detection on page 442](#)
- [waf threshold-based-detection on page 658](#)
- [waf known-bots on page 571](#)

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 details, see [Permissions on page 46](#).

Syntax

```
config waf cookie-security
  edit "<cookie-security_name>"
    set security-mode {no | encrypted | signed}
    set action {alert | alert_deny | block-period | remove_cookie | deny_no_log}
    set block-period <block-period_int>
    set severity {High | Medium | Low | Info}
    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
    end
  next
end
```

Variable	Description	Default
"<cookie-security_name>"	Enter the cookie security policy name. The maximum length is 63 characters.	No default.
security-mode {no encrypted signed}	Enter the 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 and the client to support cookies. For details, see waf web-protection-profile inline-protection on page 696. 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 according to action {alert alert_deny block-period remove_cookie deny_no_log} on page 461.	no
action {alert alert_deny block-period remove_ cookie deny_no_log}	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. • block-period—Block subsequent requests from the client for a number of seconds. Also configure block-period <block-period_int> on page 462. 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. For details, see waf x-forwarded-for on page 721. Failure to do so may cause FortiWeb to block all connections when it detects a violation of this type.	alert

Variable	Description	Default
	<code>remove_cookie</code>—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. <code>deny_no_log</code>—Deny a request. Do not generate a log message. Caution: This setting will be ignored if monitor-mode {enable disable} on page 163 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 <code>alert_deny</code>, 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 details about auto-learning requirements, see "waf web-protection-profile autolearning-profile" on page 1.	
<code>block-period <block-period_int></code>	Enter the number of seconds to block a connection when action {alert alert_deny block-period remove_cookie deny_no_log} on page 461 is set to <code>block-period</code> . The valid range is from 1 to 3,600 seconds.	600
<code>severity {High Medium Low Info}</code>	Select the severity level to use in logs and reports generated when cookie poisoning is detected.	High
<code>trigger "trigger-policy_name"></code>	Enter the name of the trigger to apply when cookie poisoning is detected. For details, see log trigger-policy on page 96. The maximum length is 63 characters. To display the list of existing trigger policies, type: <code>set trigger ?</code>	No default.
<code>cookie-replay-protection-type {no IP}</code>	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. Available only when security-mode {no encrypted signed} on page 461 is <code>encrypted</code> .	no
<code>max-age <max-age_int></code>	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

Variable	Description	Default
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
samesite { enable disable }	Enable to add the "SameSite" attribute so that you can declare that your cookie should be restricted to a first-party or same-site context.	disable
samesite-value {strict lax none}	strict: Any request from the third parties will not carry such cookies; lax: Any request from the third parties will not carry such cookies except for GET requests that navigate to the destination URL. none: Set the value as none if a cookie is required to be sent by cross origin.	lax
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 {no encrypted signed} on page 461 is encrypted, suspicious cookies are cookies for which FortiWeb does not have a corresponding encrypted cookie value. - When cookie-replay-protection-type {no IP} on page 462 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 "<time_str>" on page 463. This feature is not available if security-mode {no encrypted signed} on page 461 is signed.	Custom
allow-time "<time_str>"	Set the date on which FortiWeb starts to take the specified action against suspicious cookies if allow-	No default.

Variable	Description	Default
	suspicious-cookies{Never Always Custom} on page 463 is Custom.	
<entry_index>	Enter 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 192.0.2.50 .	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

- [waf web-protection-profile inline-protection on page 696](#)

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*:

<https://docs.fortinet.com/document/fortiweb>

To apply a CSRF protection rule, you select it in an inline protection profile. For details, see [waf web-protection-profile inline-protection on page 696](#).

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 [server-policy allow-hosts on page 106](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf csrf-protection
edit "<csrf-rule_name>"
```



```

set action {alert | alert_deny | block-period | deny_no_log}
set block-period <seconds_int>
set severity {High | Medium | Low | Info}
set trigger <trigger-policy_name>
set
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>"	Enter the name of a new or existing rule. The maximum length is 63 characters. To display the list of existing rules, enter: <pre>edit ?</pre>	No default.
action {alert alert_deny block-period deny_no_log}	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. • block-period—Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int> on page 466. • deny_no_log—Deny a request. Do not generate a	alert

Variable	Description	Default
	log message. Note: Logging and alert email occur only if the corresponding settings are enabled and configured. For details, see log disk on page 66 and log alertMail on page 60.	
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 1–3,600 seconds. This setting applies only if action {alert alert_deny block-period deny_no_log} on page 465 is <code>block-period</code>.	600
severity {High Medium Low Info}	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. For details, see log trigger-policy on page 96. The maximum length is 63 characters. To display the list of existing trigger policies, enter: <pre>set trigger ?</pre>	No default.
ajaxcheck {disable enable}	By default, FortiWeb runs a script to append the parameter <code>tknfv</code> (the anti-CSRF token) to any HTML link elements that have the <code>href</code> attribute (<code><a href></code>) and HTML form elements. Enabling this option will run another script to modify the page's native <code>XMLHttpRequest</code> function and add the CSRF parameter <code>tknfv</code> onto it. If the Ajaxcheck Status option in Advanced Protection > Man in the Browser Protection is also enabled, the AJAX requests will also contain the parameters for MiTB: <code>check_url</code>, <code>check_action</code>, and <code>local_url</code>.	disable
<entry_index>	Enter the index number of the individual entry in the table.	No default.
host <host_name>	Enter a protected host name (either a web host name or IP address) that the <code>Host :</code> field of the HTTP request matches. This setting applies only if host-status {enable disable} on page 466 is <code>enable</code>.	No default.
request-url <url_str>	Enter either a literal URL or regular expression, depending on the value of <code>request-type</code> .	No default.
host-status {enable disable}	Enter <code>enable</code> to apply this rule only to HTTP requests for specific web hosts. Also configure <code>host</code>. Disable to match the rule based on the URL and any parameter filter only.	disable

Variable	Description	Default
request-type {plain regular}	Select whether request-url <url_str> on page 466 contains a literal URL (<code>plain</code>), or a regular expression designed to match multiple URLs (<code>regular</code>).	plain
parameter-filter {enable disable}	Enter <code>enable</code> 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 <parameter-value_str> on page 467 contains a literal value (<code>plain</code>) or a regular expression designed to match multiple parameters (<code>regular</code>).	plain
parameter-value <parameter-value_str>	Enter either a literal parameter or regular expression, depending on the value of parameter-value-type {plain regular} on page 467 . To match any parameter value, for <code>parameter-value-type</code> , enter <code>regular</code> , and for <code>parameter-value</code> , enter <code>*</code> (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 [waf web-protection-profile inline-protection on page 696](#) or [waf web-protection-profile offline-protection on page 706](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```

config waf custom-access policy
    edit "<custom-policy_name>"
        config rule
            edit <entry_index>
                set rule-name "<custom-rule_name>"
                set threat-weight {low | critical | informational | moderate | substantial |
                                severe}
            next
        end
    next
end

```

Variable	Description	Default
"<custom-policy_name>"	Enter the name of a new or existing custom policy. The maximum length is 63 characters. To display a list of the existing policies, enter: <code>edit ?</code>	No default.
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,223,372,036,854,775,807.	No default.
rule-name "<custom-rule_name>"	Enter the name of the existing custom access rule to add to the policy. The maximum length is 63 characters.	No default.
threat-weight {low critical informational moderate substantial severe}	Set the weight for the threat per a custom policy	moderate

Example

For an example, see [waf custom-access rule on page 469](#).

Related topics

- [waf web-protection-profile inline-protection on page 696](#)
- [waf web-protection-profile offline-protection on page 706](#)
- [waf custom-access rule on page 469](#)

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
- HTTP Session
- Rate limit (including rate limiting for specific types of content)
- HTTP header or response code
- URL
- Predefined or custom attack or data leak signature violation
- Transaction or packet interval timeout
- Real browser enforcement
- CAPTCHA enforcement

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 [waf custom-access policy on page 468](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf custom-access rule
edit "<custom-access_name>"
    set action {alert | alert_deny | block-period | deny_no_log | redirect}
    set block-period <seconds_int>
    set severity {High | Medium | Low | Info}
    set trigger "<trigger-policy_name>"
```

```
set bot-recognition {captcha-enforcement | recaptcha-enforcement | real-browser-
    enforcement | disable}
set recaptcha <recaptcha_server_name>
set max-attempt-times <attempts_int>
set validation-timeout <seconds_int>
set mobile-app-identification {disabled | mobile-token-validation}
set bot-confirmation {enable | disable}
config access-limit-filter
    edit <entry_index>
        set access-rate-limit <rate_int>
    next
end
config HTTP-header-filter
    edit <entry_index>
        set header-name-type {custom | predefined}
        set header-field-check {enable | disable}
        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-name-type {plain | regular}
        set cus-header-rev-match {enable | disable}
        set header-value "<value_str>"
        set HTTP-hline-missing-check {enable | disable}
        set HTTP-hline-empty-check {enable | disable}
        set basic-scheme-check {enable | disable}
        set HTTP-method-check {enable | disable}
        set HTTP-method-value-type {plain | regular}
        set HTTP-method-value "<HTTP-method-value_str>"
        set HTTP-method-rev-match {enable | disable} on page 477
    next
end
config method
    edit <entry_index>
        set method-type {predefined|custom}
        set predefined-method-set {GET POST HEAD OPTIONS TRACE CONNECT DELETE PUT
            PATCH WEBDAV RPC OTHERS}
        set custom-method-type {plain | regular}
        set custom-method-value <string>
        set method-reverse-match {enable|disable}
    next
end
config source-ip-filter
    edit <entry_index>
        set source-ip <ip_range>
        set exclusive-match {no | yes}
    next
end
config user-filter
    edit <entry_index>
        set reverse-match {no | yes}
        set user-name "<user-name_str>"
    next
end
config geo-filter
```

```
edit <entry_index>
    set match-exclusive {yes | no}
    set country-list <country-list_str>
next
end
config url-filter
edit <entry_index>
    set request-file "<url_str>"
    set reverse-match {no | yes}
next
end
config HTTP-transaction
edit <entry_index>
    set HTTP-transaction-timeout "<timeout_int>"
next
end
config response-code
edit <entry_index>
    set <response-code_int>
    set response-code-max <response-code_int>
    set response-code-rev-match {enable | disable}
next
end
config content-type
edit <entry_index>
    set {text/html text/plain text/xml application/xml application/soap+xml
        application/json application/octet-stream text/javascript text/}
    set content-type-rev-match {enable | disable}
next
end
config packet-interval
edit <entry_index>
    set packet-interval-timeout <timeout_int>
next
end
config parameter
edit <entry_index>
    set name-type {plain | regular}
    set name <parameter_name>
    set value-check {enable | disable}
    set value <value_regular_expression>
    set location-check {enable | disable}
    set location {URL | HTTP-body}
    set parameter-rev-match {enable | disable}
next
end
config signature-class
edit {010000000 | 020000000 | 030000000 | 040000000 | 050000000 | 060000000 |
    090000000 | 100000000 | 110000000 | 120000000}
    set status {enable | disable}
next
end
config custom-signature
edit <entry_index>
    set custom-signature-enable {enable | disable}
    set {custom-signature-group | custom-signature}
    set "<custom-signature-name_str>"
```

```

    next
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 | Http-Session}
    next
end
next
end

```

Variable	Description	Default
"<custom-access_name>"	Enter the name of a new or existing custom access rule. The maximum length is 63 characters. To display a list of the existing rule, enter: edit ?	No default.
action {alert alert_deny block-period deny_no_log redirect}	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 <code>type {request response}</code> on page 487 is response, it 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 <code>type</code> is <code>signature-creation</code>. You can customize the web page that FortiWeb returns to the client with the HTTP status code. • block-period—Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int> on page 473. • deny_no_log—Deny a request. Do not generate a log message. Note: If FortiWeb is deployed behind a NAT load balancer, when using this option, you must also define an X-header that indicates the original client's IP.	alert

Variable	Description	Default
	Failure to do so may cause FortiWeb to block all connections when it detects a violation of this type. For details, see waf x-forwarded-for on page 721. <code>redirect</code>—Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message.	
<code>block-period <seconds_int></code>	Enter the length of time (in seconds) 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 1–3,600 seconds.	600
<code>severity {High Medium Low Info}</code>	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	High
<code>trigger "<trigger-policy_name>"</code>	Enter the name of the trigger to apply when this policy is violated. For details, see log trigger-policy on page 96. The maximum length is 63 characters. To display the list of existing trigger policies, enter: <pre>set trigger ?</pre>	No default.
<code>bot-recognition {captcha-enforcement recaptcha-enforcement real-browser-enforcement disable}</code>	Select between: <code>captcha-enforcement</code>—Requires the client to successfully fulfill a CAPTCHA request. If the client cannot successfully fulfill the request within the <code>max-attempt-times <attempts_int></code> on page 474, or doesn't fulfill the request within the <code>validation-timeout <seconds_int></code> on page 474, FortiWeb applies the <code>action</code> and sends the CAPTCHA block page. <code>recaptcha-enforcement</code>—Requires the client to successfully fulfill a reCAPTCHA request. If the client cannot successfully fulfill the request within the <code>validation-timeout <seconds_int></code> on page 474, FortiWeb applies the <code>action</code> and sends the CAPTCHA	disable

Variable	Description	Default
	block page. CAPTCHA verification will not pop out for the bot confirmation again for the same user within 10 mins timeout. <code>real-browser-enforcement</code>—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 <code>validation-timeout <seconds_int></code>, FortiWeb applies the specified action. If the client appears to be a web browser, FortiWeb allows the client to violate the rule. <code>disable</code>—Disable this option to simply apply the access rule.	
<code>recaptcha <recaptcha_server_name></code>	Enter the reCAPTCHA server you have created through user recaptcha-user	No default.
<code>mobile-app-identification {disabled mobile-token-validation}</code>	For mobile clients that cannot execute JavaScript or CAPTCHA, FortiWeb can verify the request is legitimate by verifying the JWT-token a mobile application carries when it access a web server.	Disabled
<code>bot-confirmation {enable disable}</code>	Enable to confirm if the client is indeed a bot. The system sends RBE (Real Browser Enforcement) JavaScript or CAPTCHA to the client to double check if it's a bot.	disable
<code>max-attempt-times <attempts_int></code>	If <code>captcha-enforcement</code> is selected for <code>bot-recognition {captcha-enforcement recaptcha-enforcement real-browser-enforcement disable}</code> on page 473, enter the maximum number of attempts that a client may attempt to fulfill a CAPTCHA request. The valid range is 1–5. Available only when <code>captcha-enforcement</code> is selected for <code>bot-recognition</code>.	3
<code>validation-timeout <seconds_int></code>	Specifies the maximum amount of time that FortiWeb waits for results from the web browser test. The valid range is 5–30.	20
<code>config access-limit-filter</code>		
<code><entry_index></code>	Enter the index number of the individual entry	No default.

Variable	Description	Default
	in the table. The valid range is 1–9,999,999,999,999,999,999.	
access-rate-limit <rate_int>	Enter the rate threshold for source IP addresses. The valid range is 1–65535. To disable the rate limit, enter 0. Note: Blocking a shared source IP address could block innocent clients that share the same source IP address with an offending client.	1
config HTTP-header-filter		
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} on page 475 pre-header-type {plain regular} on page 475 pre-header-rev-match {enable disable} on page 476 pre-header-rev-match {enable disable} on page 476 pre-header-rev-match {enable disable} on page 476 pre-header-rev-match {enable disable} on page 476	predefined
header-field-check {enable disable}	Enable/disable checking the HTTP header field.	No 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 <code>Accept</code>: that must be present in order for the request to be allowed. This field appears only if header-name-type {custom predefined} on page 475 is predefined.	host
pre-header-type {plain regular}	Indicate whether header-value "<value_str>" on page 478 is a literal header value (<code>plain</code>) or a regular expression that indicates multiple possible valid header values (<code>regular</code>).	plain

Variable	Description	Default
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} on page 475 and header-value "<value_str>" on page 478 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>"	Enter 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. For example, if the specified name is <code>test</code>, then both <code>atest</code>, <code>test1</code>, <code>atest1</code> will be considered a match. This field appears only if header-name-type {custom predefined} on page 475 is <code>custom</code>.	No default.
cus-header-type {plain regular}	Indicate whether header-value "<value_str>" on page 478 is a literal header value (<code>plain</code>) or a regular expression that indicates multiple possible valid header values (<code>regular</code>).	plain
cus-header-name-type {plain regular}	Indicate whether custom-header-name "<key_str>" on page 476 is a literal header name (<code>plain</code>) or a regular expression that indicates multiple possible valid header names (<code>regular</code>).	plain
cus-header-rev-match {enable disable}	Indicate how to use custom-header-name "<key_str>" on page 476 and header-value "<value_str>" on page 478 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.	disable

Variable	Description	Default
	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.	
HTTP-hline-empty-check {enable disable}	If you enable Header Empty Value Check, the request matches the condition if it contains the specified header but the value of the matched header is empty. The <code>HTTP-hline-empty-check</code> checks whether a certain header has empty value.	disable
basic-scheme-check {enable disable}	Enable to check the Misformatted Basic Scheme. This field appears only when: • <code>header-name-type</code> is predefined. • <code>predefined-header</code> is <code>authorization</code> • <code>HTTP-hline-missing-check</code> is <code>disable</code> • <code>HTTP-hline-empty-check</code> is <code>disable</code>	disable
HTTP-method-check {enable disable}	Enable HTTP Method Check and configure a plain string or regular expression for the HTTP method that FortiWeb will search for in the header field.	disable
HTTP-method-value-type {plain regular}	Select a plain string or regular string.	No default.
HTTP-method-value "<HTTP-method-value_str>"	To prevent accidental matches, specify as much of the header's value as possible. Do not use an ambiguous substring.	No default.
HTTP-method-rev-match {enable disable}	When you enable HTTP Method Check, you can also enable HTTP Method Reverse Match so that the request matches the condition if the header does not contain the HTTP method's exact value or regular expression.	disable
HTTP-hline-missing-check {enable disable}	If you enable HTTP-hline-missing-check, the request matches the condition if it does not contain the specified header name.	disable

Variable	Description	Default
	The <code>HTTP-hline-missing-check</code> checks whether a certain header is missing. <code>HTTP-hline-empty-check</code> and <code>HTTP-hline-missing-check</code> can't be enabled at the same time. This setting does not take effect for HTTP2 packets without the following headers: • <code>:method</code> • <code>:scheme</code> • <code>:path</code> • <code>:authority</code> • <code>:status</code> HTTP2 packets without the above headers will not go far to be scanned against the <code>HTTP-hline-missing-check</code> setting. It will be considered as illegitimate and be abandoned directly when it arrives at FortiWeb at the first place.	
header-value "<value_str>"	Depending on your selection in pre-header-type {plain regular} on page 475, either: • Type the literal header value. Your specified HTTP header must contain in order to match the filter. Value matching is case sensitive. For example, if the specified name is <code>test</code>, then both <code>atest</code>, <code>test1</code>, <code>atest1</code> will be considered a match. 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 <code>192\.0\.2\.*</code>, matching all and only the header values which accepted HTTP header values must match. For details about language and regular expression matching, see the <i>FortiWeb Administration Guide</i>: https://docs.fortinet.com/document/fortiweb Tip: To prevent accidental matches, specify as much of the header's value as possible. Do not use an ambiguous substring.	No default.

Variable	Description	Default
	For example, entering the value <code>192.0.2.1</code> would also match the IPs <code>192.0.2.10-19</code> and <code>192.0.2.100-199</code>. This result may be unintended. The better solution would be to configure either: - A regular expression such as <code>^192.0.2.1\$</code> or - A source IP condition instead of an HTTP header condition	
<code>config method</code>		
<code>method-type</code> {predefined custom}	Configure the HTTP methods that FortiWeb will search for in the header field. Select whether to use the predefined method types or define custom types.	predefined
<code>predefined-method-set</code> {GET POST HEAD OPTIONS TRACE CONNECT DELETE PUT PATCH WEBDAV RPC OTHERS}	Select the methods that FortiWeb will search for in the header field. Please note that if you only select WEBDAV, then some of the methods included in WEBDAV (GET, HEAD, POST, DELETE, PUT) won't be scanned by the system; The WEBDAV related attack log won't have WEBDAV keyword in it, instead, it will be shown as the individual method violations.	No default.
<code>custom-method-type</code> {plain regular}	If you have defined <code>custom</code> for <code>method-type</code> , then select whether to use plain string or regular string.	plain
<code>custom-method-value</code> <string>	To prevent accidental matches, specify as much of the header's value as possible. Do not use an ambiguous substring.	No default.
<code>method-reverse-match</code> {enable disable}	Enable method-reverse-match so that the request matches the condition if the header does not contain the HTTP method's exact value or regular expression.	disable
<code>config source-ip-filter</code>		
<code>source-ip</code> <ip_range>	Enter the IP address or IP address range that specifies the clients that FortiWeb allows. For example: <code>1.2.3.4</code> <code>2001::1</code> <code>1.2.3.4-1.2.3.40</code>	No default.

Variable	Description	Default
	2001::1–2001::100 Depending on your configuration of how FortiWeb will derive the client's IP (see waf x-forwarded-for on page 721), this may be the IP address that is indicated in an HTTP header rather than the IP header.	
<code>exclusive-match {no yes}</code>	Set whether the condition can be met when source IP does not match.	No
<code>config user-filter</code>		
<code>user-name "<user-name_str>"</code>	Enter the user name to match.	No default.
<code>reverse-match {no yes}</code>	Indicate how to use <code>user-name "<user-name_str>"</code> on page 480 when determining whether or not this rule's condition has been met. <code>no</code>—If the regular expression does match the user name, the condition is met. <code>yes</code>—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
<code>config url-filter</code>		
<code>request-file "<url_str>"</code>	Enter a regular expression that defines either all matching or all non-matching URLs. Then, also configure <code>reverse-match {no yes}</code> on page 480. For example, for the URL access rule to match all URLs that begin with <code>/wordpress</code>, you could enter <code>^/wordpress</code>, then, in <code>reverse-match {yes no}</code>, select <code>no</code>. 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 <code>reverse-match {yes no}</code>.	No default.
<code>reverse-match {no yes}</code>	Indicate how to use <code>request-file "<url_str>"</code> on page 480 when determining whether or not this rule's condition has been met.	no

Variable	Description	Default
	<code>no</code>—If the regular expression does match the request URL, the condition is met. <code>yes</code>—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 (<code>!</code>).	
<code>config HTTP-transaction</code>		
HTTP-transation-timeout "<timeout_int>"	Enter a timeout value of 1–3600 seconds. If the lifetime of a HTTP transaction exceeds this value, the transaction matches this condition.	5
<code>config response-code</code>		
<response-code_int>	Specify 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.	404
response-code-max <response-code_int>	Specify the maximum start and end code in a range of HTTP response codes.	No default.
response-code-rev-match {enable disable}	Enable it so that the response matches the condition if the code is not in the specified range.	disable
<code>config content-type</code>		
{text/html text/plain text/xml application/xml application/soap+xml application/json application/octet-stream text/javascript text/}	Specify a file content type to match. Use with <code>occurrence</code> to detect and control web scraping (content scraping) activity.	application/soap+xml application/xml (or)text/xml text/html text/plain application/json application/octet-stream text/javascript text/css
content-type-rev-match {enable disable}	Enable it so that the content type matches the condition if it's not the specified type.	disable

Variable	Description	Default
<code>config packet-interval</code>		
packet-interval-timeout <timeout_int>	Specify 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
<code>config parameter</code>		
name-type {plain regular}	Indicate whether the parameter name is a literal value (plain) or a regular expression that indicates multiple possible valid values (regular).	plain
name <parameter_name>	Enter either a literal value or a regular expression to match the parameter name.	No default.
value-check {enable disable}	Enable to check the value of the specified parameters.	disable
value <value_regular_expression>	Enter a regular expression to match the parameter value.	No default.
location-check {enable disable}	The system by default search for the parameters in both URL and HTTP body. You can enable Location Check to restrict the search to either URL or HTTP body.	disable
location {URL HTTP-body}	Specify whether to scan the parameters in URL or HTTP body.	No default.
parameter-rev-match {enable disable}	Enable parameter-rev-match so that the request matches the condition if the URL or HTTP body does not contain the specified parameter names or values.	disable
<code>config signature-class</code>		
{010000000 020000000 030000000 040000000 050000000 060000000 090000000 100000000 110000000 120000000}	Specify the ID of a signature class. Ensure the signature is enabled in signature configuration before you use it in an advanced access control rule. For details, see waf signature on page 612 .	No default.
status {enable disable}	Specify whether the HTTP transaction	disable

Variable	Description	Default
	matches this condition if it matches the specified signature.	
config custom-signature		
custom-signature-enable {enable disable}	Specify whether the current custom signature filter is enabled.	disable
{custom-signature-group custom-signature}	Specify whether "<custom-signature-name_str>" on page 483 specifies a custom signature group or an individual signature.	custom-signature-group
"<custom-signature-name_str>"	Specify 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. For details, see waf signature on page 612 .	No default.
config occurrence		
occurrence-num "<occurrence_int>"	Specify 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 1–100,000. If the number of matches exceeds this threshold, the associated HTTP source client IP address or client matches this condition.	1
within "<within_int>"	Specify the time period during which FortiWeb counts the number of times transactions match other filter types in the current rule. Enter a value between 1–600.	1
percentage-flag {enable disable}	Specify whether the current filter matches when the rate of matches with other filter types in the current rule exceeds the percentage "<percentage_int>" on page 483 .	disable
percentage "<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} on page 483 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
traced-by {Source-IP User Http-Session}	Specify 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 <code>user</code> , ensure that the value of client-management {enable disable} on page 698 is <code>enable</code> .	<code>source-ip</code>
<code>config geo-filter</code>		
<entry_index>	Enter the index number of the individual entry in the table.	No default.
match-exclusive {yes no}	If you select yes, FortiWeb matches the traffic from all countries except the ones you select. If you select no, FortiWeb matches the traffic from the countries you select.	No
country-list <country-list_str>	Enter the countries you select.	No default.

Example

This example allows access to URLs beginning with `/admin`, but only if they originate from `192.0.2.5`, 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 "192.0.2.5"
      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

- [waf custom-access policy on page 468](#)
- [log trigger-policy on page 96](#)
- [waf signature on page 612](#)

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 [waf custom-protection-rule on page 486](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

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>"	Enter the name of a new or existing group. The maximum length is 63 characters. To display the list of existing group, enter: <code>edit ?</code>	No default.
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999.	No default.

Variable	Description	Default
custom-protection-rule "<rule_name>"	Enter the name of the custom protection rule to associate with the custom protection group. The maximum length is 63 characters. To display a list of the existing rules, enter: 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

- [waf signature on page 612](#)
- [waf custom-protection-rule on page 486](#)

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 it.

To use your custom signatures, you must first group them so that they can be included in a rule. For details, see [waf custom-protection-group on page 485](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

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 | only_erase | deny_no_log}
    set block-period <seconds_int>
    set severity {High | Medium | Low | Info}
    set trigger "<trigger-policy_name>"
    set threat-weight {low | critical | informational | moderate | substantial |
        severe}
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 HTTP_METHOD HTTP_METHOD}
    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>"	Enter the name of the new or existing custom signature. The maximum length is 63 characters. To display a list of the existing rules, enter: edit ?	No default.
type {request response}	Specify the type of regular expression: - request—The expression is an attack signature. - response—The expression is a server information disclosure signature.	request
action {alert alert_deny alert_erase redirect block-period send_HTTP_response only_erase deny_no_log}	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 <code>type {request response}</code> on page 487 is response, it 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	alert

Variable	Description	Default
	signature-creation. You can customize the web page that FortiWeb returns to the client with the HTTP status code. • 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. 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. 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> on page 552. 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. Failure to do so may cause FortiWeb to block all connections when it detects a violation of this type. For details, see waf x-forwarded-for on page 721. • 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>" on page 704 and rdt-reason {enable disable} on page 704. • send_HTTP_response—Block and reply to the client with an HTTP error message, and generate an alert email, a log message, or both. • only_erase—Hide replies with sensitive information (sometimes called “cloaking”). Block the reply (or reset the connection) or remove the sensitive information without generating an alert email and/or log message. This option is applicable only if type is response; and this option is not supported in Offline Protection mode. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see "system replacemsg" on page 1. • deny_no_log—Deny a request. Do not generate a log message.	

Variable	Description	Default
	Caution: This setting will be ignored if monitor-mode {enable disable} on page 163 is enabled. Note: Logging and/or alert email will occur only if enabled and configured. For details, see log disk on page 66 and log alertMail on page 60.	
block-period <seconds_int>	If action {alert alert_deny alert_erase redirect block-period send_HTTP_response only_erase deny_no_log} on page 487 is <code>block-period</code>, enter 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. For details about viewing the list of currently blocked clients, see the <i>FortiWeb Administration Guide</i>: https://docs.fortinet.com/document/fortiweb The valid range is 1–3,600 seconds.	600
severity {High Medium Low Info}	When rule violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) 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. For details, see log trigger-policy on page 96. The maximum length is 63 characters. To display the list of existing trigger policies, enter: <pre>set trigger ?</pre>	No default.
threat-weight {low critical informational moderate substantial severe}	Set the threat weight.	moderate
<entry_index>	Enter the index number of the individual entry in the table. The valid range is from 1–9,999,999,999,999,999.	No 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 <code>expression</code>. GT—The signature matches when specified target has a value greater than the value of <code>threshold</code>. LT—The signature matches when specified target has a value less than the value of <code>threshold</code>. NE—The signature matches when specified target has a different value than <code>threshold</code>.	RE

Variable	Description	Default
	EQ— The signature matches when specified target has the same value as <code>threshold</code>.	
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 HTTP_ METHOD HTTP_ METHOD}	Enter the name of one or more locations in the HTTP request to scan for a signature match. For example, <code>ARGS_NAMES</code> for the names of parameters or <code>REQUEST_COOKIES</code> for strings in the HTTP Cookie: header.	No default.
response-target {RESPONSE_BODY RESPONSE_HEADER CONTENT_LENGTH HEADER_LENGTH BODY_LENGTH RESPONSE_CODE}	Enter the name of one or more locations in the HTTP response to scan for a signature match.	No default.
threshold <threshold_int>	Enter 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 expression <regex_pattern> on page 490. For example, when enabled, an HTTP reply containing the phrase <code>credit card</code> would not match an expression that looks for the phrase <code>credit card</code> (difference highlighted in bold).	disable
expression <regex_pattern>	When operator {RE GT LT NE EQ} on page 489 is RE, type a regular expression that matches either an attack from a client or a data leak from the server.	No default.

Variable	Description	Default
	If <code>action</code> is <code>Alert & Erase</code>, enclose the portion of the regular expression to erase in brackets. For example, the following command erases the expression <code>"webattack"</code> from the response packet: <pre>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</pre> To prevent false positives, it should not match anything else. The maximum length is 2,071 characters.	

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

- [waf custom-protection-group on page 485](#)
- [log trigger-policy on page 96](#)

waf dlp exception

Use this command to configure DLP Exception to apply to the DLP Policy.

The **DLP Exception** feature allows you to define granular bypass conditions for traffic that would otherwise trigger Data Loss Prevention (DLP) rules. You can create exception objects composed of one or more match elements, each specifying conditions such as client IP, HTTP header, URI, or payload hash. These exceptions can be assigned to DLP policies to exclude matching traffic from enforcement. This enables more accurate DLP coverage while minimizing false positives and maintaining support for trusted applications and sources.

Syntax

```
config waf dlp exception
edit <name>
config exception-element-list
edit <entry_index>
set match-target {HOST | URI | FULL_URL | PARAMETER | COOKIE | CLIENT_IP |
HTTP_HEADER | PAYLOAD_SHA256 | FILE_SHA256}
set operator {STRING_MATCH | REGEXP_MATCH | EQ | NE}
set ip <IP_range>
set value {<value_str> | <value_pattern>}
set value-check {enable | disable}
set value-name {<value-name_str> | <value-name_pattern>}
set concatenate-type {AND | OR}
next
end
next
end
```

Variable	Description	Default
<name>	Name of the DLP exception object. This name is referenced when assigning the exception to a DLP policy.	No default
config exception-element-list		
<entry_index>	Index number of the exception element entry.	No default
match-target {HOST URI FULL_URL PARAMETER COOKIE CLIENT_IP HTTP_HEADER PAYLOAD_SHA256 FILE_SHA256}	Specifies the traffic field to match against. Each target supports specific operators and field options.	No default
operator {STRING_MATCH REGEXP_MATCH EQ NE}	Defines how the value is compared: - STRING_MATCH – Direct string comparison. - REGEXP_MATCH – Regular expression comparison. - EQ, NE – Equal / Not Equal (only supported for CLIENT_IP).	No default
ip <IP_range>	Specifies the source IP address to match.	No default

Variable	Description	Default
	Only used when match-target is CLIENT_IP . Accepts both IPv4 and IPv6.	
value {<value_str> <value_pattern>}	Specifies the value to match for the selected target. For PAYLOAD_SHA256 and FILE_SHA256 , this must be a 64-character SHA-256 hash string. This field is not available when match-target is CLIENT_IP .	No default
value-check {enable disable}	Enable to match the value of a specified name-value pair. Only applicable for PARAMETER , COOKIE , and HTTP_HEADER . When enabled, value-name and value must be defined.	disable
value-name {<value-name_str> <value-name_pattern>}	Specifies the name of the parameter, cookie, or HTTP header to inspect when value-check is enabled. Only applicable to PARAMETER , COOKIE , and HTTP_HEADER .	No default
concatenate-type {AND OR}	Defines how this exception element is evaluated with others: • AND – All conditions must match. • OR – Any condition may match.	AND

Example

```
config waf dlp exception
  edit "DLP_exp"
    config exception-element-list
      edit 1
        set match-target HTTP_HEADER
        set operator STRING_MATCH
        set value XYZ_Corp_Marketing_Tool
        set value-check enable
        set value-name User-Agent
      end
    end
  end
```

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. For details, see [waf file-compress-rule on page 495](#).

To use this command, your administrator account's access control profile must have either **w** or **rw** permission to the **wafgrp** area. For details, see [Permissions on page 46](#).

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>"	Enter the name of a new or existing exception. The maximum length is 63 characters. To display a list of the existing exceptions, enter: edit ?	No default.
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999.	No default.
host "<protected-host_name>"	Enter the name of a protected host that the <code>Host :</code> field of an HTTP request must be in order to match the exception. The maximum length is 255 characters. This setting applies only if <code>host-status {enable disable}</code> on page 494 is <code>enable</code> .	No default.
host-status {enable disable}	Enable to apply this exception only to HTTP requests for specific web hosts. Also configure <code>host "<protected-host_name>"</code> on page 494 . Disable to match the exception based upon the other criteria, such as the URL, but regardless of the <code>Host :</code> field.	disable
request-file "<url_str>"	Enter the literal URL, such as <code>/archives</code> , to which the exception applies. The URL must begin with a slash (<code>/</code>). Do not include the name of the host, such as <code>www.example.com</code> , which is configured separately using <code>host</code> . 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 "192.0.2.2"
        set host-status enable
        set request-file "/archives"
      next
    end
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

- [waf file-compress-rule on page 495](#)

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.

When FortiWeb needs to inspect or modify the complete response body, compression applies only to responses with a pre-compressed file size smaller than the `max-cache-size` setting in System Advanced Settings. If a file exceeds this limit, FortiWeb transmits it uncompressed. You can adjust the maximum file size using the `config system advanced` command's `max-cache-size` setting. For details, see [system advanced on page 233](#).

However, if FortiWeb does not need to inspect or modify the full response body, compression applies to all response sizes.

To apply a compression rule, select it in an inline protection profile. For details, see [waf web-protection-profile inline-protection on page 696](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf file-compress-rule
  edit "<rule_name>"
    set compression-type {gzip | brotli | zstd}
    set compression-level {level1 | level2 | ...}
    set exclude-url "<exclusion-rule_name>"

  next
end
```

```

config content-types
  edit "<content-types_id>"
    set content-type "<content-type_name>"

```

```
end
```

Variable	Description	Default
"<rule_name>"	Enter the name of a new or existing rule. The maximum length is 63 characters. To display the list of existing rules, enter: <code>edit ?</code>	No default.
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999.	No default.
compression-type {gzip brotli zstd}	Set the file compression type. gzip — FortiWeb will use gzip for file compression. For details, see https://tools.ietf.org/html/rfc1952. brotli — FortiWeb will use Brotli for file compression. For details, see https://tools.ietf.org/html/rfc7932. zstd — FortiWeb will use Zstandard (zstd) for file compression. For details, see https://datatracker.ietf.org/doc/html/rfc8478.	No default.
compression-level {level1 level2 ...}	Set the compression level for the file to be compressed. This option is available only when you select brotli or zstd for the compression-type. Set the compression level based on the selected compression type: brotli — The valid range is level1–level11. zstd — The valid range is level1–level20.	No default.
content-type "<content-type_name>"	Enter 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 - application/json - application/rss+xml To compress multiple file types, add each file type in a separate table entry with its own <entry_index> on page 496. See Example on page 497.	No default.

Variable	Description	Default
<code>exclude-url "<exclusion-rule_name>"</code>	Enter the name of an exclusion to use with the rule, if any. For details, see waf exclude-url on page 493 . The maximum length is 63 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 "file-compress-rule_name"
    set compression-type gzip
    set compression-level level2
    set 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

- [waf exclude-url on page 493](#)

waf file-upload-restriction-policy

Use this command to set file security policies that FortiWeb will use to manage 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](#) (page 1) command. Each rule identifies the host and/or URL to which the restriction applies and the types of files allowed. To apply a file security 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 details, see [Permissions on page 46](#).

Syntax

```
config waf file-upload-restriction-policy
  edit "<file-upload-restriction-policy_name>"
    set action {alert | alert_deny | block-period | deny_no_log}
    set block-period <seconds_int>
```

```

set severity {High | Medium | Low | Info}
set trigger <trigger-policy_name>
set trojan-detection {enable | disable}
set av-scan {enable | disable}
set fortisandbox-check {enable | disable}
set hold-session-while-scanning-file {enable | disable}
set icap-server-check {enable | disable}
set exchange-mail-detection {enable | disable}
set owa-protocol {enable | disable}
set activesync-protocol {enable | disable}
set mapi-protocol {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>"	Enter the name of an existing or new file security policy. The maximum length is 63 characters. To display the list of existing policies, enter: <pre>edit ?</pre>	No default.
action {alert alert_deny block-period deny_no_log}	Enter 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. For details, see "system replacemsg" on page 1 and the <i>FortiWeb Administration Guide</i>: http://docs.fortinet.com/fortiweb/admin-guides • block-period—Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int> on page 499. • deny_no_log—Deny a request. Do not generate a log message. Note: If FortiWeb is deployed behind a NAT load balancer, when using this option, you must also define an X-header that indicates the original client's IP. Failure to do so may cause FortiWeb to block all connections when it detects a violation of this type. For details, see waf x-forwarded-for on page 721.	alert

Variable	Description	Default
	Caution: This setting will be ignored if monitor-mode {enable disable} on page 163 is enabled. Note: Logging and/or alert email will occur only if enabled and configured. For details, see log disk on page 66 and log alertMail on page 60. Note: If an auto-learning profile will be selected in the policy with Offline Protection profiles that use this rule, you should select <code>alert</code>. If the <code>action</code> is <code>alert_deny</code>, the FortiWeb appliance will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For details about auto-learning requirements, see "waf web-protection-profile autolearning-profile" on page 1.	
<code>block-period <seconds_int></code>	If action {alert alert_deny block-period deny_no_log} on page 498 is <code>block-period</code> , type the number of seconds that violating requests will be blocked. The valid range is 1–3,600 seconds.	600
<code>severity {High Medium Low Info}</code>	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	Low
<code>trigger <trigger-policy_name></code>	Enter the name of the trigger to apply when this policy is violated. For details, see log trigger-policy on page 96. The maximum length is 63 characters. To display the list of existing triggers, enter: <pre>set trigger ?</pre>	No default.
<code>trojan-detection {enable disable}</code>	Enter <code>enable</code> 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
<code>av-scan {enable disable}</code>	Enter <code>enable</code> to scan for viruses, malware, and greyware.	disable
<code>fortisandbox-check {enable disable}</code>	Enter <code>enable</code> to send matching files to FortiSandbox for evaluation. Also specify the FortiSandbox settings for your FortiWeb. For details, see system fortisandbox on page 305. FortiSandbox evaluates the file and returns the results to FortiWeb. If trojan-detection {enable disable} on page 499 is <code>enable</code> and FortiWeb detects a virus, it does not send the file to FortiSandbox.	disable

Variable	Description	Default
exchange-mail-detection {enable disable}	Enter <code>enable</code> so that FortiWeb will scan email attachments in applications using OWA or ActiveSync protocols. If enabled, FortiWeb will perform Trojan detection, an antivirus scan, and will send the attachments to FortiSandbox. Note: To perform Trojan detection, an antivirus scan, and send attachments to FortiSandbox, you must enable trojan-detection {enable disable} on page 499, trojan-detection {enable disable} on page 499, and fortisandbox-check {enable disable} on page 499, respectively, in the file security policy.	disable
owa-protocol {enable disable}	Available only when exchange-mail-detection {enable disable} on page 500 is set to <code>enable</code> . If enabled, FortiWeb will scan attachments in Exchange Email sent and received via a web browser login.	disable
activesync-protocol {enable disable}	Available only when exchange-mail-detection {enable disable} on page 500 is set to <code>enable</code> . If enabled, FortiWeb will scan attachments in Exchange Email sent and received via a mobile phone login.	disable
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999,999.	No default.
file-upload-restriction-rule <rule_name>	Enter the name of an upload restriction rule to use with the policy, if any. For details, see "server-policy custom-application application-policy" on page 1. The maximum length is 63 characters. To display the list of existing rules, enter: <pre>set file-upload-restriction-rule ?</pre>	No default.
hold-session-while-scanning-file {enable disable}	Enable it, and FortiWeb waits for up to 30 minutes. If FortiWeb holds the session for over 30 minutes while FortiSandbox scans the file in the request, FortiWeb will forward the session without taking any other actions. This option is available only when you enable Send files to FortiSandbox.	disable
mapi-protocol {enable disable}	FortiWeb will scan attachments in Email sent and received via the Messaging Application Programming Interface (MAPI), a new transport protocol implemented in Microsoft Exchange Server 2013 Service Pack 1 (SP1). Available only when Scan attachments in Email is enabled.	disable
icap-server-check {enable disable}	Enable so that FortiWeb sends files to ICAP server that matches the uploading or downloading direction.	disable

Related topics

- [server-policy custom-application application-policy on page 1](#)
- [log trigger-policy on page 96](#)
- [system fortisandbox on page 305](#)

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 security policy. For details, see [waf file-upload-restriction-policy on page 497](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf file-upload-restriction-rule
  edit "<file-upload-restriction-rule_name>"
    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>
    set type {Allow| Block}
    set octet-stream-filename-position {Default | Header | Parameter | Resource}
    set octet-stream-filename-string <Header or Parameter names>
    set enable_base64_decode {enable | disable}
    set json-file-support {enable | disable} on page 503
    set json-key-for-filename <filename> on page 503
    set json-key-field <FileContents> on page 503
    set file-uncompress {enable | disable}
    set uncompress-nest-limit <int>
    set uncompress-oversize-limit <int>
  config file-types
    edit <entry_index>
      set file-type-id "<id_str>"
      set file-type_name "<file-type-extension_str>"
    next
  config custom-file-types
    edit <entry_index>
      set file-type <custom-file-type-str>
    next
  end
next
end
```

Variable	Description	Default
"<file-upload-restriction-rule_name>"	Enter the name of a new or existing rule. The maximum length is 63 characters. To display the list of existing rules, enter: <code>edit ?</code>	No default.
host-status {enable disable}	Enable to apply this exception only to HTTP requests for specific web hosts. Disable to match the exception based upon the other criteria, such as the URL, but regardless of the <code>Host :</code> field.	disable
host "<protected-host_name>"	Enter the name of a protected host that the <code>Host :</code> 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 {enable disable} on page 502 is <code>enable</code> .	No default.
request-file "<url_pattern>"	Depending on your selection in request-type {regular plain} on page 502 , type either: - The literal URL, such as <code>/fileupload</code>, that the HTTP request must contain in order to match the signature exception. The URL must begin with a slash (<code>/</code>). - A regular expression, such as <code>^/*\.php</code>, matching all and only the URLs to which the signature exception should apply. The pattern is not required to begin with a slash (<code>/</code>). However, it must at least match URLs that begin with a slash, such as <code>/index.cfm</code>. Do not include the name of the web host, such as <code>www.example.com</code> , which is configured separately in analyzer-policy "<fortianalyzer-policy_name>" on page 97 . The maximum length is 255 characters. Note: Regular expressions beginning with an exclamation point (<code>!</code>) are not supported. For information on language and regular expression matching, see the <i>FortiWeb Administration Guide</i> : https://docs.fortinet.com/document/fortiweb	No default.
request-type {regular plain}	Select whether analyzer-policy "<fortianalyzer-policy_name>" on page 97 will contain a literal URL (<code>plain</code>), or a regular expression designed to match multiple URLs (<code>regular</code>).	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 maximum acceptable values are: 102400 KB: FortiWeb 100D, 100E, 100F, 400C, 400D, 400E, 400F, 600D, 600E, 600F, 1000C, 3000CFsx, 4000C	0

Variable	Description	Default
	204800 KB: FortiWeb 1000D, 2000D, 3000D, 3000DFsx, 4000D, 1000E, 2000E, 3010E, 1000F, 2000F 358400 KB: FortiWeb 3000E, 4000E, 3000F, 4000F	
type {Allow Block}	Select to Allow or Block file types and custom file types	Block
octet-stream-filename-position {Default Header Parameter Resource}	Identify where to retrieve the filename of 'application/octet-stream' type file.	Default
octet-stream-filename-string <Header or Parameter names>	Specify the header or parameter names to get the file name of octet-stream. e.g. X-File-Name;X-Name.	No default.
json-file-support {enable disable}	Enable JSON File Support if you want FortiWeb to further parse the file contained in JSON file.	Disable
json-key-for-filename <filename>	FortiWeb will parse the JSON file to find the value of the <code>filename</code> parameter, and compare it against the value you set for json-key-for-filename . This is optional.	No default.
json-key-field <FileContents>	FortiWeb will parse the JSON file to find the value of the <code>content</code> parameter, and compare it against the value you set for json-key-field . Both json-key-for-filename and json-key-field require exact match and are case sensitive. If both of them matches, FortiWeb will apply File Security policy to the file contained in JSON file. If only json-key-field matches, FortiWeb will apply File Security policy to the file contained in JSON file, and in the attack log the name of the file will be shown as "JSON File". If only json-key-for-filename matches, it equals to no match. FortiWeb will not execute further scan to the file contained in JSON file.	No default.
enable_base64_decode {enable disable}	Enable to decode the file contained in the JSON file with base64.	enable
file-uncompress {enable disable}	Enable file unzip in CLI to verify file type and size in the compressed files.	disable
uncompress-nest-limit <int>	Type the maximum number of allowed levels of compression ("nesting") that FortiWeb will attempt to decompress. The valid range is 1-100.	12

Variable	Description	Default
uncompress-oversize-limit <int>	Type the maximum size in kilobytes (KB) of the memory buffer that FortiWeb will use to temporarily undo the compression. When the file has multiple compression levels and the size of the decompressed files reaches the maximum when FortiWeb decompresses to a certain level, then FortiWeb will only check the already-decompressed files. The files that are not decompressed will pass through FortiWeb without scanning.	5,000
<entry_index>	Enter the index number of the individual entry in the table. Each entry in the table can define one file type. The valid range is 1–9,999,999,999,999,999.	No 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) • 00203 (MSI) • 00204 (BAT)	No default.
file-type_name "<file-type-extension_str>"	Enter the extension, such as <code>MP3</code> , 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.	No default.

Variable	Description	Default
	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.	
file-type <custom-file-type-str>	If the file type is not one of the Recognized file types, use this command to enter your custom file type.	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

- [server-policy custom-application application-policy on page 1](#)

waf ftp-command-restriction-rule

Use this command to create FTP command restriction rules to specify acceptable FTP commands that clients can use to communicate with your server(s). Certain FTP commands can expose your server(s) to attack. For example, because attackers can exploit the `PORT` command to carry out FTP bounce attacks, restricting the `PORT` command can harden your network's security if you're using FTP.

For details about applying an FTP command restriction rule to an FTP server policy, see [waf ftp-protection-profile](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).



If `ftp-security` isn't enabled in `feature-visibility`, you must enable it before you can create an FTP command restriction rule. To enable `ftp-security`, see [system feature-visibility on page 288](#).

Syntax

```
config waf ftp-command-restriction-rule
edit "<rule_name>"
    set action {alert | alert_deny | block-period | deny_no_log}
    set block-period <block_period_int>
    set severity {High | Info | Low | Medium}
    set trigger "<policy_name>"
    next
end
config command-types
    edit <entry_index>
        set command-type <ftp_command>

    next
end
```

Variable	Description	Default
"<rule_name>"	Enter a unique name that can be referenced in other parts of the configuration. Don't use spaces or special characters. The maximum length is 63 characters.	No default.
<entry_index>	Enter an index number of the individual entry in the table. The valid range is 1–999,999,999,999,999. You must create an entry index for each FTP command that you plan to include in the rule.	No default.
command-type <ftp_command>	Enter an FTP command that you want to include in the rule. You can include these FTP commands in the rule: • ABOR • ACCT • ALLO • APPE • AUTH • CDUP • CWD • DELE • EPRT • EPSV • FEAT • HELP • MLSD • MODE • NLST • OPTS • PASS • PASV • PORT • PROT • PWD • QUIT • REIN • REST • RNTO • SITE • SIZE • SMNT • STAT • STOR • STOU • STRU • SYST • TYPE • USER • XCUP	No default.

Variable	Description	Default
	• LIST • MDTM • MKD • RETR • RMD • RNFR • XMKD • XPWD • XRMD	
action {alert alert_deny block-period deny_no_log}	Select which action FortiWeb will take when it detects a violation of the rule: • <code>alert</code>—Accept the connection and generate an alert email and/or log message. • <code>alert_deny</code>—Block the request (or reset the connection) and generate an alert and/or log message. • <code>deny_no_log</code>—Block the request (or reset the connection). • <code>block-period</code>—Block subsequent requests from the client for a number of seconds. Also configure waf ftp-command-restriction-rule on page 505. Note: This setting will be ignored if <code>monitor-mode {enable disable}</code> on page 163 is enabled in a server policy.	alert
block-period <block_period_int>	Enter the number of seconds that you want to block subsequent requests from a client after FortiWeb detects that the client has violated the rule. The valid range is 1–3,600 seconds. This setting is available only if <code>action {alert alert_deny block-period deny_no_log}</code> on page 507 is set to <code>block-period</code>.	600
severity {High Info Low Medium}	When rule violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs a violation of the rule: • Info • Low • Medium • High	Medium
trigger "<policy_name>"	Enter the name of a trigger policy, if any, that FortiWeb will use when it logs and/or sends an alert email about a violation of the rule.	No default.

Related Topic

- [waf ftp-protection-profile](#) on page 510
- [system feature-visibility](#) on page 288
- [waf ftp-file-security](#) on page 508

waf ftp-file-security

Use this command to create FTP file check rules so that FortiWeb places restrictions on uploading or downloading files and scans files that clients attempt to upload to or download from your server(s). When configured, FortiWeb can also send files to FortiSandbox for analysis and perform an antivirus scan.

For details about applying an FTP file check rule to an FTP server policy, see [waf ftp-protection-profile](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).



If `ftp-security` isn't enabled in `feature-visibility`, you must enable it before you can create an FTP file check rule. To enable `ftp-security`, see [system feature-visibility on page 288](#).

Syntax

```
config waf ftp-file security
  edit "<rule_name>"
    set action {alert | alert_deny | block-period | deny_no_log}
    set block-period <block_period_int>
    set severity {High | Info | Low | Medium}
    set trigger "<policy_name>"
    set check-dir {both | download | upload}
    set av-scan {enable | disable} on page 509
    set send-files-to-fortisandbox {enable | disable}
    set icap-server-check {enable | disable}

  next
end
```

Variable	Description	Default
"<rule_name>"	Enter a unique name that can be referenced in other parts of the configuration. Don't use spaces or special characters. The maximum length is 63 characters.	No default.
action {alert alert_deny block-period deny_no_log}	Select which action FortiWeb will take when it detects a violation of the rule: <code>alert</code>—Accept the connection and generate an alert email and/or log message. <code>alert_deny</code>—Block the request (or reset the connection) and generate an alert and/or log message. <code>deny_no_log</code>—Block the request (or reset the connection). <code>block-period</code>—Block subsequent requests from the client for a number of seconds. Also configure waf ftp-	alert_deny

Variable	Description	Default
	file-security on page 508 . Note: This setting will be ignored if monitor-mode {enable disable} on page 163 is enabled in a server policy.	
block-period <block_period_int>	Enter the number of seconds that you want to block subsequent requests from a client after FortiWeb detects that the client has violated the rule. The valid range is 1–3,600 seconds. This setting is available only if waf ftp-file-security on page 508 is set to <code>block-period</code>.	600
severity {High Info Low Medium}	When rule violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs a violation of the rule: • Info • Low • Medium • High	Medium
trigger "<policy_name>"	Enter the name of a trigger policy, if any, that FortiWeb will use when it logs and/or sends an alert email about a violation of the rule.	No default.
check-dir {both download upload}	Select one of the following: • <code>both</code>—FortiWeb applies the rule to files being either downloaded from or uploaded to your server(s). • <code>download</code>—FortiWeb applies the rule to files being downloaded from your server(s). • <code>upload</code>—FortiWeb applies the rule to files being uploaded to your server(s).	upload
av-scan {enable disable}	Enable so that FortiWeb performs an antivirus scan on files that match the waf ftp-file-security on page 508 .	disable
send-files-to-fortisandbox {enable disable}	Enable so that FortiWeb sends files to FortiSandbox that match the waf ftp-file-security on page 508. Also specify the FortiSandbox settings for your FortiWeb. For details, see system fortisandbox on page 305. FortiSandbox evaluates the file and returns the results to FortiWeb. If waf ftp-file-security on page 508 is enabled and FortiWeb detects a virus, it does not send the file to FortiSandbox.	disable
icap-server-check {enable disable}	Enable so that FortiWeb sends files to ICAP server that matches the uploading or downloading directions.	disable

Related Topic

- [system feature-visibility on page 288](#)
- [waf ftp-command-restriction-rule on page 505](#)
- [waf ftp-protection-profile on page 510](#)

waf ftp-protection-profile

Use this command to configure an FTP security inline profile.

FTP security inline profiles combine previously-configured rules, profiles, and policies in a comprehensive set that can be applied in an FTP server policy. Apply the profile in an FTP server policy. For details, see [server-policy policy on page 150](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `traroutegrp` area. For details, see [Permissions on page 46](#).

Before creating an FTP security inline profile

Prior to creating an FTP security inline profile, you should create and configure the rules, profiles, and policies that you plan to add to the FTP security inline profile. You can include the following:

- FTP Command Restriction rules (see [waf ftp-command-restriction-rule on page 505](#))
- FTP File Check rules (see [waf ftp-file-security on page 508](#))
- IP Reputation intelligence (see [waf ip-intelligence-ignore-x-forwarded-for on page 560](#))
- Geo IP rules (see [waf geo-block-list on page 511](#))
- IP List rules (see [waf ip-list on page 561](#))



If `ftp-security` isn't enabled in `feature-visibility`, you must enable it before you can create an FTP security inline profile. To enable `ftp-security`, see [system feature-visibility on page 288](#).

Syntax

```
config waf ftp-protection-profile
edit "<policy_name>"
    set ftp-file-check "<rule_name>"
    set ftp-geo-ip "<rule_name>"
    set ftp-ip-check "<rule_name>"
    set ftp-ip-intelligence {enable | disable}
    set ftp-restriction-command-type "<rule_name>"
```

Variable	Description	Default
"<policy_name>"	Enter a unique name that can be referenced in other parts of the configuration. Don't use spaces or special characters. The maximum length is 63 characters.	No default.
ftp-file-check "<rule_name>"	Enter the name of an FTP file check rule that you previously created. If you haven't created an FTP file check rule to include in this profile yet, see waf ftp-file-security on page 508 for instructions about creating one.	No default.
ftp-geo-ip "<rule_name>"	Enter the name of a geo IP block policy that you previously created. If you haven't created a geo IP block policy to include in this profile yet, see waf geo-block-list on page 511 for instructions about creating one.	No default.
ftp-ip-check "<rule_name>"	Enter the name of an IP List that you previously created. If you haven't created an IP List rule to include in this profile yet, see waf ip-list on page 561 for instructions about creating one.	No default.
ftp-ip-intelligence {enable disable}	Enable to include the active IP reputation policy in this profile. If you haven't created an IP reputation policy to include in this profile yet, see "To configure an IP reputation policy" on page 1 for instructions about creating one.	disable
ftp-restriction-command-type "<rule_name>"	Enter the name of an FTP command restriction rule that you previously created. If you haven't created an FTP command restriction rule to include in this profile yet, see waf ip-intelligence-ignore-x-forwarded-for on page 560 for instructions about creating one.	No default.

Related Topics

- [server-policy policy on page 150](#)
- [waf ftp-command-restriction-rule on page 505](#)
- [waf ftp-file-security on page 508](#)
- [waf ip-intelligence-ignore-x-forwarded-for on page 560](#)
- [waf geo-block-list on page 511](#)
- [waf ip-list on page 561](#)

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 Customer Service & Support website: <https://support.fortinet.com>

Optionally, you can also specify a list of IP addresses or IP address ranges that are exempt from this blacklist. For details, see [waf geo-ip-except on page 514](#).

Alternatively, you can block clients individually (see ["server-policy custom-application application-policy" on page 1](#)) or based upon their reputation (see [waf ip-intelligence-ignore-x-forwarded-for on page 560](#)).

To apply the rule, select it in a protection profile. For details, see [waf web-protection-profile inline-protection on page 696](#) or [waf web-protection-profile offline-protection on page 706](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf geo-block-list
  edit "<geography-to-ip_name>"
    set severity {High | Medium | Low | Info}
    set action { alert_deny | block-period | deny_no_log}
    set block-period <block_period_int>
    set trigger "<trigger-policy_name>"
    set ignore-x-forwarded-for {enable | disable}
  config country-list
    edit <entry_index>
      set country-name "<region_name>"
    next
  end
next
end
```

Variable	Description	Default
"<geography-to-ip_name>"	Enter the name of a new or existing rule. The maximum length is 63 characters. To display the list of existing rules, enter: <code>edit ?</code>	No default.
severity {High Medium Low Info}	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	Low
action { alert_deny block-period deny_no_log}	Select which action FortiWeb will take when it detects a violation of the rule: <code>alert_deny</code>—Block the request (or reset the connection) and generate an alert and/or log message. <code>deny_no_log</code>—Block the request (or reset the connection).	block-period

Variable	Description	Default
	<code>block-period</code>—Block subsequent requests from the client for a number of seconds. Also configure <code>block-period</code>. Note: This setting will be ignored if <code>monitor-mode {enable disable}</code> on page 163 is enabled in a server policy.	
<code>block-period <block_period_int></code>	Enter the number of seconds that you want to block subsequent requests from a client after FortiWeb detects that the client has violated the rule. The valid range is 1–3,600 seconds. This setting is available only if <code>Action</code> is set to <code>block-period</code>.	60
<code>trigger "<trigger-policy_name>"</code>	Enter the name of the trigger to apply when this rule is violated. For details, see log trigger-policy on page 96. The maximum length is 63 characters. To display the list of existing trigger policies, enter: <pre>set trigger ?</pre>	No default.
<code>ignore-x-forwarded-for {enable disable}</code>	By default, FortiWeb scans the IP addresses in the X-Forwarded-For header at the HTTP layer. This causes high resource consumption. To enhance the performance, you can enable Ignore X-Forwarded-For so that the IP addresses can be scanned at the TCP layer instead. This avoids HTTP packets being processed unnecessarily.	disable
<code><entry_index></code>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999.	No default.
<code>country-name "<region_name>"</code>	Enter 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

- [log trigger-policy on page 96](#)
- [waf geo-ip-except on page 514](#)
- [waf web-protection-profile inline-protection on page 696](#)
- [server-policy custom-application application-policy on page 1](#)
- [waf ip-intelligence-ignore-x-forwarded-for on page 560](#)
- [debug flow trace on page 759](#)

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 details about creating the blocklist by country or region, see [waf geo-block-list on page 511](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

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>"	Enter the name of a new or existing list of exceptions. To display the list of existing rules, enter: <code>edit ?</code>	No default.
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999.	No default.

Variable	Description	Default
<code>ip {"<address_ipv4>" "<ip_range_ipv4>"}</code>	Enter 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 geo-location blocklist exception list `allow-north-america`.

```
config waf geo-ip-except
  edit "allow-north-america"
    set ip "92.0.2.0-192.0.2.5"
  end
next
end
```

Related topics

- [waf geo-block-list on page 511](#)
- [server-policy custom-application application-policy on page 1](#)
- [waf ip-intelligence-ignore-x-forwarded-for on page 560](#)
- [debug flow trace on page 759](#)

waf graphql-validation rule

Use this command to create GraphQL protection rules and configure GraphQL protection policies.

Syntax

```
config waf graphql-validation rule
  edit "<graphql_rule_name>"
    set host-status {enable | disable}
    set host "<host_name_str>"
    set request-type {plain | regular}
    set request-url <string>
    set action {alert | alert_deny | block-period | redirect | send_403_forbidden |
      deny_no_log}
    set block-period <period_int>
    set severity {High Low | Medium | Info}
    set trigger "<trigger_policy_name>"
    set enable-introspection {enable | disable}
    set enable-fragment {enable | disable}
    set graphql-data-size <integer>
    set field-number <integer>
    set value-size <integer>
    set object-depth <integer>
    set alias-batch-query {enable | disable}
```

```

    set alias-batch-query-number <integer>
    set array-batch-query {enable | disable}
    set array-batch-query-number <integer>
  next
end
config waf graphql-validation policy
  edit <graphql_policy_name>
    set enable-signature-detection {enable | disable}
    config input-rule-list
      edit <graphql_rule_list_id>
        set graphql_input_rule <graphql_input_rule_str>
      next
    end
  next
end

```

Variable	Description	Default
"<graphql_rule_name>"	Enter a name that can be referenced by other parts of the configuration. You will use the name to select the rule in a GraphQL protection policy.	No default.
host-status {enable disable}	Enable to compare the GraphQL rule to the <code>Host:</code> field in the HTTP header. If enabled, also configure <code>host "<host_name_str>"</code> on page 516.	disable
host "<host_name_str>"	Enter the name of a protected host that the <code>Host:</code> field of an HTTP request must match in order for the rule to apply. For details, see server-policy allow-hosts on page 106 .	No default.
request-type {plain regular}	Select whether request-type {plain regular} on page 516 must contain either: <code>plain</code>—The field is a string that the request URL must match exactly. <code>regular</code>—The field is a regular expression that defines a set of matching URLs.	No default.
request-url <string>	Depending on your selection for request-type {plain regular} on page 516 , enter either: <code>plain</code>—The literal URL, such as <code>/index.php</code>, that the HTTP request must contain in order to match the rule. The URL must begin with a slash (<code>/</code>). <code>regular</code>—A regular expression, such as <code>^/*.php</code>, matching the URLs to which the rule should apply. The pattern does not require a slash (<code>/</code>), but it must match URLs that begin with a slash, such as <code>/index.cfm</code>. Do not include the domain name, such as <code>www.example.com</code> , which is configured separately in <code>host "<host_name_str>"</code> on page 516.	No default.

Variable	Description	Default
action {alert alert_deny block-period redirect send_403_forbidden deny_no_log}	Select one of the following actions that FortiWeb performs when a request violates the rule: <code>alert</code>—Accept the request and generate an alert email and/or log message. <code>alert_deny</code>—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. For details, see "system replacemsg" on page 1. <code>block-period</code>—Block subsequent requests from the client for a number of seconds. Also configure <code>block-period <period_int></code> on page 517. <code>redirect</code>—Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. <code>send_403_forbidden</code>—Reply to the client with an HTTP 403 Access Forbidden error message and generate an alert email and/or log message. <code>deny_no_log</code>—Deny a request. Do not generate a log message. Caution: FortiWeb ignores this setting when <code>monitor-mode {enable disable}</code> on page 163 is enabled. Note: Logging and/or alert email will occur only if enabled and configured. For details, see log disk on page 66 and log alertMail on page 60.	alert
block-period <period_int>	Enter the amount of time (in seconds) that you want to block subsequent requests from a client after FortiWeb detects a rule violation. This setting is available only when <code>action {alert alert_deny block-period redirect send_403_forbidden deny_no_log}</code> on page 517 is <code>block-period</code>. The valid range is 1–3,600 seconds.	600
severity {High Low Medium Info}	When rule violations are recorded in the attack log, each log message contains a Severity Level field. Select which severity level FortiWeb will use when it logs a violation of the rule: - Low - Medium - High - Info	Low
trigger "<trigger_policy_name>"	Enter the name of the trigger, if any, to apply when the rule is violated. The maximum length is 63 characters. For details, see log trigger-policy on page 96.	No default.

Variable	Description	Default
	To display a list of existing triggers, enter: set trigger ?	
enable-introspection {enable disable}	Enable to allow introspection queries.	disable
enable-fragment {enable disable}	Enable to allow fragments.	disable
graphql-data-size <integer>	It sets a limit on the size of the HTTP request body in the POST method or the size of URL parameters in the GET method.	1024
field-number <integer>	It limits the number of terminal fields within a query, thereby limiting the number of fields within objects.	256
value-size <integer>	It sets a maximum length on any user input value within a GraphQL query. - If the value is an array, each item in the array is evaluated against the specified value size. - If the value is an object, only the values contained within the object are compared to the value size, not the keys themselves.	256
object-depth <integer>	It limits the depth of a GraphQL query, which limits how deeply nested the query can be.	32
alias-batch-query {enable disable}	Enable this option to allow alias batching.	disable
alias-batch-query-number <integer>	It sets a limit on the number of queries that can be found within an alias batch. Only available when Alias Batching is enabled.	8
array-batch-query {enable disable}	Enable this option to allow array batching	disable
array-batch-query-number <integer>	It sets a limit on the number of queries that can be found within an array batch. Only available when Array Batching is enabled.	8
<graphql_policy_name>	Enter the name of a GraphQL protection policy. You will use the name to select the policy in other parts of the configuration.	No default.
<graphql-rule-list_id>	Enter the index number of an entry to create or modify a rule for the policy.	No default.
enable-signature-detection {enable disable}	Enable to scan for matches with signature attacks in GraphQL API requests.	disable
graphql_input_rule <graphql_input_rule_str>	Enter the sequence number of a GraphQL protection rule to add to the GraphQL protection policy.	No default.

Related topics

- [waf json-schema on page 565](#)
- [waf web-protection-profile inline-protection on page 696](#)

waf grpc-security rule

Use this command to configure gRPC related settings.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf grpc-security rule
edit grpc-security_rule_name
    set host-status {enable | disable}
    set host <host_str>
    set url <url_str>
    set idl-file <file_name>
    set rate-limit <int>
    set size-limit <int>
    set req-message-name <string>
    set rsp-message-name <string>
    set action {alert | deny_no_log | alert_deny | block-period}
    set block-period <int>
    set severity {High | Medium | Low | Info}
    set replace-response {enable | disable}
    set trigger <trigger-policy_name>
next
end
```

Variable	Description	Default
grpc-security_rule_name	Enter the WebSocket security rule name.	No default.
host-status {enable disable}	Enable to compare the WebSocket security rule to the <code>Host:</code> field in the HTTP header.	No default.
host <host_str>	Select the IP address or fully qualified domain name (FQDN) of the protected host to which this rule applies. This option is available only if Host Status is enabled.	No default.
url <url_str>	The URL of the gPRC API request you want to protect.	No default.

Variable	Description	Default
	You can enter the literal URL, such as <code>/folder1/index.htm</code> that the HTTP request must contain in order to match the rule, or use wildcards to match multiple URLs, such as <code>/folder1/*</code> or <code>/folder1/*/index.htm</code> . The URL must begin with a slash (/).	
idl-file <file_name>	Enter the name of the IDL file you have uploaded in the gRPC IDL File tab in Web Protection > Protocol > gRPC . FortiWeb will decode the traffic according to the IDL file.	No default.
rate-limit <int>	Specify the maximum number of messages within a gRPC API request.	20
size-limit <int>	Specify the maximum size of each message body in a gRPC API request.	4194303
req-message-name <string>	The name of message in the gRPC API request. FortiWeb will apply this gRPC security rule to the matched message. The format should be " <i><package_name>.<message_name></i> ", for example <code>routeguide.Point</code> . It's case sensitive. <pre> option objc_class_prefix = "RTG"; package routeguide; // Interface exported by the server. service RouteGuide { // A simple RPC. // // Obtain the feature at a given position. rpc GetFeature(Point) Features; message Point { int32 latitude = 1; int32 longitude = 2; } </pre>	No default.
rsp-message-name <string>	The name of message in the gRPC API response. FortiWeb will apply this gRPC security rule to the matched message. Refer to <code>req-message-name</code> for the format of the name.	No default.
action {alert deny_no_log alert_deny block-period}	Select which action the FortiWeb appliance will take when it detects a violation. Alert —Accept the connection and generate an alert email and/or log message. alert_deny —Block the request (or reset the connection) and generate an alert and/or log message. deny_no_log —Block the request (or reset the connection).	Alert

Variable	Description	Default
	block-period —Block subsequent requests from the client for a number of seconds. Also configure waf grpc-security rule on page 519 .	
block-period <int>	If <code>action</code> is <code>block-period</code> , type the number of seconds that the client will be blocked.	600
severity {High Medium Low Info}	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	medium
replace-response {enable disable}	For gRPC API traffic, FortiWeb now supports obscuring sensitive data in server's response if it matches the Information Disclosure and Personally Identifiable Information signatures. FortiWeb will detect any sensitive data in the back-end server's response and replace it with "xxx". Please note that to make this function work, ensure that the Action for Information Disclosure and Personally Identifiable Information has been set to Erase or Erase & Alert in Web Protection > Known Attacks > Signatures .	disable
trigger <trigger-policy_name>	Enter the name of the trigger to apply when this rule is violated (see log trigger-policy on page 96). The maximum length is 63 characters. To display the list of existing trigger policies, enter: <code>set trigger ?</code>	No default.

Related topics

[waf grpc-security policy on page 521](#)

waf grpc-security policy

Use this command to create gRPC policy.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf grpc-security policy
edit "<"<policy_name>"
    config rule-list
        edit rule-list_id on page 522
            set rule "<rule_name>"
        next
    next
```

```

    end
  next
end

```

Variable	Description	Default
"<policy_name>"	Enter the gPRC Security policy name.	No default.
rule-list_id	Enter the sequence number of the rule in the rule list.	
rule "<rule_name>"	Select the created gPRC security rule name.	No default.

Related topics

[waf grpc-security rule on page 519](#)

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 [waf web-protection-profile inline-protection on page 696](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

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>"	Enter the name of a new or existing hidden field rule group. The maximum length is 63 characters. To display the list of existing groups, enter: <code>edit ?</code>	No default.
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999,999.	No default.

Variable	Description	Default
hidden-field-rule "<hidden-field-rule_name>"	Enter the name of an existing hidden field rule to add to the group. The maximum length is 63 characters. To display the list of existing rules, enter: <pre>set hidden-field-rule ?</pre>	No default.

Related topics

- [waf hidden-fields-rule on page 523](#)
- [waf web-protection-profile inline-protection on page 696](#)

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 website 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 [waf hidden-fields-protection on page 522](#).

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 [server-policy allow-hosts on page 106](#).



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*:

<https://docs.fortinet.com/document/fortiweb>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf hidden-fields-rule
edit "<hidden-field-rule_name>"
```

```

set action {alert | alert_deny | redirect | block-period | send_403_forbidden |
    deny_no_log}
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 severity {High | Medium | Low | Info}
set trigger "<trigger-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>"	Enter the name of a new or existing rule. The maximum length is 63 characters. To display the list of existing rules, enter: edit ?	No default.
action {alert alert_deny redirect block-period send_403_forbidden deny_no_log}	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. For details, see "system replacemsg" on page 1. • block-period—Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int> on page 552. 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. Failure to do so may cause FortiWeb to block all	alert

Variable	Description	Default
	connections when it detects a violation of this type. For details, see waf x-forwarded-for on page 721. <code>redirect</code>—Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. Also configure <code>redirect-url "<redirect_fqdn>"</code> on page 704 and <code>rdt-reason {enable disable}</code> on page 704. <code>send_403_forbidden</code>—Reply to the client with an HTTP 403 Access Forbidden error message and generate an alert email and/or log message. <code>deny_no_log</code>—Deny a request. Do not generate a log message. <code>block-period</code>—Block subsequent requests from the client for a number of seconds. Caution: This setting will be ignored if <code>monitor-mode {enable disable}</code> on page 163 is enabled. Note: Logging and/or alert email will occur only if enabled and configured. For details, see log disk on page 66 and log alertMail on page 60. Note: If you select an auto-learning profile with this rule, you should select <code>alert</code>. If the <code>action</code> is <code>alert_deny</code>, 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 details about auto-learning requirements, see "waf web-protection-profile autolearning-profile" on page 1.	
<code>block-period <seconds_int></code>	If <code>action {alert alert_deny redirect block-period send_403_forbidden deny_no_log}</code> on page 524 is <code>block-period</code>, enter the number of seconds that the connection will be blocked. The valid range is 1–3,600 seconds.	600
<code>host "<protected-hosts_name>"</code>	Enter the name of a protected host that the <code>Host :</code> field of an HTTP request must be in order to match the rule. The maximum length is 255 characters. This setting applies only if <code>host-status {enable disable}</code> on page 525 is <code>enable</code>.	No default.
<code>host-status {enable disable}</code>	Enable to apply this hidden field rule only to HTTP requests for specific web hosts. Also configure <code>host "<protected-hosts_name>"</code> on page 525. Disable to match the input rule based upon the other criteria, such as the URL, but regardless of the <code>Host :</code> field.	disable
<code>request-file "<url_str>"</code>	Enter the literal URL, such as <code>/login.jsp</code>, that contains the hidden form.	No default.

Variable	Description	Default
	The URL must begin with a slash (/). Do not include the name of the web host, such as <code>www.example.com</code> , which is configured separately in host "<protected-hosts_name>" on page 525 . Regular expressions are not supported. The maximum length is 255 characters.	
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 Info}	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	High
trigger "<trigger-policy_name>"	Enter the name of the trigger to apply when this rule is violated. For details, see log trigger-policy on page 96 . The maximum length is 63 characters. To display the list of existing trigger policies, enter: <code>set trigger ?</code>	No default.
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999,999.	No default.
argument "<hidden-field_str>"	Enter the name of the hidden form input, such as <code>languagepref</code> . The maximum length is 63 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

- [server-policy allow-hosts on page 106](#)
- [waf hidden-fields-protection on page 522](#)
- [log trigger-policy on page 96](#)

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*:

<https://docs.fortinet.com/document/fortiweb>

To apply HTTP authentication policies, select them in an inline protection profile. For details, see [waf web-protection-profile inline-protection on page 696](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf HTTP-authen HTTP-authen-policy
  edit "<auth-policy_name>"
    set cache {enable | disable}
    set alert-type {none | fail | success | all}
    set cache-timeout <timeout_int>
    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>"	Enter the name of a new or existing HTTP authentication policy. The maximum length is 63 characters. To display the list of existing policies, enter: edit ?	No default.

Variable	Description	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> on page 528 . This can be used can improve performance by preventing frequent queries.	No default.
alert-type {none fail success all}	Enter the instances when alerts will be issued for HTTP authentication attempts: <code>none</code>—No alerts are issued for HTTP authentication. <code>fail</code>—Alerts are issued only for HTTP authentication failures. <code>success</code>—Alerts are issued for successful HTTP authentication. <code>all</code>—Alerts are issued for all failed and successful HTTP authentication.	none
cache-timeout <timeout_int>	Enter the query cache timeout, in seconds. The valid range is 0–3,600. This option is available only when cache {enable disable} on page 528 is enabled.	300
auth-timeout <timeout_int>	Enter the connection timeout (in milliseconds) for the query to the FortiWeb's query to the remote authentication server in milliseconds. The valid range is 0–60,000. To prevent dropped connections if the authentication server does not answer queries quickly enough, increase this value.	2000
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999.	No default.
HTTP-authen-rule "<HTTP-auth-rule_name>"	Enter the name of an existing HTTP authentication rule. The maximum length is 63 characters. To display the list of existing rules, enter: <code>set HTTP-authen-rule ?</code>	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

- [waf HTTP-authen HTTP-authen-rule on page 529](#)
- [waf web-protection-profile inline-protection on page 696](#)

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 [waf HTTP-authen HTTP-authen-policy on page 527](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

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>"	Enter the name of a new or existing rule. The maximum length is 63 characters. To display the list of existing rules, enter: edit ?	No default.
host "<protected-hosts_name>"	Enter the name of a protected host that the <code>Host :</code> 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 <code>host-status</code> is <code>enable</code> .	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>" on page 530 . Disable to match the HTTP authentication rule based upon the other criteria, such as the URL, but regardless of the <code>Host :</code> field.	disable
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999,999.	No default.
authen-type {basic digest ntlm}	Select which type of HTTP authentication to use, either: <code>basic</code>—Clear text, Base64-encoded user name and password. Supports local user accounts, and RADIUS and LDAP user queries. NTLM user queries are not supported. <code>digest</code>—Hashed user name, realm, and password. RADIUS, LDAP and NTLM user queries are not supported. <code>ntlm</code>—Encrypted user name and password. Local user	basic

Variable	Description	Default
	accounts and RADIUS and LDAP user queries are not supported.	
request-url "<path_str>"	Enter the literal URL, such as <code>/employees/holidays.html</code> , that a request must match in order to trigger HTTP authentication. The maximum length is 255 characters.	No default.
user-group "<user-group_name>"	Enter the name of a user group that is authorized to use the URL in request-url "<path_str>" on page 531 . The maximum length is 63 characters. To display the list of existing user groups, enter: <code>set user-group ?</code>	No default.
user-realm "<realm_str>"	Enter the realm, such as <code>Restricted Area</code> , to which the request-url "<path_str>" on page 531 belongs. The maximum length is 63 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 <code>All_Employees</code> could have access to the request-url "<path_str>" on page 531 URLs <code>/wiki/Main</code> and <code>/wiki/ToDo</code>. These URLs both belong to the realm named <code>Intranet Wiki</code>. Because they use the same realm name, users authenticating to reach <code>/wiki/Main</code> usually will not have to authenticate again to reach <code>/wiki/ToDo</code>, as long as both requests are within the same browser session. This field does not appear if <code>authen-type</code> is <code>ntlm</code>, which does not support HTTP-style realms.	No default.

Example

For an example, see [waf HTTP-authen HTTP-authen-policy on page 527](#).

Related topics

- [user user-group on page 413](#)
- [waf HTTP-authen HTTP-authen-policy on page 527](#)

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 command is similar to [waf layer4-connection-flood-check-rule on page 586](#). 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. For details, see [waf application-layer-dos-prevention on page 440](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf HTTP-connection-flood-check-rule
  edit "<rule_name>"
    set action {alert | alert_deny | block-period | deny_no_log}
    set block-period <seconds_int>
    set HTTP-connection-threshold <limit_int>
    set severity {High | Medium | Low | Info}
    set trigger-policy "<trigger-policy_name>"
  next
end
```

Variable	Description	Default
"<rule_name>"	Enter the name of a new or existing rule. The maximum length is 63 characters. To display the list of existing rules, enter: <code>edit ?</code>	No default.
action {alert alert_deny block-period deny_no_log}	Select one of the following actions that the FortiWeb appliance will perform when the count exceeds the rate limit: • <code>alert</code>—Accept the connection and generate an alert email and/or log message.	alert

Variable	Description	Default
	<code>alert_deny</code>—Block the connection and generate an alert email and/or log message. <code>block-period</code>—Block subsequent requests from the client for a number of seconds. Also configure <code>block-period <seconds_int></code> on page 533. <code>deny_no_log</code>—Deny a request. Do not generate a log message. Caution: This setting will be ignored if <code>monitor-mode {enable disable}</code> on page 163 is enabled. Note: Logging and/or alert email will occur only if enabled and configured. For details, see log disk on page 66 and log alertMail on page 60. Note: If an auto-learning profile will be selected in the policy with Offline Protection profiles that use this rule, you should select <code>alert</code>. If the action is <code>alert_deny</code>, the FortiWeb appliance will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For details about auto-learning requirements, see "waf web-protection-profile autolearning-profile" on page 1.	
<code>block-period <seconds_int></code>	Enter the length of time (in seconds) for which the FortiWeb appliance will block additional requests after a client exceeds the rate threshold. The valid range is 1–3,600 seconds.	600
<code>HTTP-connection-threshold <limit_int></code>	Enter the maximum number of TCP connections allowed from the same client. The valid range is 1–1,024.	1
<code>severity {High Medium Low Info}</code>	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	Medium
<code>trigger-policy "<trigger-policy_name>"</code>	Enter the name of the trigger to apply when this rule is violated. For details, see log trigger-policy on page 96 . The maximum length is 63 characters. To display the list of existing trigger policies, enter: <code>set trigger ?</code>	No default.

Related topics

- [log trigger-policy on page 96](#)
- [waf application-layer-dos-prevention on page 440](#)

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 details, see [Permissions on page 46](#).

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 Internal-resource-limits-check {enable | disable} on page 536
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-name-length {enable | disable}
set max-HTTP-header-value-length {enable | disable}
set max-HTTP-request-filename-length {enable | disable}
set max-HTTP-request-length {enable | disable}
set max-url-param-name-len {enable | disable}
set max-url-param-value-len {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 http2-max-requests {enable | disable}
set parameter-name-check {enable | disable}
set parameter-value-check {enable | disable}
set redundant-header-check {enable | disable}
set source-ip-status {enable|disable}
set source-ip "<ip_range>"
set url-param-name-check {enable | disable}
```

```

set url-param-value-check {enable | disable}
set duplicate-parameter-check {enable | disable}
set null-byte-in-url-check {enable | disable}
set Illegal-byte-in-url-check {enable | disable}
set web-socket-protocol-check {enable | disable}
set odd-and-even-space-attack-check {enable | disable}
set rpc-protocol-check {enable | disable} on page 538
set Post-request-ctype-check {enable | disable}
set h2-rst-stream-check {enable | disable} on page 539
set h2-rst-stream-freq-check {enable | disable}
set cl-te-coexist-check {enable | disable}
set waf HTTP-constraints-exceptions
set missing-host-check {enable | disable}
set range-overlapping-check {enable | disable}
set multipart-formdata-bad-request-check {enable | disable}
set h3-bidir-concurrent-stream-check {enable | disable}
set h3-unidir-concurrent-stream-check {enable | disable}
move "<source-exception_id>" to {before | after | up | down} "<destination-exception_id>"

next
end
next
end

```

Variable	Description	Default
"<HTTP-exception_name>"	Enter the name of a new or existing HTTP protocol constraint exception. The maximum length is 63 characters. To display the list of existing exceptions, enter: edit ?	No default
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999.	No default
request-file "<url_pattern>"	Enter either: - The literal URL, such as <code>/index.php</code>, that the HTTP request must contain in order to match the input rule. The URL must begin with a slash (<code>/</code>). - A regular expression, such as <code>^/*.php</code>, matching all and only the URLs to which the input rule should apply. The pattern is not required to begin with a slash (<code>/</code>). However, it must at least match URLs that begin with a slash, such as <code>/index.cfm</code>. Do not include the name of the web host, such as <code>www.example.com</code> , which is configured separately in <code>host</code> . The maximum length is 255 characters.	No default
request-type {plain regular}	Enter either <code>plain</code> or <code>regular</code> (for a regular expression) to match the string entered in <code>request-file "<url_pattern>"</code> on page 535.	No default

Variable	Description	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>" on page 97. Disable to match the exception based upon the other criteria, such as the URL, but regardless of the <code>Host :</code> 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.	
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 <code>Content Type :</code> value uses the format <code><type>/<subtype></code> .	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-responses-code-check {enable disable}	Enable to omit the constraint on whether the HTTP response code is a 3-digit number.	disable
Internal-resource-limits-check {enable disable}	Enable to omit the constraint on the maximum number of limits allowed by HTTP parser.	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

Variable	Description	Default
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-name-length {enable disable}	Enable to omit the constraint on the maximum acceptable size in bytes of a single HTTP header name.	disable
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-request-length {enable disable}	Enable to omit the constraint on the maximum HTTP request length.	disable
max-url-param-name-len {enable disable}	Enable to omit the constraint on the maximum acceptable length in bytes of the parameter name.	disable
max-url-param-value-len {enable disable}	Enable to omit the constraint on the maximum acceptable length in bytes of the parameter value.	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 <code>Range</code> : fields of an HTTP header.	disable
http2-max-requests {enable disable}	Enable to omit the constraint on the maximum acceptable number of requests in an HTTP/2 connection	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

Variable	Description	Default
Post-request-ctype-check {enable disable}	Enable to omit the constraint on whether the Content-Type : header is available.	disable
source-ip-status {enable disable}	Enable to check requests for matching the HTTP constraint exceptions rule by their source IP addresses.	disable
source-ip "<ip_range>"	Enter the source IP of the protected requests to which this exception applies. Only a single IPv4/IPv6 address, or a IPv4/IPv6 range is acceptable. For example: • 1.2.3.4 • 2001::1 • 1.2.3.4-1.2.3.40 • 2001::1-2001::100 Available only when source-ip-status {enable disable} on page 538 is enable.	No default.
url-param-name-check {enable disable}	Enable to omit the constraint on illegal characters in the parameter name.	disable
url-param-value-check {enable disable}	Enable to omit the constraint on illegal characters in the parameter value.	disable
redundant-header-check {enable disable}	Enable to omit the constraint on the redundant instances of Content-Length, Content-Type and Host header fields.	disable
duplicate-parameter-check {enable disable}	Enable to omit the constraint on duplicate parameter names.	disable
null-byte-in-url-check {enable disable}	Enable to omit the constraint on null bytes in URL.	disable
Illegal-byte-in-url-check {enable disable}	Enable to omit the constraint on illegal bytes in URL.	disable
web-socket-protocol-check {enable disable}	Enable to omit detecting traffic that uses the WebSocket TCP-based protocol.	disable
odd-and-even-space-attack-check {enable disable}	Enable to omit the constraint on detecting Odd and Even Space Attack.	disable
rpc-protocol-check {enable disable}	Enable to omit detecting traffic that uses the PRC protocol.	disable

Variable	Description	Default
"<source-exception_id> to {before after up down} "<destination- exception_id>"	adjust the priority of the exception entries.	no default
h2-rst-stream-check {enable disable}	Enable to omit the constraint on the maximum acceptable number of HTTP/2 RST Streams in an HTTP/2 connection.	disable
h2-rst-stream-freq-check {enable disable}	Enable to omit the constraint on the maximum occurrences of the HTTP/2 RST Stream per second.	disable
cl-te-coexist-check {enable disable}	Enable to omit the constraint on content-length and transfer-encoding coexist.	disable
inconsistent-cl-check {enable disable}	Enable to omit the constraint on the response has redundant body than the content-length specified.	disable
missing-host-check {enable disable}	Enable to omit the constraint on the Host header is missing.	disable
range-overlapping-check {enable disable}	Enable to omit detecting RangeAmp Overlapping Byte Ranges (OBR) attacks.	disable
multipart-formdata-bad- request-check {enable disable}	Enable to omit detecting whether the multipart request chunk contains the strings "Content-Disposition" and "Name".	disable
h3-bidir-concurrent-stream- check {enable disable}	Enable to omit the constraint on the maximum number of bidirectional concurrent streams in an HTTP/3 connection.	disable
h3-unidir-concurrent- stream-check {enable disable}	Enable to omit the constraint on the maximum number of unidirectional concurrent streams in an HTTP/3 connection.	disable

Example

This example omits header length limits for HTTP requests to `www.example.com` and `192.0.2.1` 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 "192.0.2.1"
    set host-status enable
    set max-HTTP-body-length enable
    set request-file "/login.asp"
next
end
next
end
```

Related topics

- [waf web-protection-profile inline-protection on page 696](#)
- [waf web-protection-profile offline-protection on page 706](#)
- [log trigger-policy on page 96](#)
- [waf HTTP-protocol-parameter-restriction on page 543](#)

waf HTTP-header-security

Use this command to insert special HTTP response headers to protect clients from certain attacks, including XSS, clickjacking, and MIME sniffing attacks. The special HTTP response headers define security policies to client browsers so that the browsers avoid exposure to known vulnerabilities when handling requests.

For more information on HTTP Header Security, see the *FortiWeb Administration Guide*:

<https://docs.fortinet.com/document/fortiweb>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `admingrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf HTTP-header-security
edit "<HTTP-header-security_name>"
    config HTTP-header-security-list
        set name {x-content-type-options | x-frame-options | x-xss-protection | content-
            security-policy | feature-policy | referrer-policy | }
        set value {nosniff | allow-from | deny | sameorigin | sanitizing-mode | block-
            mode}
        set waf HTTP-header-security
        set allow-from-source "<allow-from_str>"
        set request-type {plain | regular}
        set request-file "<request-file_str>"
        set request-status {enable | disable}
    next
end
next
end
```

Variable	Description	Default
"<HTTP-header-security_name>"	Enter of name of an HTTP header security policy. The maximum length is 63 characters.	No default.
request-status {enable disable}	Enable to set a URL Filter.	disable
request-type {plain regular}	Defines the Request URL Type as a simple string (plain) or a regular expression (regular) for the URL Filter. Available only if request-status {enable disable} on page 541 is set to enable.	No default.
request-file "<request-file_str>"	Sets the Request URL for the URL Filter. Available only if request-status {enable disable} on page 541 is set to enable.	No default.
<entry-index_int>	Creates or edits a Secure Header Rule in the selected HTTP Header Security Policy.	No default.
name {x-content-type-options x-frame-options x-xss-protection content-security-policy feature-policy referrer-policy }	Defines the Secure Header Type in the Secure Header Rule. The following options are available: <code>x-frame-options</code>—Prevents browsers from Clickjacking attacks by providing appropriate restrictions on displaying pages in frames. <code>x-content-type-options</code>—Prevents browsers from MIME content-sniffing attacks by disabling the browser's MIME sniffing function. <code>x-xss-protection</code>—Enables a browser's built-in Cross-site scripting (XSS) protection. <code>content-security-policy</code>—FortiWeb adds the Content-Security-Policy HTTP header to a web page, allowing you to specify restrictions on resource types and sources. This prevents certain types of attacks, including XSS and data injection attacks. <code>feature-policy</code>—Provides a mechanism to allow and deny the use of browser features in its own frame, and in content within any <code><iframe></code> elements in the document. For example, fullscreen 'self' https://game.com https://map.example.com;geolocation *; camera 'none' <code>referrer-policy</code>—Controls how much referrer information (sent via the Referer header) should be included with requests. The value of Referrer-Policy can be "no-	No default.

Variable	Description	Default
	referrer", "no-referrer-when-downgrade", "same-origin", "origin", "strict-origin", "origin-when-cross-origin", "strict-origin-when-cross-origin", or "unsafe-url". • <code>permissions-policy</code>—<code>permissions-policy</code> has been introduced in version 7.4.1 to replace <code>feature-policy</code> in alignment with the industry standard. It's recommended to upgrade to permission policy through FortiWeb GUI, because it provides a Validate button to check syntax errors that are introduced by changing from <code>feature-policy</code> to <code>permissions-policy</code>. See "HTTP Security Headers" in <i>FortiWeb Administration Guide</i>.	
value {nosniff allow-from deny sameorigin sanitizing-mode block-mode}	Defines the response according to the defined Secure Header Type. The <code>x-frame-options</code> header can be implemented with one of the following options: • <code>deny</code>—The browser will not allow any frame to be displayed. • <code>sameorigin</code>—The browser will not allow a frame to be displayed unless the page of the frame originated from the same site. • <code>allow-from</code>—The browser will not allow a frame to be displayed unless the page of the frame originated from the specified domain. The <code>x-content-type-options</code> header can be implemented with one option: • <code>nosniff</code>—The browser will not guess any content type that is not explicitly specified when downloading extensions. The <code>x-xss-protection</code> header can be implemented with one of the following options: • <code>sanitizing-mode</code>—The browser will sanitize the malicious scripts when a XSS attack is detected. • <code>block-mode</code>—The browser will block the page when a XSS attack is detected.	No default.
allow-from-source "<allow-from_str>"	Sets the specified domain if the name {x-content-type-options x-frame-options x-xss-protection content-security-policy feature-policy referrer-policy } on page 541 is <code>x-frame-options</code> and the Header Value is set to <code>allow-from</code>.	No default.

Example

This example creates a HTTP header security policy.

```
config waf HTTP-header-security
  edit HTTP_header_security1
    set request-status enable
    set request-type plain
    set request-file "/bWAPP/clickjacking.php"
  config HTTP-header-security-list
    edit 1
      set name x-content-type-options
      set value nosniff
    next
    edit 2
      set name x-frame-options
      set value deny
    next
    edit 3
      set name x-xss-protection
      set value block-mode
    next
  next
end
```

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, enable [waf HTTP-protocol-parameter-restriction on page 543](#) to harden your configuration. To configure the buffer size, see [system advanced on page 233](#).

You can configure each protocol parameter independently with a threat weight, 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 [waf web-protection-profile inline-protection on page 696](#) and [waf web-protection-profile offline-protection on page 706](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf HTTP-protocol-parameter-restriction
edit "<HTTP-constraint_name>"
    set <constraint_name>-check {enable | disable}
    set <constraint_name>-action {alert | alert_deny | block-period | deny_no_log |
        client-id-block-period}
    set <constraint_name>-block-period <seconds_int>
    set <parameter_name>-threat-weight {low | critical | informational | moderate |
        substantial | severe}
    set <constraint_name>-severity {High | Medium | Low | Info}
    set <constraint_name>-trigger "<trigger-policy_name>"
    set Illegal-content-length-check-severity {High| Medium | Low | Info}
    set waf HTTP-protocol-parameter-restriction

next
end
```

Variable	Description	Default
"<HTTP-constraint_name>"	Enter the name of a new or existing HTTP protocol constraint. The maximum length is 63 characters. To display the list of existing constraints, enter: <pre>edit ?</pre> For more information on the description of each constraints, refer to "HTTP/HTTPS protocol constraints" in FortiWeb Administration Guide.	No default.
Illegal-content-length-check-severity {High Medium Low Info}	Set the threat severity in response to invalid Content-Length: header value.	Medium
<constraint_name>-check {enable disable}	Specify whether FortiWeb includes the specified constraint when it applies this set of constraints.	The default values vary depending on different constraints.
<constraint_name>-action {alert alert_deny block-period deny_no_log client-id-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. deny_no_log—Deny a request. Do not	alert

Variable	Description	Default
	generate a log message. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see "system replacemsg" on page 1. <code>block-period</code>—Block subsequent requests from the client's IP address for a number of seconds. Also configure <code><constraint_name>-block-period <seconds_int></code> on page 546. 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 waf x-forwarded-for on page 721). Failure to do so may cause FortiWeb to block all connections when it detects a violation of this type. <code>client-id-block-period</code>—Block subsequent requests from the client id for a number of seconds. Also configure <code><constraint_name>-block-period <seconds_int></code> on page 546. Note: To use this option you must enable Client Management in the server policy. Caution: The action setting is ignored when the value of <code>monitor-mode {enable disable}</code> on page 163 is <code>enable</code>. Note: Logging and/or alert email will occur only if enabled and configured. For details, see log disk on page 66 and log alertMail on page 60. Note: If you select an auto-learning profile with this rule, you should select <code>alert</code>. If the action is <code>alert_deny</code>, 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 details about auto-learning requirements, see "waf web-protection-profile autolearning-profile" on page 1. 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.	

Variable	Description	Default
	For example, for maximum HTTP header length violations, you might type the accompanying setting: <pre>set max-HTTP-header-length-action alert</pre> Note: Available actions vary depending on operating mode and protocol parameter.	
<constraint_name>-severity {High Medium Low Info}	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: <pre>set max-HTTP-header-length-severity High</pre>	Medium
<constraint_name>-trigger "<trigger-policy_name>"	Enter the name of the trigger to apply when this rule is violated (see log trigger-policy on page 96). The maximum length is 63 characters. To display the list of existing trigger policies, enter: <pre>set trigger ?</pre> 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: <pre>set max-HTTP-header-length-trigger trigger-policy1</pre>	No default.
<constraint_name>-block-period <seconds_int>	If action is block-period, type the number of seconds that the connection will be blocked.	600
<parameter_name>-threat-weight {low critical informational moderate substantial severe}	Set the threat weight for an event when FortiWeb detects a violation of a parameter restriction rule. For details, see the <i>FortiWeb Administration Guide</i>: https://docs.fortinet.com/document/fortiweb.	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

- [waf web-protection-profile inline-protection on page 696](#)
- [waf web-protection-profile offline-protection on page 706](#)
- [log trigger-policy on page 96](#)
- [server-policy custom-application application-policy on page 1](#)
- [debug application HTTP on page 1](#)
- [debug flow trace on page 759](#)

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 [client-management {enable | disable} on page 698](#) 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 details, see [Permissions on page 46](#).

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 | deny_no_log}
    set bot-recognition {captcha-enforcement | recaptcha-enforcement | real-browser-
      enforcement | disable}
    set recaptcha <recaptcha_server_name>
    set max-attempt-times <attempts_int>
```

```

set validation-timeout <seconds_int>
set block-period <seconds_int>
set severity {High | Medium | Low | Info}
set trigger-policy "<trigger-policy_name>"
set mobile-app-identification {disabled | mobile-token-validation}
set bot-confirmation {enable | disable}

```

```

next
end

```

Variable	Description	Default
"<rule_name>"	Enter the name of a new or existing rule. The maximum length is 63 characters. To display the list of existing rules, enter: <pre>edit ?</pre>	No default.
access-limit-in-HTTP-session <limit_int>	Enter the maximum number of HTTP connections allowed per second from the same client. The valid range is 0–4,096. To disable the limit, enter 0.	0
action {alert alert_deny block-period deny_no_log}	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. For details, see "system replacemsg" on page 1. block-period—Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int> on page 549. 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 waf x-forwarded-for on page 721). Failure to do so may cause FortiWeb to block all connections when it detects a violation of this type. deny_no_log—Deny a request. Do not generate a log message. Caution: This setting will be ignored if monitor-mode {enable disable} on page 163 is enabled.	alert

Variable	Description	Default
	Note: Logging and/or alert email will occur only if enabled and configured. For details, see log disk on page 66 and log alertMail on page 60. Note: If you select an auto-learning profile with this rule, you should select <code>alert</code>. If the action is <code>alert_deny</code>, 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 details about auto-learning requirements, see "waf web-protection-profile autolearning-profile" on page 1.	
<code>bot-recognition {captcha-enforcement recaptcha-enforcement real-browser-enforcement disable}</code>	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 <seconds_int> on page 549, 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, <code>wget</code>).	<code>disable</code>
<code>recaptcha <recaptcha_server_name></code>	Enter the reCAPTCHA server you have created through user recaptcha-user	No default.
<code>max-attempt-times <attempts_int></code>	If <code>captcha-enforcement</code> is selected for bot-recognition {captcha-enforcement recaptcha-enforcement real-browser-enforcement disable} on page 549, enter the maximum number of attempts that a client may attempt to fulfill a CAPTCHA request. The valid range is 1–5. Available only when <code>captcha-enforcement</code> is selected for <code>bot-recognition</code>.	3
<code>validation-timeout <seconds_int></code>	Specify the maximum amount of time (in seconds) that FortiWeb waits for results from the client for Real Browser Enforcement. The valid range is 5–30.	20
<code>block-period <seconds_int></code>	If action is <code>block-period</code> , type the number of seconds that the connection will be blocked.	600

Variable	Description	Default
	This setting applies only if <code>action</code> is <code>block-period</code> . The valid is from 1 to 10,000 seconds.	
severity {High Medium Low Info}	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	Medium
trigger-policy "<trigger-policy_name>"	Enter the name of the trigger to apply when this rule is violated. For details, see log trigger-policy on page 96 . The maximum length is 63 characters. To display the list of existing trigger policies, enter: <code>set trigger ?</code>	No default.
mobile-app-identification {disabled mobile-token-validation}	Disabled: Disable not to carry out the mobile token verification. Mobile Token Validation: Requires the client to use mobile token for verification. To apply mobile token validation, you must enable Mobile App Identification in waf web-protection-profile inline-protection on page 696	Disabled
bot-confirmation {enable disable}	Enable to choose how to verify users when the rules of bot detection are triggered.	Disabled

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

- [log trigger-policy on page 96](#)
- [waf application-layer-dos-prevention on page 440](#)

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 [waf parameter-validation-rule on page 610](#).

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 [server-policy allow-hosts on page 106](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf input-rule
edit "<input-rule_name>"
    set action {alert | alert_deny | redirect | send_403_forbidden | block-period |
        deny_no_log}
    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 maximum-parameter-number <int>
    set json-parameter-support {enable | disable}
    set severity {High | Medium | Low | Info}
    set trigger "<trigger-policy_name>"
    set block_unknown_parameters {enable | disable}
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>
        set location {url | body}
        set from-json {yes | no}
    next
end
```

```

    next
end

```

Variable	Description	Default
"<input-rule_name>"	Enter the name of a new or existing rule. The maximum length is 63 characters. To display the list of existing rules, enter: edit ?	No default.
action {alert alert_deny redirect send_403_forbidden block-period deny_no_log}	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. For details, see "system replacemsg" on page 1. block-period—Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int> on page 552. 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>" on page 704 and rdt-reason {enable disable} on page 704. 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} on page 163 is enabled. Note: Logging and/or alert email will occur only if enabled and configured. For details, see log disk on page 66 and log alertMail on page 60. 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 details about auto-learning requirements, see "waf web-protection-profile autolearning-profile" on page 1.	alert
block-period <seconds_int>	Enter the number of seconds to block the source IP. The valid range is 1–3,600 seconds.	600

Variable	Description	Default
	This setting applies only if action {alert alert_deny redirect send_403_forbidden block-period deny_no_log} on page 552 is <code>block-period</code> .	
<code>host "<protected-host_name>"</code>	Enter the name of a protected host that the <code>Host :</code> 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 {enable disable} on page 553 is <code>enable</code> .	No default.
<code>host-status {enable disable}</code>	Enable to apply this input rule only to HTTP requests for specific web hosts. Also configure host "<protected-host_name>" on page 553 . Disable to match the input rule based upon the other criteria, such as the URL, but regardless of the <code>Host :</code> field.	<code>disable</code>
<code>request-file "<url_str>"</code>	Depending on your selection in request-type {plain regular} on page 553 , enter either: - The literal URL, such as <code>/index.php</code>, that the HTTP request must contain in order to match the input rule. The URL must begin with a slash (<code>/</code>). - A regular expression, such as <code>^/*.php</code>, matching all and only the URLs to which the input rule should apply. The pattern is not required to begin with a slash (<code>/</code>). However, it must at least match URLs that begin with a slash, such as <code>/index.cfm</code>. Do not include the name of the web host, such as <code>www.example.com</code> , which is configured separately in host "<protected-host_name>" on page 553 . The maximum length is 255 characters. Note: Regular expressions beginning with an exclamation point (<code>!</code>) are not supported. For information on language and regular expression matching, see the <i>FortiWeb Administration Guide</i> : https://docs.fortinet.com/document/fortiweb	No default.
<code>request-type {plain regular}</code>	Select whether request-file "<url_str>" on page 553 will contain a literal URL (<code>plain</code>), or a regular expression designed to match multiple URLs (<code>regular</code>).	<code>plain</code>
<code>maximum-parameter-number <int></code>	Limit the maximum number of parameters in a request; The valid range is from 0 to 1024; When the value is 0, FortiWeb will not check the parameter number.	0
<code>json-parameter-support {enable disable}</code>	Enabled to check the parameters in JSON or not. The JSON data could be in URL or Body. If enabled, the maximum-parameter-number will include JSON parameters.	<code>disable</code>

Variable	Description	Default
severity {High Medium Low Info}	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	Low
trigger "<trigger-policy_name>"	Enter the name of the trigger to apply when this rule is violated. For details, see log trigger-policy on page 96 . The maximum length is 63 characters. To display the list of existing trigger policies, enter: <code>set trigger ?</code>	No default.
block_unknown_parameters {enable disable}	By default, FortiWeb forwards parameters that are not in the configured input rule list to subsequent security modules for further inspection. If you prefer to directly block requests containing unlisted parameters, you can enable this setting.	disable
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999.	No default.
is-essential {yes no}	Select <code>yes</code> if the parameter is required for HTTP requests to this combination of <code>Host :</code> field and URL. Otherwise, select <code>no</code> .	no
max-length <limit_int>	Enter the maximum allowed length of the parameter value. The valid range is 0–1,024. To disable the limit, enter 0.	0
location {url body}	Specify where this parameter is from. The parameter will only be checked when it's from the selected location. You can select both url and body, for example, <code>set location url body</code> .	url body
from-json {yes no}	Specify whether this parameter is from JSON. You must also enable json-parameter-support for this option to function.	no
type-checked {enable disable}	Enable to use predefined or configured data types when validating parameters. Also configure argument-type {custom-data-type data-type regular-expression} on page 554 . Disable to ignore <code>data-type</code> and <code>custom-data-type</code> settings.	disable
argument-type {custom-data-type data-type regular-expression}	Specify the type of argument.	data-type
argument-name-type {plain regular}	Specify one of the following options: <code>plain</code>—<code>argument-name</code> is the name attribute of the parameter's input tag exactly as it appears in the form on the web page. <code>regular</code>—<code>argument-name</code> is a regular expression	plain

Variable	Description	Default
	designed to match the name attribute of the parameter's input tag.	
argument-name "<input_name>"	If argument-name-type {plain regular} on page 554 is <code>plain</code>, specify the name of the input as it appears in the HTTP content, such as <code>username</code>. The maximum length is 63 characters. If <code>argument-name-type</code> is <code>regular</code>, specify a regular expression designed to match the name attribute of the parameter's input tag.	No default.
argument-expression "<regex_pattern>"	Enter 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.	
custom-data-type "<custom-data-type_name>"	Enter the name of a custom data type, if any. The maximum length is 63 characters. To display the list of custom data types, enter: <pre>set custom-data-type ?</pre> This setting applies only if type-checked {enable disable} on page 554 is <code>enable</code>.	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, enter: <pre>set data type ?</pre> For match descriptions of each option, see "server-policy pattern data-type-group" on page 1. Alternatively, configure argument-type {custom-data-type data-type regular-expression} on page 554. This option is ignored if you configure <code>argument-type</code>, 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

- [server-policy allow-hosts on page 106](#)
- [waf parameter-validation-rule on page 610](#)

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 [waf ip-intelligence-exception on page 559](#) 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} on page 702](#) in the server policy's protection profile.

Alternatively, you can block sets of many clients based upon their geographical origin (see [waf geo-block-list on page 511](#)) or manually by specific IPs (see ["server-policy custom-application application-policy" on page 1](#)).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```

config waf ip-intelligence
edit <entry_index>
    set action {alert | alert_deny | redirect | send_403_forbidden | block-period |
        deny_no_log}
    set block-period <seconds_int>
    set category "<category_name>"
    set severity {Low | Medium | High | Info}
end

```

```

    set status {enable | disable}
    set trigger "<trigger-policy_name>"
  next
end

```

Variable	Description	Default
<entry_index>	Enter the index number of the individual entry in the table entry in the table.	No default.
action {alert alert_deny redirect send_403_forbidden block-period deny_no_log}	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. For details, see "system replacemsg" on page 1. block-period—Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int> on page 557. 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>" on page 704 and rdt-reason {enable disable} on page 704. send_403_forbidden—Reply to the client with an HTTP 403 Access Forbidden error message and generate an alert email and/or log message. deny_no_log—Deny a request. Do not generate a log message. Caution: FortiWeb ignores this setting when monitor-mode {enable disable} on page 163 is enabled. Note: Logging and/or alert email will occur only if enabled and configured. For details, see log disk on page 66 and log alertMail on page 60. 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 details about auto-learning requirements, see "waf web-protection-profile autolearning-profile" on page 1.	block-period
block-period <seconds_int>	Enter the number of seconds to block the source IP. The valid range is 1–3,600 seconds.	60

Variable	Description	Default
	This setting applies only if action {alert alert_deny redirect send_403_forbidden block-period deny_no_log} on page 557 is <code>block-period</code> .	
<code>category "<category_name>"</code>	Enter 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 63 characters. Category names vary by the version number of your FortiGuard IRIS package.	No Default.
<code>status {enable disable}</code>	Enable to block clients whose source IP belongs to this category according to the FortiGuard IRIS service.	<code>disable</code>
<code>severity {Low Medium High Info}</code>	When rule violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance uses when a blacklisted IP address attempts to connect to your web servers: • Low • Medium • High • Info	Low
<code>trigger "<trigger-policy_name>"</code>	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. For details, see log trigger-policy on page 96 . The maximum length is 63 characters. To display the list of existing trigger policies, enter: <code>set trigger ?</code>	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"
    set ignore-x-forwarded-for disable
  next
end
```

Related topics

- [waf ip-intelligence-exception on page 559](#)
- [log trigger-policy on page 96](#)
- [waf web-protection-profile inline-protection on page 696](#)
- [waf web-protection-profile offline-protection on page 706](#)
- [waf geo-block-list on page 511](#)
- [server-policy custom-application application-policy on page 1](#)
- [debug flow trace on page 759](#)

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 details, see [Permissions on page 46](#).

Syntax

```
config waf ip-intelligence-exception
  edit <entry_index>
    set status {enable | disable}
    set group-type {ip-string | ip-group}
    set ip-group <name>
    set ip "<client_ipv4>"
  next
end
```

Variable	Description	Default
<entry_index>	Enter the index number of the individual entry in the table entry in the table. The valid range is 1–9,999,999,999,999,999,999.	No default.
status {enable disable}	Enable to exempt clients from IP reputation-based blocking.	disable
group-type {ip-string ip-group}	Select ip-string to enter IP addresses or ranges, or ip-group to reference the IP groups you have created through <code>config server-policy ip-group</code> .	ip-string
ip "<client_ipv4>"	Enter the client's source IP address. Available only when the <code>group-type</code> is <code>ip-string</code> .	No default.

Variable	Description	Default
ip-group <name>	If you have selected ip-group for group-type , then specify the IP Group you have created through <code>config server-policy ip-group</code> . By using the IP group, you can save the effort to type the IP addresses every time you need to re-use them. Available only when the <code>group-type</code> is <code>ip-group</code> .	No default.

Example

See [waf ip-intelligence-ignore-x-forwarded-for](#) on page 560.

Related topics

- [waf ip-intelligence-ignore-x-forwarded-for](#) on page 560

waf ip-intelligence-ignore-x-forwarded-for

Use this command to configure ignoring x-forwarded-for in reputation-based source IP blacklisting.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions](#) on page 46.

Syntax

```
config waf ip-intelligence-ignore-x-forwarded-for
    set ignore-x-forwarded-for {enable | disable}
end
```

Variable	Description	Default
ignore-x-forwarded-for {enable disable}	By default, FortiWeb scans the IP addresses in the X-Forwarded-For header at the HTTP layer. This causes high resource consumption. To enhance the performance, you can enable Ignore X-Forwarded-For so that the IP addresses can be scanned at the TCP layer instead. This avoids HTTP packets being processed unnecessarily.	disable

Related topics

- [waf ip-intelligence](#) on page 556
- [waf ip-intelligence-exception](#) on page 559

- [log trigger-policy](#) on page 96
- [waf web-protection-profile inline-protection](#) on page 696
- [waf web-protection-profile offline-protection](#) on page 706
- [waf geo-block-list](#) on page 511
- [server-policy custom-application application-policy](#) on page 1
- [debug flow trace](#) on page 759

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 [debug flow trace](#) on page 759.
- **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. For details, see [debug flow trace](#) on page 759.
- **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 [waf ip-intelligence-ignore-x-forwarded-for](#) on page 560) or geographical origin (see [waf geo-block-list](#) on page 511).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions](#) on page 46.

Syntax

```
config waf ip-list
edit "<ip-list_name>"
    set severity {Low | Medium | High | Info}
    set action { alert_deny | block-period | deny_no_log}
    set block-period <block_period_int>
    set ignore-x-forwarded-for {enable | disable}
    set trigger-policy "<trigger-policy_name>"
config members
    edit waf ip-list
        set group-type {ip-string | ip-group | IP-external}
        set ip "<client_ip>"
        set ip-group <name>
        set type {trust-ip | black-ip | allow-only-ip }
    next
end
```

```

next
end

```

Variable	Description	Default
"<ip-list_name>"	Enter the name of a new or existing rule. The maximum length is 63 characters. To display the list of existing rules, enter: edit ?	No default.
action { alert_deny block-period deny_no_log }	Select which action FortiWeb will take when it detects a violation of the rule: • <code>alert_deny</code>—Block the request (or reset the connection) and generate an alert and/or log message. • <code>deny_no_log</code>—Block the request (or reset the connection). • <code>block-period</code>—Block subsequent requests from the client for a number of seconds. Also configure <code>block-period</code>. Note: This setting will be ignored if <code>monitor-mode {enable disable}</code> on page 163 is enabled in a server policy.	block-period
block-period <block_period_int>	Enter the number of seconds that you want to block subsequent requests from a client after FortiWeb detects that the client has violated the rule. The valid range is 1–3,600 seconds. This setting is available only if <code>Action</code> is set to <code>block-period</code> .	60
severity {Low Medium High Info}	When rule violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance will use when a blacklisted IP address attempts to connect to your web servers: • Low • Medium • High • info	low
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. The maximum length is 63 characters. For details, see log trigger-policy on page 96 . To display the list of existing trigger policies, enter: set trigger ?	No default.

Variable	Description	Default
ignore-x-forwarded-for {enable disable}	By default, FortiWeb scans the IP addresses in the X-Forwarded-For header at the HTTP layer. This causes high resource consumption. To enhance the performance, you can enable Ignore X-Forwarded-For so that the IP addresses can be scanned at the TCP layer instead. This avoids HTTP packets being processed unnecessarily.	disable
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999,999.	No default.
group-type {ip-string ip-group IP-external}	Select ip-string to enter IP addresses or ranges, or ip-group to reference the IP groups you have created through <code>config server-policy ip-group</code> , or IP-external to reference an external IP address resource you have created through <code>config system external-resource</code> .	ip-string
ip "<client_ip>"	If you have selected ip-string for group-type , then 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). Multiple addresses or ranges should be separated with comma ",". - A range or addresses (e.g. 1.2.3.4,2001::1,1.2.3.4-1.2.3.40,2001::1-2001::100).	No default.
ip-group <name>	If you have selected ip-group for group-type , then specify the IP Group you have created through <code>config server-policy ip-group</code> . By using the IP group, you can save the effort to type the IP addresses every time you need to re-use them.	No default.
type {trust-ip black-ip allow-only-ip }	Select either: black-ip—The source IP address that is distrusted, 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—The source IP address is trusted and allowed to access your web servers, unless it fails a previous scan. For details, see "Sequence of scans" on page 1.	trust-ip

Variable	Description	Default
	By default, if the IP address of a request is neither in the Block IP nor Trust IP list, FortiWeb will pass this request to other scans to decide whether it is allowed to access your web servers. However, you can define the <code>allow-only-ip</code> IP addresses so that such requests can be screened against the Allow Only IPs before they are passed to other scans. <code>allow-only-ip</code>—If the source IP address is a <code>allow-only-ip</code>, it will be passed to other scans to decide whether it's allowed to access your web servers. If not, FortiWeb will take actions according to the trigger policy. If the Allow Only range is empty, then the source IP addresses which are not in the Block IP and Trust IP list will be passed directly to other scans. Requests that are blocked according to the IP Lists will receive a warning message as the HTTP response. The warning message page includes ID: 70007, which is the ID of all attack log messages about requests from blocked IPs.	

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

- [log trigger-policy on page 96](#)
- [waf web-protection-profile inline-protection on page 696](#)
- [waf web-protection-profile offline-protection on page 706](#)
- [waf geo-block-list on page 511](#)
- [waf ip-intelligence-ignore-x-forwarded-for on page 560](#)
- [debug flow trace on page 759](#)

waf json-schema

Use this command to view JSON schema files that have already been uploaded to FortiWeb. You can upload JSON schema files only in the web UI.

You can reference the JSON schema file in a JSON protection rule, or add multiple JSON schema files in a group (Config waf json-schema group) then reference it in JSON 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 details, see [Permissions on page 46](#).

Syntax

```
config waf json-schema file
  edit "<json_schema_file_name>"
    set json-schema-version {Auto-identify | Draft-3| Draft-4| Draft-6| Draft-7| Draft-
      201909| Draft-202012}
  next
end
```

Variable	Description	Default
"<json_schema_file_name>"	To display a list of existing JSON schema files, enter: edit ?	No default.
json-schema-version {Auto-identify Draft-3 Draft-4 Draft-6 Draft-7 Draft-201909 Draft-202012}	Select a JSON schema version. The system will check if schema file is valid against the specified version. If your select <code>Auto-identify</code> , FortiWeb will use the version stated by the '\$schema' key in the JSON Schema file. If '\$schema' is not found or incorrect, then all versions will be checked.	Auto-identify

Related topics

- [waf json-validation rule on page 566](#)
- [waf json-schema group](#)

waf json-schema group

Use this command to group multiple JSON Schemas together. The schema group can be referenced in a JSON Protection Rule. If a request does not match any of the schema in the group it will be considered as a violation.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
Config waf json-schema group
  edit <json-schema-group-name>
    config members
      edit 1
        set member-name <schema-name1>
      next
      edit 2
        set member-name <schema-name2>
      next
    end
  end
end
```

Variable	Description	Default
<json-schema-group-name>	Enter a name for the JSON schema group.	No default.
member-name <schema-name>	select a JSON Schema you have created through <code>config waf json-schema</code> file.	No default.

Related topics

- [waf json-schema](#)
- [waf json-validation rule on page 566](#)

waf json-validation rule

Use this command to create JSON protection rules and configure JSON protection policies.

Syntax

```
config waf json-validation rule
  edit "<json_rule_name>"
    set host-status {enable | disable}
    set host "<host_name_str>"
    set request-type {plain | regular}
    set request-file "<file_str>"
    set Schema-type {single-schema|schema-group}
```

```

set Schema-file <schema-file>
set Schema-group <schema-group>
set action {alert | alert_deny | block-period | redirect | send_403_forbidden |
  deny_no_log}
set block-period <period_int>
set severity {High | Low | Medium | Info}
set trigger "<trigger_policy_name>"
set waf json-validation rule
set json-limits {enable | disable}
set json-data-size "<json-data-size_int>"
set key-size "<key-size_int>"
set key-number "<key-number_int>"
set value-size "<value-size_int>"
set value-number-in-array "<value-number-in-array_int>"
set object-depth "<object-depth_int>"
next
end
config waf json-validation policy
edit "<json_policy_name>"
set enable-signature-detection {enable | disable}
config input-rule-list
edit "<input-rule-list_id>"
set json_input_rule "<json_input_rule_str>"
next
end
next
end

```

Variable	Description	Default
"<json_rule_name>"	Enter a name that can be referenced by other parts of the configuration. You will use the name to select the rule in a JSON protection policy.	No default.
host-status {enable disable}	Enable to compare the JSON rule to the <code>Host:</code> field in the HTTP header. If enabled, also configure <code>host "<host_name_str>"</code> on page 567.	disable
host "<host_name_str>"	Enter the name of a protected host that the <code>Host:</code> field of an HTTP request must match in order for the rule to apply. For details, see server-policy allow-hosts on page 106 .	No default.
request-type {plain regular}	Select whether request-type {plain regular} on page 567 must contain either: <code>plain</code>—The field is a string that the request URL must match exactly. <code>regular</code>—The field is a regular expression that defines a set of matching URLs.	No default.
request-file "<file_str>"	Depending on your selection for request-type {plain regular} on page 567 , enter either: <code>plain</code>—The literal URL, such as <code>/index.php</code>, that the HTTP request must contain in order to match the rule. The URL must begin with a slash (<code>/</code>).	No default.

Variable	Description	Default
	regular—A regular expression, such as <code>^/*\.php</code>, matching the URLs to which the rule should apply. The pattern does not require a slash (/), but it must match URLs that begin with a slash, such as <code>/index.cfm</code>. Do not include the domain name, such as <code>www.example.com</code>, which is configured separately in host "<host_name_str>" on page 567.	
Schema-type {single-schema schema-group}	Select whether to use a single schema file or a schema group. If a request does not match the schema it will be considered as a violation.	single-schema
Schema-file <schema-file>	Select the schema file you have uploaded it through the JSON Schema tab in API Protection > JSON Protection in GUI. Please note the schema file can't be uploaded through CLI.	No default.
Schema-group <schema-group>	Select the schema group you have created through <code>config waf json-schema group</code> . For more information, see waf json-schema group on page 565 .	No default.
action {alert alert_deny block-period redirect send_403_forbidden deny_no_log}	Select one of the following actions that FortiWeb performs when a request violates the rule: 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. For details, see "system replacemsg" on page 1. block-period—Block subsequent requests from the client for a number of seconds. Also configure block-period <period_int> on page 569. redirect—Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. send_403_forbidden—Reply to the client with an HTTP 403 Access Forbidden error message and generate an alert email and/or log message. deny_no_log—Deny a request. Do not generate a log message. Caution: FortiWeb ignores this setting when monitor-mode {enable disable} on page 163 is enabled. Note: Logging and/or alert email will occur only if enabled and configured. For details, see log disk on page 66 and log alertMail on page 60.	alert

Variable	Description	Default
block-period <period_int>	Enter the amount of time (in seconds) that you want to block subsequent requests from a client after FortiWeb detects a rule violation. This setting is available only when action {alert alert_deny block-period redirect send_403_forbidden deny_no_log} on page 568 is block-period. The valid range is 1–3,600 seconds.	600
severity {High Low Medium Info}	When rule violations are recorded in the attack log, each log message contains a Severity Level field. Select which severity level FortiWeb will use when it logs a violation of the rule: - Low - Medium - High - Info	Low
trigger "<trigger_policy_name>"	Enter the name of the trigger, if any, to apply when the rule is violated. The maximum length is 63 characters. For details, see log trigger-policy on page 96 . To display a list of existing triggers, enter: set trigger ?	No default.
json-limits {enable disable}	Enable to define limits for data size, key, and value, etc.	disable
json-data-size "<json-data-size_int>"	Enter the total size of JSON data in the JSON file. The valid range is 0–10240.	1024
key-size "<key-size_int>"	Enter the key size of each object. The valid range is 0–10240. The	64
key-number "<key-number_int>"	Enter the total key number of each JSON file. The valid range is 0–2147483647.	256
value-size "<value-size_int>"	Enter the value size of each key. The valid range is 0–10240.	128
value-number-in-array "<value-number-in-array_int>"	Enter the total value number in an array. The valid range is 0–2147483647.	256
object-depth "<object-depth_int>"	Enter the number of the nested objects. The valid range is 0–2147483647.	32
"<json_policy_name>"	Enter the name of a JSON protection policy. You will use the name to select the policy in other parts of the configuration.	No default.
"<input-rule-list_id>"	Enter the index number of an entry to create or modify a rule for the policy.	No default.
enable-signature-	Enable to scan for matches with attack and data leak	disable

Variable	Description	Default
detection {enable disable}	signatures in JSON data submitted by clients in HTTP requests with Content-Type: values application/json or text/json.	
json_input_rule "<json_input_rule_ str>"	Enter the sequence number of a JSON protection rule to add to the JSON protection policy.	No default.

Example

The below example creates a JSON protection rule and applies the rule to a new JSON protection policy.

```
config waf json-validation rule
  edit "example_rule_name_1"
    set action block-period
    set block-period 3000
    set severity Medium
    set trigger "example_trigger_policy_name"
    set host-status enable
    set host "example_host_name"
    set request-type plain
    set request-file "/index.php"
    set schema-file "example_schema_file_name"
    set json-limits enable
    set json-data-size 1030
    set key-size 100
    set key-number 300
    set value-size 200
    set object-depth 60
  next
end
config waf json-validation policy
  edit "example_policy_name"
    config input-rule-list
      edit "example_rule_1"
        set "example_rule_1"
      next
    end
  next
end
```

Related topics

- [waf json-schema on page 565](#)
- [waf web-protection-profile inline-protection on page 696](#)

waf known-bots

Known Bots protects your websites, mobile applications, and APIs from malicious bots such as DoS, Spam, and Crawler, etc, and known good bots such as known search engines without affecting the flow of critical traffic. This feature identifies and manages a wide range of attacks from automated tools no matter where these applications or APIs are deployed.

Use these commands to configure known bots prevention.

Syntax

```
config waf known-bots
edit "known-bots_rule_name"
    set crawler-action {alert | redirect | deny_no_log | alert_deny | block_period | send_
        HTTP_response}
    set crawler-block-period <period_int>
    set crawler-severity {High | Medium | Low | Info}
    set crawler-status {enable | disable}
    set crawler-threat-weight {low | critical | informational | moderate | substantial |
        severe}
    set crawler-trigger <trigger_policy_name>
    set dos-action {alert | redirect | deny_no_log | alert_deny | block_period | send_
        HTTP_response}
    set dos-block-period <period_int>
    set dos-severity {High | Medium | Low | Info}
    set dos-status {enable | disable}
    set dos-threat-weight {low | critical | informational | moderate | substantial |
        severe}
    set dos-trigger <trigger_policy_name>
    set known-engines-action {alert | bypass | redirect | deny_no_log | alert_deny |
        block_period | send_HTTP_response}
    set known-engines-block-period <period_int>
    set known-engines-severity {High | Medium | Low | Info}
    set known-engines-status {enable | disable}
    set known-engines-threat-weight {low | critical | informational | moderate |
        substantial | severe}
    set known-engines-trigger <trigger_policy_name>
    set scanner-action {alert | redirect | deny_no_log | alert_deny | block_period | send_
        HTTP_response}
    set scanner-block-period <period_int>
    set scanner-severity {High | Medium | Low | Info}
    set scanner-status {enable | disable}
    set scanner-threat-weight {low | critical | informational | moderate | substantial |
        severe}
    set scanner-trigger <trigger_policy_name>
    set spam-action {alert | redirect | deny_no_log | alert_deny | block_period | send_
        HTTP_response}
    set spam-block-period <period_int>
    set spam-severity {High | Medium | Low | Info}
    set spam-status {enable | disable}
    set spam-threat-weight {low | critical | informational | moderate | substantial |
        severe}
    set spam-trigger <trigger_policy_name>
```

```

set trojan-action {alert | redirect | deny_no_log | alert_deny | block_period | send_
    HTTP_response}
set trojan-block-period <period_int>
set trojan-severity {High | Medium | Low | Info}
set trojan-status {enable | disable}
set trojan-threat-weight {low | critical | informational | moderate | substantial |
    severe}
set trojan-trigger <trigger_policy_name>
config malicious-bot-disable-list
    edit "<malicious-bot-disable-list_name>"
    next
end
config known-good-bots-disable-list
    edit "<known-good-bots-disable-list_name>"
    next
end
next
end

```

Variable	Description	Default
"known-bots_rule_name"	Enter a name for the known bots rule name.	No default
crawler-action {alert redirect deny_no_log alert_deny block_period send_HTTP_response}	Select the action FortiWeb takes when this type attack is identified. • 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. For details, see system replacemsg-image on page 366. • deny_no_log—Block the request (or reset the connection). • redirect—Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. • block_period—Block subsequent requests from the client for a number of	alert_deny

Variable	Description	Default
	seconds. Also configure crawler-block-period <period_int> on page 573. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see system replacemsg-image on page 366. <code>send_HTTP_response</code>—Block and reply to the client with an HTTP error message and generate an alert email and/or log message. Note: Logging and/or alert email will occur only if enabled and configured. See log on page 784 and log alertMail on page 60.	
<code>crawler-block-period <period_int></code>	Enter the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects this type attack.	600
<code>crawler-severity {High Medium Low Info}</code>	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs an attack: - High - Medium - Low - Info	High
<code>crawler-status {enable disable}</code>	Enable or disable the bot type detection for this rule.	enable
<code>crawler-threat-weight {low critical informational moderate substantial severe}</code>	Set the threat weight for crawler bot attack.	moderate
<code>crawler-trigger <trigger_policy_name></code>	Enter the name of the trigger to apply when this policy is violated. For details, see log trigger-policy on page 96.	No default

Variable	Description	Default
	To display the list of existing triggers, enter: <code>set trigger ?</code>	
<code>dos-action {alert redirect deny_no_log alert_deny block_period send_HTTP_response}</code>	Select the action FortiWeb takes when this type attack is identified. <code>alert</code>—Accept the request and generate an alert email and/or log message. <code>alert_deny</code>—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. For details, see system replacemsg-image on page 366. <code>deny_no_log</code>—Block the request (or reset the connection). <code>redirect</code>—Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. <code>block_period</code>—Block subsequent requests from the client for a number of seconds. Also configure <code>dos-block-period <period_int></code> on page 575. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see system replacemsg-image on page 366. <code>send_HTTP_response</code>—Block and reply to the client with an HTTP error message and generate an alert email and/or log message.	<code>alert_deny</code>

Variable	Description	Default
	Note: Logging and/or alert email will occur only if enabled and configured. See log on page 784 and log alertMail on page 60 .	
dos-block-period <period_int>	Enter the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects this type attack.	600
dos-severity {High Medium Low Info}	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs an attack: • High • Medium • Low • Info	High
dos-status {enable disable}	Enable or disable the bot type detection for this rule.	enable
dos-threat-weight {low critical informational moderate substantial severe}	Set the threat weight for DoS bot attack.	critical
dos-trigger <trigger_policy_name>	Enter the name of the trigger to apply when this policy is violated. For details, see log trigger-policy on page 96 . To display the list of existing triggers, enter: <pre>set trigger ?</pre>	No default
known-engines-action {alert bypass redirect deny_no_log alert_deny block_period send_HTTP_response}	Select the action FortiWeb takes when this type attack is identified. • <code>alert</code>—Accept the request and generate an alert email and/or log message. • <code>bypass</code>—allow the request. • <code>alert_deny</code>—Block the request (or reset the connection) and generate an alert email and/or log message.	bypass

Variable	Description	Default
	You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see system replacemsg-image on page 366. • <code>deny_no_log</code>—Block the request (or reset the connection). • <code>redirect</code>—Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. • <code>block_period</code>—Block subsequent requests from the client for a number of seconds. Also configure known-engines-block-period <period_int> on page 576. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see system replacemsg-image on page 366. • <code>send_HTTP_response</code>—Block and reply to the client with an HTTP error message and generate an alert email and/or log message. Note: Logging and/or alert email will occur only if enabled and configured. See log on page 784 and log alertMail on page 60.	
<code>known-engines-block-period <period_int></code>	Enter the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects this type attack.	600

Variable	Description	Default
known-engines-severity {High Medium Low Info}	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs an attack: • High • Medium • Low • Info	Info
known-engines-status {enable disable}	Enable or disable the bot type detection for this rule.	enable
known-engines-threat-weight {low critical informational moderate substantial severe}	Set the threat weight for known search engines attack.	informational
known-engines-trigger <trigger_policy_name>	Enter the name of the trigger to apply when this policy is violated. For details, see log trigger-policy on page 96 . To display the list of existing triggers, enter: set trigger ?	No default
scanner-action {alert redirect deny_no_log alert_deny block_period send_HTTP_response}	Select the action FortiWeb takes when this type attack is identified. • <code>alert</code>—Accept the request and generate an alert email and/or log message. • <code>alert_deny</code>—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. For details, see system replacemsg-image on page 366. • <code>deny_no_log</code>—Block the request (or reset the connection). • <code>redirect</code>—Redirect the	alert_deny

Variable	Description	Default
	request to the URL that you specify in the protection profile and generate an alert email and/or log message. <code>block_period</code>—Block subsequent requests from the client for a number of seconds. Also configure scanner-block-period <period_int> on page 578. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see system replacemsg-image on page 366. <code>send_HTTP_response</code>—Block and reply to the client with an HTTP error message and generate an alert email and/or log message. Note: Logging and/or alert email will occur only if enabled and configured. See log on page 784 and log alertMail on page 60.	
<code>scanner-block-period <period_int></code>	Enter the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects this type attack.	600
<code>scanner-severity {High Medium Low Info}</code>	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs an attack: - High - Medium - Low - Info	High
<code>scanner-status {enable disable}</code>	Enable or disable the bot type detection for this rule.	enable

Variable	Description	Default
scanner-threat-weight {low critical informational moderate substantial severe}	Set the threat weight for scanner bot attack.	critical
scanner-trigger <trigger_policy_name>	Enter the name of the trigger to apply when this policy is violated. For details, see log trigger-policy on page 96 . To display the list of existing triggers, enter: set trigger ?	No default
spam-action {alert redirect deny_no_log alert_deny block_period send_HTTP_response}	Select the action FortiWeb takes when this type attack is identified. • 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. For details, see system replacemsg-image on page 366. • deny_no_log—Block the request (or reset the connection). • redirect—Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. • block_period—Block subsequent requests from the client for a number of seconds. Also configure spam-block-period <period_int> on page 580. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see system replacemsg-image on	alert_deny

Variable	Description	Default
	page 366. <code>send_HTTP_response</code>—Block and reply to the client with an HTTP error message and generate an alert email and/or log message. Note: Logging and/or alert email will occur only if enabled and configured. See log on page 784 and log alertMail on page 60.	
spam-block-period <period_int>	Enter the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects this type attack.	600
spam-severity {High Medium Low Info}	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs an attack: - High - Medium - Low - Info	High
spam-status {enable disable}	Enable or disable the bot type detection for this rule.	enable
spam-threat-weight {low critical informational moderate substantial severe}	Set the threat weight for scanner bot attack.	critical
spam-trigger <trigger_policy_name>	Enter the name of the trigger to apply when this policy is violated. For details, see log trigger-policy on page 96. To display the list of existing triggers, enter: <pre>set trigger ?</pre>	No default
trojan-action {alert redirect deny_no_log alert_deny block_period send_HTTP_response}	Select the action FortiWeb takes when this type attack is identified. <code>alert</code>—Accept the request and generate an alert email	alert_deny

Variable	Description	Default
	and/or log message. • <code>alert_deny</code>—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. For details, see system replacemsg-image on page 366. • <code>deny_no_log</code>—Block the request (or reset the connection). • <code>redirect</code>—Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. • <code>block_period</code>—Block subsequent requests from the client for a number of seconds. Also configure trojan-block-period <period_int> on page 581. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see system replacemsg-image on page 366. • <code>send_HTTP_response</code>—Block and reply to the client with an HTTP error message and generate an alert email and/or log message. Note: Logging and/or alert email will occur only if enabled and configured. See log on page 784 and log alertMail on page 60.	
<code>trojan-block-period <period_int></code>	Enter the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects this type attack.	600

Variable	Description	Default
trojan-severity {High Medium Low Info}	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs an attack: - High - Medium - Low - Info	High
trojan-status {enable disable}	Enable or disable the bot type detection for this rule.	enable
trojan-threat-weight {low critical informational moderate substantial severe}	Set the threat weight for Trojan bot attack.	critical
trojan-trigger <trigger_policy_name>	Enter the name of the trigger to apply when this policy is violated. For details, see log trigger-policy on page 96 . To display the list of existing triggers, enter: <code>set trigger ?</code>	No default
"<malicious-bot-disable-list_name>"	Select the malicious bot list not to be scanned.	No default
"<known-good-bots-disable-list_name>"	Select the known good bots list not to be scanned.	No default

Related Topics

- [waf web-protection-profile inline-protection on page 696](#)

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 and include that policy in an inline protection profile. For details, see [waf application-layer-dos-prevention on page 440](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

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 | deny_no_log}
set bot-recognition {captcha-enforcement | recaptcha-enforcement | real-browser-
    enforcement | disable}
set recaptcha <recaptcha_server_name>
set max-attempt-times <attempts_int>
set block-period <seconds_int>
set severity {High | Medium | Low | Info}
set trigger-policy "<trigger-policy_name>"
set validation-timeout <seconds_int>
set mobile-app-identification {disabled | mobile-token-validation}
set bot-confirmation {enable | disable}
next
end
```

Variable	Description	Default
"<rule_name>"	Enter the name of a new or existing rule. The maximum length is 63 characters. To display the list of existing rules, enter: <code>edit ?</code>	No default.
access-limit-standalone-ip <limit_int>	Enter the maximum number of HTTP requests allowed per second from any source IP address representing a single client. The valid range is 0–65,536. To disable the limit, enter 0.	0
access-limit-share-ip <limit_int>	Enter 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 0–65,536. To disable the limit, enter 0.	0
action {alert alert_deny block-period deny_no_log}	Select one of the following actions that the FortiWeb appliance will perform when the count exceeds either threshold limit: <code>alert</code>—Accept the request and generate an alert email and/or log message. <code>alert_deny</code>—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. For	alert

Variable	Description	Default
	details, see "system replacemsg" on page 1. <code>block-period</code>—Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int> on page 585. 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. Failure to do so may cause FortiWeb to block all connections when it detects a violation of this type. For details, see waf x-forwarded-for on page 721. <code>deny_no_log</code>—Deny a request. Do not generate a log message. Caution: This setting will be ignored if monitor-mode {enable disable} on page 163 is enabled. Note: Logging and/or alert email will occur only if enabled and configured. For details, see log disk on page 66 and log alertMail on page 60. Note: If you select an auto-learning profile with this rule, you should select <code>alert</code>. If the <code>action</code> is <code>alert_deny</code>, 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 details about auto-learning requirements, see "waf web-protection-profile autolearning-profile" on page 1.	
<code>bot-recognition {captcha-enforcement recaptcha-enforcement real-browser-enforcement disable}</code>	Select between: <code>captcha-enforcement</code>—Requires the client to successfully fulfill a CAPTCHA request. If the client cannot successfully fulfill the request within the max-attempt-times <attempts_int> on page 585, or doesn't fulfill the request within the validation-timeout <seconds_int> on page 585, FortiWeb applies the <code>action</code> and sends the CAPTCHA block page. <code>recaptcha-enforcement</code>—Requires the client to successfully fulfill a reCAPTCHA request. If the client cannot successfully fulfill the request within the validation-timeout <seconds_int> on page 585, FortiWeb applies the <code>action</code> and sends the reCAPTCHA block page. <code>real-browser-enforcement</code>—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 <code>validation-timeout</code>, FortiWeb applies the specified action. If	<code>disable</code>

Variable	Description	Default
	the client appears to be a web browser, FortiWeb allows the client to violate the rule. <code>disable</code>—Not to carry out the real browser verification.	
<code>recaptcha <recaptcha_server_name></code>	Enter the reCAPTCHA server you have created through user recaptcha-user	No default.
<code>max-attempt-times <attempts_int></code>	If <code>captcha-enforcement</code> is selected for bot-recognition, enter the maximum number of attempts that a client may attempt to fulfill a CAPTCHA request. The valid range is 1–5. Available only when <code>captcha-enforcement</code> is selected for bot-recognition.	3
<code>block-period <seconds_int></code>	Enter the number of seconds to block access to the client. This applies only when the action {alert alert_deny block-period deny_no_log} on page 583 setting is <code>block-period</code>. The valid range is 1–10,000 seconds.	600
<code>severity {High Medium Low Info}</code>	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	Medium
<code>trigger-policy "<trigger-policy_name>"</code>	Enter the name of the trigger to apply when this rule is violated. For details, see log trigger-policy on page 96. The maximum length is 63 characters. To display the list of existing trigger policies, enter: <pre>set trigger ?</pre>	No default.
<code>validation-timeout <seconds_int></code>	Enter the maximum amount of time (in seconds) that FortiWeb waits for results from the client for bot-recognition. The valid range is 5–30.	20
<code>mobile-app-identification {disabled mobile-token-validation}</code>	Disabled: Disable not to carry out the mobile token verification. Mobile Token Validation: Requires the client to use mobile token for verification. To apply mobile token validation, you must enable Mobile App Identification in waf web-protection-profile inline-protection on page 696	Disabled
<code>bot-confirmation {enable disable}</code>	Enable to choose how to verify users when the rules of bot detection are triggered.	Disabled

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

- [log trigger-policy on page 96](#)
- [waf application-layer-dos-prevention on page 440](#)
- [waf layer4-connection-flood-check-rule on page 586](#)

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 command is similar to [waf HTTP-connection-flood-check-rule on page 532](#). 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 [server-policy policy on page 150](#). 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 and include that policy in an inline protection profile. For details, see [waf application-layer-dos-prevention on page 440](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf layer4-connection-flood-check-rule
```

```

edit "<rule_name>"
  set layer4-connection-threshold <limit_int>
  set action {alert | alert_deny | block-period | deny_no_log}
  set block-period <seconds_int>
  set severity {High | Medium | Low | Info}
  set trigger-policy "<trigger-policy_name>"
next
end

```

Variable	Description	Default
"<rule_name>"	Enter the name of a new or existing rule. The maximum length is 63 characters. To display the list of existing rules, enter: <pre>edit ?</pre>	No default.
layer4-connection-threshold <limit_int>	Enter the maximum number of TCP connections allowed from the same IP address. The valid range is 0–65,536.	0
action {alert alert_deny block-period deny_no_log}	Select one of the following actions that the FortiWeb appliance will perform when the count exceeds the rate limit: <code>alert</code>—Accept the connection and generate an alert email and/or log message. <code>alert_deny</code>—Block the connection and generate an alert email and/or log message. <code>block-period</code>—Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int> on page 587. <code>deny_no_log</code>—Deny a request. Do not generate a log message. Caution: This setting will be ignored if monitor-mode {enable disable} on page 163 is enabled. Note: Logging and/or alert email will occur only if enabled and configured. For details, see log disk on page 66 and log alertMail on page 60. Note: If an auto-learning profile will be selected in the policy with Offline Protection profiles that use this rule, you should select <code>alert</code>. If the action is <code>alert_deny</code>, the FortiWeb appliance will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For details about auto-learning requirements, see "waf web-protection-profile autolearning-profile" on page 1.	alert
block-period <seconds_int>	Enter the length of time (in seconds) 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 1–3,600.	600

Variable	Description	Default
severity {High Medium Low Info}	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	Medium
trigger-policy "<trigger-policy_name>"	Enter the name of the trigger to apply when this rule is violated. For details, see log trigger-policy on page 96 . The maximum length is 63 characters. To display the list of existing trigger policies, enter: 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

- [log trigger-policy on page 96](#)
- [waf application-layer-dos-prevention on page 440](#)
- [waf layer4-access-limit-rule on page 582](#)

waf link-cloaking link-cloaking-rule

Use this command to prevent web pages in your application from being scanned by web crawlers and scanning software. Link cloaking transforms the fixed links to automatically generated links by JavaScript codes. For example, `<a href="https://example/login">` will be transformed to `href="https://jisc.waasonline.com/index/login"`, where the link tag `<a>` is cut off so that the crawlers can't recognize it. When the link is loaded in the client's browser, the lost code will be added back automatically.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf link-cloaking link-cloaking-rule
  edit <link_cloaking_name>
    set host-status {enable | disable}
    set host <name>
    set url-type {plain | regular}
```

```

set url-pattern "<url_string>"
config exceptions
  edit 1
    set url-type
    set url-pattern
  next
end
next
end

```

Variable	Description	Default
<link_cloaking_name>	Enter a name for the rule.	no default
host-status {enable disable}	Enable to require that the <code>Host :</code> field of the HTTP request matches a protected host name entry in order to match the link cloaking rule.	disable
host <name>	Enter the protected host names entry (either a web host name or a IP address) that the <code>Host :</code> field of the HTTP request must be in to match the rule.	no default
url-type {plain regular}	Enter to select between: <code>plain</code>—A simple string; a string of text that contains a literal URL. <code>regular</code>—A regular expression; a string of text that defines a search pattern for a URL that may come in many variations.	plain
url-pattern "<url_string>"	Depending on the <code>url-type</code> , enter either: plain—The literal URL, such as <code>/index.php</code>, that the HTTP request must contain in order to match the rule. The URL must begin with a slash (<code>/</code>). regular—A regular expression, such as <code>^/*\.php</code>, matching the URLs to which the rule should apply. The pattern does not require a slash (<code>/</code>), but it must match URLs that begin with a slash, such as <code>/index.cfm</code>. Do not include the domain name, such as <code>www.example.com</code> , which is configured separately in <code>[bot-detection-exception-list] <No.> host <string></code> .	no default
exceptions	If you want to exclude certain links from Link Cloaking, type a literal URL or use regular expression to match multiple URLs.	no default

waf link-cloaking link-cloaking-policy

Use this command to add link cloaking rule to link cloaking policy.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf link-cloaking link-cloaking-policy
  edit <link_cloaking_policy_name>
    config rule-list
      edit <index>
        set rule <name> on page 590
      next
    end
  next
end
```

Variable	Description	Default
<link_cloaking_policy_name>	Enter a name for the policy.	no default
rule <name>	Enter the name of the link cloaking rule to be added in the policy.	no default

waf machine-learning url-replacer-rule/policy

Use this command to enable the machine learning feature and configure its settings.

Syntax

```
config waf machine-learning url-replacer-rule
  edit url-replacer-rule_name
    set type {pre-defined | custom-defined}
    set app-type {jsp | owa-2003}
    set url-replacer-policy_name
    set url "<url_str>"
    set new-url "<new-url_str>"
    set param "<param_str>"
    set new-param "<new-param_str>"
  next
end
config waf machine-learning url-replacer-policy
  edit url-replacer-policy_name
    config rule list
      edit rule-id "<rule_id>"
        set type URL_Replacer
        set plugin-name "<plugin-name_str>"
      next
    end
  next
end
```

Variable	Description	Default
url-replacer-rule_name	Specify a unique name that can be referenced by other parts of the configuration. The name can be up to 63 characters long with no space or special character.	No default.
type {pre-defined custom-defined}	Select either of the following: - Predefined—Use one of the predefined URL replacers which can be selected from the Application Type below. - Custom-Defined—Define your own URL replacer by configuring the URL Path, New URL, Param Change, and New Param fields below.	No default.
app-type {jsp owa-2003}	If you have selected Predefined in the Type field above, then you must click the down arrow and select either of the following from the list menu: - JSP—Use the URL replacer designed for Java server pages (JSP) web applications, where parameters are often separated by semi-colon (;). - OWA 2003— Use the URL replacer designed for default URLs in Microsoft Outlook Web App (OWA), where user name and directory parameters are often embedded within the URL, as illustrated below: <pre>(^/public/)(.*) (^/exchange/)([^\s/+]*) (([/\s/+])(. *))*</pre> These two application types are predefined URL	No default.

Variable	Description	Default
	interpreter plug-ins used by popular web applications.	
url "<url_str>"	Enter a regular expression, such as <code>(^[^/]+)/(.*)</code>, matching all and only the URLs to which the URL replacer should apply. The URL path can be up to 255 characters long. The pattern does not require a backslash (<code>/</code>). However, it must at least match URLs that begin with a backslash as they appear in the HTTP header, such as <code>/index.html</code>. Do not include the domain name, such as <code>www.example.com</code>.	No default.
new-url "<new-url_str>"	Enter either a literal URL, such as <code>/index.html</code> , or a regular expression with a back-reference (such as <code>\$1</code>) defining how the URL will be interpreted. The new URL can be up to 255 characters long.	No default.
param "<param_str>"	Enter either the parameter's literal value, such as <code>user1</code> , or a back-reference (such as <code>\$0</code>) defining how the value will be interpreted.	No default.
new-param "<new-param_str>"	Type either the parameter's literal name, such as <code>username</code> , or a backreference (such as <code>\$2</code>) defining how the parameter's name will be interpreted in the auto-learning report. You can use up to 255 characters.	No default.
url-replacer-policy_name	Specify a unique name that can be referenced by other parts of the configuration. The name can be up to 63 characters long with no space or special character.	No default.
rule-id "<rule_id>"	Select the sequence number of the URL Replacer Rules	No default.

Variable	Description	Default
type URL_Replacer	Select the type URL_Replacer.	No default.
plugin-name "<plugin-name_str>"	Enter the plugin name.	No default.

Related Topic

- [waf machine-learning-policy](#)

waf machine-learning-policy

How an anomaly detection model is built?

FortiWeb uses machine learning model to analyze the parameters in your domain and decide whether the value of the parameter is legitimate or not. The machine learning model is built upon vast amount of parameter value samples collected from the real requests to the domain.

When a sample is collected, the system generalized it into a pattern. For example, "abcd_123@abc.com" and "abcdefgcedf_12345678@efg.com" will both be generalized to the pattern "A_N@A.A". The anomaly detection model is built based on the patterns, not the raw samples.

FortiWeb analyzes the characteristics of the patterns and builds an initial model when 400 samples are collected. The system runs the initial model to detect anomalies, while it keeps collecting more samples to refine it.

Once the number of samples accumulates to 1200, the system will evaluate whether the patterns vary largely since the initial model is built:

- If there are very few patterns generalized, it indicates the patterns are stable. The system will switch the initial model to a standard model.
- If a lot of new patterns keeps coming in, the system will continue collecting more samples to cover as much patterns as possible. It won't switch to standard model until the patterns become stable.

The standard model is much more reliable and accurate compared with the initial model. However, your domains may change as new URLs are added and existing parameters provide new functions. This means the mathematical model of the same parameter might be different from what FortiWeb originally observed. To keep the machine learning model up to date, FortiWeb continues collecting new samples to update it, where the outdated patterns are discarded and new patterns are introduced.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf machine-learning-policy
edit <machine-learning-policy_id>
    set start-min-count <start-min-count_int>
    set renovate-short-time <renovate-short-time_int>
```

```

set waf machine-learning-policy
set switch-min-count <switch-min-count_int>
set switch-percent <switch-percent_int>
set sliding-win-time <sliding-win-time_int>
set sub-window-size <sub-window-size_int>
set waf machine-learning-policy
set denoise-percent <denoise-percent_int>
set denoise-threshold <denoise-threshold_int>
set sample-limit-by-ip <sample-limit-by-ip_int>
set svm-model {xss | sql-injection | code-injection | command-injection | lfi-rfi
    | common-injection | remote-exploits}
set svm-sensitivity-level {1 | 2 | 3 | 4}
set anomaly-detection-threshold <anomaly-detection-threshold_int>
set waf machine-learning-policy
set action-anomaly {alert | alert_deny | block-period}
set block-period-anomaly <block-period_int>
set severity-definitely {High | Info | Low | Medium}
set trigger-definitely <policy_name>
set status {enable | disable}
set ip-expire-intval <int>
set ip-expire-cnts <int>
set ip-argcount-limit {enable | disable}
set ip-list-type {Trust | Black}
set url-replacer-policy <policy_name>
set threat-model {enable | disable} on page 596
set parameters-limit-per-conn {enable | disable}
set anomaly-detection-threshold <anomaly-detection-threshold_int>
config allow-domain-name
    edit <allow-domain-name_id>
        set domain-name <domain-name_str>
        set domain-index <domain-index_id>
        set hmm-probability-sample-length-check {enable | disable}
        set sample-length-threshold <int>
        set hmm-probability-threshold <int>
        set character-set {AUTO | ISO-8859-1 | ISO-8859-2 | ISO-8859-3 | ISO-8859-4 |
            ISO-8859-5 | ISO-8859-6 | ISO-8859-7 | ISO-8859-8 | ISO-8859-9 | ISO-
            8859-10 | ISO-8859-15 | GB2312 | BIG5 | ISO-2022-JP | ISO-2022-JP-2 |
            Shift-JIS | ISO-2022-KR | UTF-8}
    next
end
config source-ip-list
    edit <source-ip-list_id>
        set <ip>
    next
end
next
end

```

Variable	Description	Default
<machine-learning-policy_id>	Enter the ID of the machine learning policy. It's the number displayed in the "#" column of the machine learning policy table on the Machine Learning Policy page. The valid range is 0–65535.	No default

Variable	Description	Default
start-min-count <start-min-count_int>	An initial model will be built if the sample count reaches <code>start-min-count</code> .	400
renovate-short-time <renovate-short-time_int>	The system keeps updating the initial model. <code>renovate-short-time</code> defines how frequently FortiWeb updates the model if new patterns keep coming in. The valid range is 15 to 1440.	15 (minutes)
renovate-long-time <renovate-long-time_int>	<code>renovate-long-time</code> defines how frequently FortiWeb updates the initial model even if no new pattern is generalized out of the samples collected in the past hours. For example, assuming you set the value to 8 (hours), and in the past 8 hours there isn't any new pattern, FortiWeb will update the model every 8 hours anyway. The valid range is 8 to 720.	8 (hours)
switch-min-count <switch-min-count_int>	When the number of samples reaches <code>switch-min-count</code> , FortiWeb will evaluate whether to build a standard model. The valid range is 800 to 3000.	1200
switch-percent <switch-percent_int>	$\text{switch-percent} = \frac{\text{the number of generalized patterns}}{\text{the number of raw samples}} * 100 (\%)$ When the <code>switch-percent</code> is smaller than the value you set, FortiWeb switches the initial model to the standard model. The valid range is 2 to 20.	5 (%)
sliding-win-time <sliding-win-time_int>	After the standard model is built, FortiWeb keeps updating it according to the newest samples so that the model can be up to date even when your domain changes, such as when new URLs are added and existing parameters provide new functions. <code>sliding-win-time</code> defines how frequently FortiWeb updates the standard model. The valid range is 15-1440 in minutes.	15 (minutes)
sub-window-size <sub-window-size_int>	If there isn't any new pattern generalized during the <code>sliding-win-time</code> , the system will not update the standard model until the number of samples reaches the <code>sub-window-size</code> . The <code>sub-window-size</code> can be set as 50 or 100.	50
sub-window-count <sub-window-count_int>	Every time the standard model is updated, FortiWeb counts it as one <code>sub-window-count</code> . If a certain times of <code>sub-window-count</code> have passed and there isn't any sample coming in for a pattern, FortiWeb considers this pattern outdated, and will discard it. The <code>sub-window-count</code> can be set as 20, 40, or 80. For example, assuming the <code>sub-window-count</code> is 20, then FortiWeb will discard a pattern if there isn't any sample collected for it after the model has been updated for 20 times consecutively.	40

Variable	Description	Default
denoise-percent <denoise-percent_int>	It's important to reduce the noisy samples in order to build an accurate model. During the sample collecting period, the system ranks all the samples by their probabilities. The ones with the lowest probabilities will be selected as noisy reduction samples, and will be filtered further with <code>denoise-threshold</code> to determine whether it is a noise. For example, if you set <code>denoise-percent</code> to 3, then the 3% samples with the lowest probabilities will be selected as noisy reduction samples. The valid range is 1 to 10.	3 (%)
denoise-threshold <denoise-threshold_int>	The system uses the following formula to determine whether the noisy reduction samples are indeed noises: The probability of the sample $> \mu + \text{denoise-threshold} * \sigma$. μ is the average probabilities of the noisy samples. σ is the denoise standard deviation. Assume there is a circle with most of the samples crowded in the center, and several samples scattered around the edge of the circle. If the probability of the sample is larger than the value of "μ + the strictness level * σ", it means this sample is scattered far away from the center cluster. It indicates this sample might be an anomaly, i.e. a noise. If you set the <code>denoise-threshold</code> larger, it means the system tolerates a longer distance that a sample is scattered from the center cluster. In this way, less samples will be treated as noises. If you want to identify more samples as noises, set the <code>denoise-threshold</code> smaller. The valid range is 1 to 10.	2
threat-model {enable disable}	Enable to scan anomalies to verify whether they are attacks. It provides a method to check whether an anomaly is a real attack by the trained Support Vector Machine Model.	enable
svm-model {xss sql-injection code-injection command-injection lfi-rfi common-injection remote-exploits}	Enable or disable threat models for different types of threats such as cross-site scripting, SQL injection and code injection. Currently, seven trained Support Vector Machine Model are provided for seven attack types.	enable
svm-sensitivity-level {1 2 3 4}	Increasing the security level introduces more conditions that a request must meet to pass the scan. For example, a request that successfully passes at level 1 might be flagged as an anomaly at level 4 due to stricter criteria. While higher security levels enhance protection by enforcing more rigorous requirements, they also increase the risk of mistakenly blocking legitimate traffic.	1

Variable	Description	Default
	This command is a replacement of the old command <code>svm-type {standard extended}</code> since 7.6.0. The 'standard' option in the old command now corresponds to sensitivity Level 1, and 'extended' maps to Level 4.	
anomaly-detection-threshold <anomaly-detection-threshold_int>	The value of the anomaly-detection-threshold ranges from 1 to 10. The system uses the following formula to calculate the anomaly threshold: The probability of the anomaly > μ + the strictness level * σ If the probability of the sample is larger than the value of "μ + the strictness level * σ", this sample will be identified as anomaly. μ and σ are calculated based on the probabilities of all the samples collected during the sample collection period, where μ is the average value of all the parameters' probabilities, σ is the standard deviation. They are fixed values. So, the value of "μ + the strictness level * σ" varies with the strictness level you set. The smaller the value of the strictness level is, the more strict the anomaly detection model will be. This option sets a global value for all the parameters. If you want to adjust the strictness level for a specific parameter, See Manage anomaly-detecting settings.	0.1
parameters-limit-per-conn {enable disable}	Enable to avoid collecting samples solely for the parameters in the same connection. The anomaly detection will be more effective if the system builds machine learning models for parameters diversely distributed in different connections.	enable
action-anomaly {alert alert_deny block-period}	Choose the action FortiWeb takes when definite attack is verified. alert—Accepts the connection and generates an alert email and/or log message. alert_deny—Blocks the request (or resets the connection) and generates an alert and/or log message. block-period—Blocks the request for a certain period of time.	alert_deny
block-period-anomaly <block-period_int>	Enter the number of seconds that you want to block the requests. The valid range is 1–3,600 seconds. This option only takes effect when you choose Period Block in Action.	600
severity-definitely {High Info Low Medium}	Select the severity level for this anomaly type. The severity level will be displayed in the alert email and/or log message.	High
trigger-definitely <policy_name>	Select a trigger policy that you have set in Log&Report > Log Policy > Trigger Policy. If definite anomaly is detected, it will trigger the system to send email and/or log messages according to the trigger policy.	No default.
status {enable disable}	Enable to change the status to Running, while disable to change the status to Stopped.	enable

Variable	Description	Default
url-replacer-policy <policy_name>	Select the name of the URL Replacer Policy that you have created in Machine Learning Templates. If web applications have dynamic URLs or unusual parameter styles, you must adapt URL Replacer Policy to recognize them.	No default.
trigger-potential <policy_name>	Select a trigger policy that you have set in Log&Report > Log Policy > Trigger Policy. If potential anomaly is detected, it will trigger the system to send email and/or log messages according to the trigger policy.	
<allow-domain-name_id>	Enter the ID of the policy. The valid range is 1–65,535.	No default.
ip-list-type {Trust Black}	Allow or deny sample collection from the Source IP list.	Trust
domain-name <domain-name_str>	Add full domain name or use wildcard '*' to cover multiple domains under one profile.	No default.
domain-index <domain-index_id>	The number automatically assigned by the system when the domain name is created.	No default.
hmm-probability-sample-length-check {enable disable}	Enable to check whether the parameter value is in unexpected length or of high anomaly probability.	disable
sample-length-threshold <int>	If the length of the parameter value is larger than the specified threshold, the system will not send it to SVM model for further validation. Instead, it will be directly treated as an anomaly. The valid range is 0-1,024. 0 means not applicable.	0
hmm-probability-threshold <int>	If the anomaly probability of the parameter value is larger than the specified threshold, the system will not send it to SVM model for further validation. Instead, it will be directly treated as an anomaly. The valid range is 0-2,000. 0 means not applicable. If you are not sure how to set a proper probability value, there are two places where you can refer: - In Parameter View, beside the Strictness Level for Anomaly option, there is a Test Sample button. Click it and enter a parameter value to check its probability. Repeat the tests with different values until you get an idea on a reasonable probability threshold. - In Attack Log, find an Anomaly Detection attack. Click it to view the log details. You will find its probability.	0

Variable	Description	Default
character-set {AUTO ISO-8859-1 ISO-8859-2 ISO-8859-3 ISO-8859-4 ISO-8859-5 ISO-8859-6 ISO-8859-7 ISO-8859-8 ISO-8859-9 ISO-8859-10 ISO-8859-15 GB2312 BIG5 ISO-2022-JP ISO-2022-JP-2 Shift-JIS ISO-2022-KR UTF-8}	The corresponding character code when manually setting the domain.	No default.
<source-ip-list_id>	Enter the ID of the source IP. The valid range is 1–9,223,372,036,854,775,807	No default.
<ip>	Enter the IP range for the source IP list.	No default.
ip-expire-intval <int> ip-expire-cnts <int>	An parameter is in unconfirmed status initially, and it will be set to confirmed if the parameter is contained in the requests from a certain number of different source IPs within the given time. Otherwise, the parameter will be discarded. <code>ip-expire-cnts</code> defines the "the number of different source IPs", while the <code>ip-expire-intval</code> defines the given time period. The valid range for <code>ip-expire-intval</code> is 1-24 in hours, and the default value is 4. The valid range for <code>ip-expire-cnts</code> is 1-5, and the default value is 3.	4/3
ip-argcount-limit {enable disable}	Enable it so that each source IP can create at most 20 new arguments in every 30 minutes.	disable
sample-limit-by-ip <sample-limit-by-ip_int>	The limitation number of samples collected from each IP. The valid range is 0–5000.	30

Related Topics

- [waf machine-learning url-replacer-rule/policy on page 590](#)

waf mitb-policy

Use this command to configure MiTB policies.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf mitb-policy
  edit "<mitb-rule_name>"
    config rule list
      edit "<rule-list_id>"
        set "<mitb-rule_name>"
      next
    end
  next
end
```

Variable	Description	Default
"<rule-list_id>"	Select the sequence number of the MiTB rules.	No default.
"<mitb-rule_name>"	Enter the name of a MiTB policy.	No default.

Related topics

- [waf mitb-rule on page 600](#)

waf mitb-rule

Use this command to configure MiTB rules.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf mitb-rule
  edit mitb-rule_name
    set action {alert| alert_deny}
    set severity {High | Medium | Low | Info}
    set trigger "<trigger-policy_name>"
    set host-status {enable | disable}
    set host "<host_str>"
    set request-url "<request-url_str>"
    set request-type {plain | regular}
```



```

set post-url "<post-url_str>"
set ajaxcheck {enable | disable}
set mid-proxy {enable | disable}
edit protected-parameter-list_name
    set type {regular-input | password-input}
    set obfuscate {enable | disable}
    set encrypt {enable | disable}
    set anti-keyLogger {enable | disable}
next
end

config allowed-external-domains-list
    edit allowed-external-domains-list_id
        set domain "<domain_str>"
    next
end

```

Variable	Description	Default
mitb-rule_name	Enter a name that can be referenced by other parts of the configuration.	No default.
action {alert alert_deny}	Select the action the FortiWeb appliance takes when it detects a violation of the rule: Alert —Accept the connection and generate an alert email and/or log message. Alert & Deny —Block the request (or reset the connection) and generate an alert and/or log message.	Alert
severity {High Medium Low Info}	Select which severity level the FortiWeb appliance will use when it logs a violation of the rule.	Low
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 violation of the rule.	No default.
host-status {enable disable}	Enable to compare the MiTB rule to the <code>Host :</code> field in the HTTP header.	No default.
host "<host_str>"	Select the IP address or FQDN of a protected host.	No default.
request-url "<request-url_str>"	The URL hosting the webpage which contains the parameters (field names or passwords) you want to protect.	No default.
request-type {plain regular}	Select either of the URL types.	plain
post-url "<post-url_str>"	Enter the URL triggered after you submit your access request.	No default.
ajaxcheck {enable disable}	Enable to validate AJAX requests against an allowlist of permitted external domains.	disable

Variable	Description	Default
mid-proxy {enable disable}	Enable Middle Proxy to let FortiWeb detect SSL stripping by comparing client-reported security attributes—protocol, host, User-Agent (UA), and security headers—against stored data. For example, if the server response includes an HSTS header but the client reports its absence, FortiWeb flags a potential attack.	disable
protected-parameter-list_name	Enter the protected parameter list name.	No default.
type {regular-input password-input}	Select the input type to carry out the protection.	regular-input
obfuscate {enable disable}	Enable to obfuscate the configured parameter name.	No default.
encrypt {enable disable}	Enable to encrypt the parameter value.	No default.
anti-keyLogger {enable disable}	Enable anti-keyLogger to prevent hackers from intercepting your password input.	No default.
allowed-external-domains-list_id	Enter the allowed external domain list ID.	No default.
domain "<domain_str>"	Set the domain, for example, www.alloweddomain.com.	No default.

Related topics

- [waf mitb-policy](#)

waf mobile-api-protection

When a client accesses a web server from a mobile application, the Mobile Application Identification module checks whether the request carries the JWT-token field and whether the token carried is valid, and sets flags for the following cases:

- The traffic doesn't carry the JWT-token header
- The traffic carries the JWT-token header and the token is valid
- The traffic carries the JWT-token header, while the token is invalid

The mobile API protection feature checks the flags. With the API protection policy and rule configured, actions set in the protection rule will be performed.

Syntax

```
config waf mobile-api-protection-rule
edit <mobile-api-protection-rule_name>
    set host-status {enable | disable}
    set host <host_str>
    set action {alert | deny_no_log | alert_deny | block-period}
```

```

    set block-period <block-period_int>
    set severity {High | Medium | Low | Info}
    set trigger <trigger_policy_name>
    config url-list
        edit <url-list_id>
            set url-type {plain | regular}
            set url-pattern <url-pattern_str>
        next
    end
next
end

config waf mobile-api-protection-policy
    edit <mobile-api-protection-policy_name>
        config rule-list
            edit <rule-list_id>
                set rule <rule_name>
            next
        end
    next
end

```

Variable	Description	Default
<mobile-api-protection-rule_name>	Enter the name for the mobile API protection rule.	No default.
host-status {enable disable}	Enable to compare the mobile API protection rule to the <code>Host:</code> field in the HTTP header.	Disable
host <host_str>	Select the IP address or fully qualified domain name (FQDN) of the protected host to which this rule applies. This option is available only if <code>host-status {enable disable}</code> is enable.	No default.
action {alert deny_no_log alert_deny block-period}	Select which action the FortiWeb appliance will take when it detects a violation. alert—Accept the connection and generate an alert email and/or log message. alert_deny—Block the request (or reset the connection) and generate an alert and/or log message. deny_no_log—Block the request (or reset the connection). block-period—Blocks the request for a certain period of time.	Alert
block-period <block-period_int>	Enter the number of seconds that you want to block the requests. The valid range is 1–3,600 seconds. This option only takes effect when you choose Period Block in <code>action {alert deny_no_log alert_deny block-period}</code>.	600

Variable	Description	Default
severity {High Medium Low Info}	When FortiWeb records rule violations in the attack log, each log message contains a Severity Level field. Select the severity level that FortiWeb will record when the rule is violated: - Low - Medium - High - Informative The default value is High .	High
trigger <trigger_policy_name>	Select the trigger, if any, that FortiWeb carries out when it logs and/or sends an alert email about a rule violation. For details, see " Viewing log messages " on page 1.	No default.
<url-list_id>	Type the index number of the individual URL within the URL list, or keep the field's default value of auto to let the FortiWeb appliance automatically assign the next available index number.	No default.
url-type {plain regular}	Select whether the URL Pattern field will contain a literal URL (plain), or a regular expression designed to match multiple URLs (regular).	plain
url-pattern <url-pattern_str>	Depending on the <code>url-type</code> , enter either: plain—The literal URL, such as <code>/index.php</code>, that the HTTP request must contain in order to match the rule. The URL must begin with a slash (<code>/</code>). regular—A regular expression, such as <code>^/*\.php</code>, matching the URLs to which the rule should apply. The pattern does not require a slash (<code>/</code>), but it must match URLs that begin with a slash, such as <code>/index.cfm</code>. Do not include the domain name, such as <code>www.example.com</code> , which is configured separately in <code>[bot-detection-exception-list] <No.> host <string></code> .	No default
<mobile-api-protection-policy_name>	Enter the name for the mobile API protection policy.	No default.
<rule-list_id>	Type the index number of the individual rule within the rule list, or keep the field's default value of auto to let the FortiWeb appliance automatically assign the next available index number.	No default.
rule <rule_name>	Select the mobile API protection rule from the drop-down list.	No default.

waf openapi-file

Use this command to create openapi file name.

Syntax

```
config waf openapi-file
  edit "<openapi-file_name>"
end
```

Variable	Description	Default
"<openapi-file_name>"	Enter the name of an openapi file.	No default.

Related topics

- [waf openapi-validation-policy on page 605](#)

waf openapi-validation-policy

Use this command to create new openapi validation policy and configure related settings.

Syntax

```
config waf openapi-validation-policy
  edit openapi-validation-policy_name
    set action {alert | alert_deny | block-period | redirect | send_403_forbidden |
      deny_no_log}
    set block-period "<seconds_int>"
    set inherit-action-for-non-JSON-media-types {enable|disable}
    set inherit-action-for-unlisted-media-types {enable|disable}
    set severity {Low | Medium | High | Info}
    set trigger "<trigger-policy>"
  config schema-file
    edit schema-file_id on page 606
      set openapi-file <datasource> on page 606
  end
```

Variable	Description	Default
openapi-validation-policy_name	Enter the name for the OpenAPI validation policy.	No default
action {alert alert_	Select which action FortiWeb will take when it detects a	alert

Variable	Description	Default
deny block-period redirect send_403_forbidden deny_no_log}	violation of the policy.	
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 1–3600 seconds.	600
inherit-action-for-non-JSON-media-types {enable disable}	When enabled, FortiWeb processes content as JSON if <code>x-is-json: true</code> , even when the media type does not explicitly match <code>application/json</code> or <code>text/json</code> .	enable
inherit-action-for-unlisted-media-types {enable disable}	Controls whether to apply the default action for media types not listed in the OAS document.	enable
severity {Low Medium High Info}	Select which severity level the FortiWeb appliance will use when it logs a violation of the rule.	Low
trigger "<trigger-policy>"	Select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a violation of the rule.	No default
schema-file_id	The scheme file by the sequence number.	No default.
openapi-file <datasource>	Select the created OpenAPI file.	No default.

Related topics

- [waf openapi-file on page 605](#)

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 [waf web-protection-profile inline-protection on page 696](#) and [waf web-protection-profile offline-protection on page 706](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```

config waf padding-oracle
  edit "<padding-oracle_rule_name>"
    set action {alert | alert_deny | block-period | deny_no_log}
    set block-period <block-period_int>
    set severity {High | Medium | Low | Info}
    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
end

```

Variable	Description	Default
"<padding-oracle_rule_name>"	Enter the name of a new or existing rule. The maximum length is 63 characters. To display the list of existing policies, enter: <pre>edit ?</pre>	No default.
action {alert alert_deny block-period deny_no_log}	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 (or 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 <block-period_int> on page 608. deny_no_log—Deny a request. Do not generate a log message. 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. Failure to do so may cause FortiWeb to block all connections when it detects a violation of this type. For details, see waf x-forwarded-for on page 721. Attack log messages contain <code>Padding Oracle Attack</code> when this feature detects a possible attack. Because this attack involves some repeated brute force, the attack log may not appear immediately, but should occur within 2 minutes, depending on your configured DoS alert interval.	alert

Variable	Description	Default
	Caution: This setting will be ignored if monitor-mode {enable disable} on page 163 is enabled. Note: Logging and/or alert email occur only when the these features are enabled and configured. For details, see log attack-log on page 61 and log alertMail on page 60. Note: To use this rule set with auto-learning, select <code>alert</code>. If <code>action</code> is <code>alert_deny</code> 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.	
<code>block-period <block-period_int></code>	Enter 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 {alert alert_deny block-period deny_no_log} on page 607 is <code>block-period</code>. The valid range is 1–36,000 seconds.	600
<code>severity {High Medium Low Info}</code>	When rule violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Specify the severity level FortiWeb uses when it logs a violation of this rule.	Medium
<code>trigger "<trigger-policy_name>"</code>	Enter 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. For details, see log trigger-policy on page 96. To display the list of existing triggers, enter: <pre>set trigger ?</pre>	No default.
<code><entry_index></code>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999.	No default.
<code>host-status {enable disable}</code>	Specify <code>enable</code> to apply this rule only to HTTP requests for specific web hosts. Also specify host "<host_str>" on page 608. Specify <code>disable</code> to match the rule based on the other criteria, such as the URL, but regardless of the <code>Host:</code> field.	disable
<code>host "<host_str>"</code>	Specify which protected host names entry (either a web host name or IP address) that the <code>Host:</code> field of the HTTP request must be in to match the rule. This option is available only if the value of host-status {enable disable} on page 608 is enabled.	No default.

Variable	Description	Default
	Maximum length is 255 characters.	
url-type {plain regular}	Enter to determine how the value of <code>protected-url "<protected-url_str>"</code> on page 609 is specified: <code>plain</code>—A literal URL. <code>regular</code>—A regular expression designed to match multiple URLs.	plain
protected-url "<protected-url_str>"	If the value of <code>url-type {plain regular}</code> on page 609 is <code>plain</code>, enter the literal URL that HTTP requests that match the rule contain. For example: <pre>/profile.jsp</pre> The URL must begin with a backslash (/). If the value of <code>url-type</code> is <code>regular</code>, specify a regular expression matching all and only the URLs to which the rule should apply. For example: <pre>^/*\.jsp\?uid\=(.*)</pre> The pattern does not require a slash (/); however, it must at least match URLs that begin with a slash, such as <code>/profile.cfm</code>. Do not include the domain name, such as <code>www.example.com</code>, which is specified by <code>host</code>. Regular expressions beginning with an exclamation point (!) are not supported. For information on language and regular expression matching, see the <i>FortiWeb Administration Guide</i>: https://docs.fortinet.com/document/fortiweb	No default.
target "<cookie parameter url>"	Specify which parts of the client's requests FortiWeb examines for padding attack attempts: <code>url</code>—A URL (for example, the parameter <code>/user/0000012FE03BC2</code> is embedded in the URL). <code>parameter</code>—A parameter (for example, the parameter <code>/index.php?user=0000012FE03BC2</code> appended to a traditional GET or POST body). <code>cookie</code>—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
    end
  end
```

Related topics

- [waf web-protection-profile inline-protection on page 696](#)
- [waf web-protection-profile offline-protection on page 706](#)

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 [waf web-protection-profile inline-protection on page 696](#) and [waf web-protection-profile offline-protection on page 706](#).

Before you can configure parameter validation rules, you must first configure one or more input rules. For details, see [waf input-rule on page 551](#).

You can use SNMP traps to notify you when a parameter validation rule is enforced. For details, see [system snmp community on page 375](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf parameter-validation-rule
  edit "<rule_name>"
    set cache-mode {enable | disable}
    config input-rule-list
      edit <entry_index>
        set input-rule "<input-rule_name>"
      next
    end
  next
end
```

Variable	Description	Default
cache-mode {enable disable}	Parameter Validation processes and forwards incoming requests as soon as they are received, which helps maintain fast processing time. However, this approach can occasionally result in requests being interrupted midway if illegal parameters are detected in the later part of the request. To prevent FortiWeb from forwarding the partial requests mentioned above, you can enable <code>cache-mode</code>. When cache mode is enabled, the Parameter Validation module will store the entire request in a cache before performing validation and forwarding.	disable
"<rule_name>"	Enter the name of a new or existing rule. The maximum length is 63 characters. To display the list of existing rules, enter: <pre>edit ?</pre>	No default.
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999.	No default.
input-rule "<input-rule_name>"	Enter the name of an input rule to use in the parameter validation rule. The maximum length is 63 characters. To display the list of existing input rules, enter: <pre>set input-rule ?</pre>	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

- [waf input-rule on page 551](#)
- [waf web-protection-profile inline-protection on page 696](#)
- [waf web-protection-profile offline-protection on page 706](#)

waf signature

Use this command to configure web 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
- Remote file inclusion (RFI)
- Local file inclusion (LFI)
- OS commands
- Trojans/viruses
- Exploits
- Sensitive server information disclosure
- Credit card data leaks

To defend against known attacks, FortiWeb scans:

- Parameters in the URL of HTTP `GET` requests
- Parameters in the body of HTTP `POST` requests
- XML in the body of HTTP `POST` requests (if [waf web-protection-profile inline-protection on page 696](#) is enabled)
- Cookies
- Headers
- JSON Protocol Detection
- Uploaded filename(`MULTIPART_FORM_DATA_FILENAME`)

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 details, see [amf3-protocol-detection {enable | disable} on page 700](#) and [waf web-protection-profile inline-protection on page 696](#) (for inline protection profiles) or [amf3-protocol-detection {enable | disable} on page 709](#) (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 details, see [Permissions on page 46](#).

Updating signatures

Known attack signatures can be updated. For details about uploading a new set of attack definitions, see the *FortiWeb Administration Guide*:

<https://docs.fortinet.com/document/fortiweb>

You can also create your own. For details, see [waf custom-protection-rule on page 486](#).

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 [waf custom-protection-group on page 485](#).

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*:
<https://docs.fortinet.com/document/fortiweb>

Overriding signature category configuration

To override category-wide actions for a specific signature, configure:

- [config signature_disable_list on page 614](#)—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 on page 614](#)—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 on page 614](#)—Only log/alert when detecting the attack, even if the category in general is configured to block.
- [config filter_list on page 614](#)—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 [waf web-protection-profile inline-protection on page 696](#) and [waf web-protection-profile offline-protection on page 706](#).

You can use SNMP traps to notify you when an attack or data leak has been detected. For details, see [system snmp community on page 375](#).

Syntax

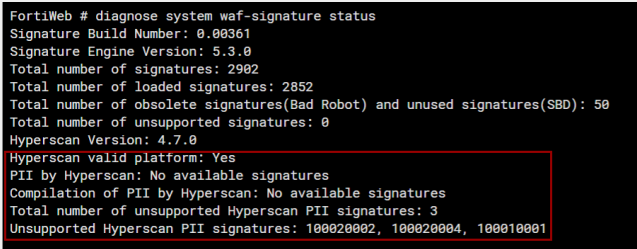
```
config waf signature
  edit "<signature-set_name>"
    set credit-card-detection-threshold <instances_int>
    set custom-protection-group "<group_name>"
    set sensitivity-level {1|2|3|4}
    set personally-identifiable-information-hyperscan-mode {enable | disable}
  config main_class_list
    edit {010000000 | 020000000 | 030000000 | 040000000 | 050000000 | 060000000 |
      070000000 | 080000000 | 090000000 | 100000000 | 110000000 | 120000000}
      set action {alert | alert_deny | block-period | only_erase | send_HTTP_response
        | alert_erase | redirect | deny_no_log}
      set block-period <seconds_int>
      set severity {Low | Medium | High | Info}
      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 | 110000000 | 120000000}
  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 {low | critical | informational | moderate | substantial |
                    severe}
  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 | HTTP_HEADER | JSON_ELEMENTS}
  set operator {STRING_MATCH | REGEXP_MATCH | EQ | NE | INCLUDE | EXCLUDE}
  set HTTP-method {get post head options trace connect delete put others patch}
  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>"	Enter the name of a new or existing rule. The maximum length is 63 characters. To display the list of existing rules, enter: edit ?	No default.
credit-card-detection-threshold <instances_int>	Enter the number of credit cards that triggers the credit card number detection feature.	1

Variable	Description	Default
	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 1–128.	
custom-protection-group "<group_name>"	Enter the name of the custom signature group to be used, if any. The maximum length is 63 characters. To display the list of existing custom signature groups, enter: <pre>set custom-protection-group ?</pre>	No default.
sensitivity-level {1 2 3 4}	Increasing the level adds additional signatures but also adds the chance of blocking legitimate traffic.	4
personally-identifiable-information-hyperscan-mode {enable disable}	Enable to use hyperscan to detect personally identifiable information in the response body. Run <code>diagnose system waf-signature status</code> to verify whether your FortiWeb model and the FDS support hyperscan. As shown in the following screenshot, the "Hyperscan valid platform" confirms that your FortiWeb model supports hyperscan. However, the remaining lines indicate that the current version of the FDS does not yet support hyperscan signatures.  <pre>FortiWeb # diagnose system waf-signature status Signature Build Number: 0.00361 Signature Engine Version: 5.3.0 Total number of signatures: 2902 Total number of loaded signatures: 2852 Total number of obsolete signatures(Bad Robot) and unused signatures(SBD): 50 Total number of unsupported signatures: 0 Hyperscan Version: 4.7.0 Hyperscan valid platform: Yes PII by Hyperscan: No available signatures Compilation of PII by Hyperscan: No available signatures Total number of unsupported Hyperscan PII signatures: 3 Unsupported Hyperscan PII signatures: 100020002, 100020004, 100010001</pre>	disable
{010000000 020000000 030000000 040000000 050000000 060000000 070000000 080000000 090000000 100000000 110000000 120000000}	Enter the ID of a signature class (or, for subclass overrides, the subclass ID). To display the list of signature classes, enter: <pre>edit ?</pre>	No default.
action {alert alert_deny block-period only_erase send_HTTP_response alert_erase redirect deny_no_log}	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. <code>alert</code>—Accept the request and generate an alert email and/or log message.	alert

Variable	Description	Default
	Note: Does not cloak, except for removing sensitive headers. (Sensitive information in the body remains unaltered.) • <code>alert_deny</code>—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. For details, see "system replacemsg" on page 1. • <code>block-period</code>—Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int> on page 617. 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. Failure to do so may cause FortiWeb to block all connections when it detects a violation of this type. For details, see waf x-forwarded-for on page 721. • <code>only_erase</code>—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. • <code>send_HTTP_response</code>—Block and reply to the client with an HTTP error message, and generate an alert email, a log message, or both • <code>alert_erase</code>—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. • <code>deny_no_log</code>—Deny a request. Do not generate a log message. Note: This option is not fully supported in Offline Protection mode. Effects will be identical to <code>alert</code>; sensitive information will not be blocked or erased.	
	• <code>redirect</code>—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>" on page 704 and rdt-reason {enable disable} on page 704.	

Variable	Description	Default
	Caution: FortiWeb ignores this setting if monitor-mode {enable disable} on page 163 is enabled. Note: Actions that generate log messages alert email actions require the features to be enabled and configured. For details, see log disk on page 66 and log alertMail on page 60. Note: If you select an auto-learning profile in the policy with Offline Protection profiles that use this rule, select <code>alert</code>. If the <code>action</code> is <code>alert_deny</code>, the FortiWeb appliance resets the connection when it detects an attack and the session information for the auto-learning feature will be incomplete. For details about auto-learning requirements, see "waf web-protection-profile autolearning-profile" on page 1.	
<code>block-period <seconds_int></code>	Enter 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 1–3,600 seconds. The setting is applicable only if <code>action</code> is <code>period-block</code>. Note: This is not a single setting. You can configure the block period separately for each signature category.	600
<code>severity {Low Medium High Info}</code>	When rule violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) 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
<code>trigger "trigger-policy_name"</code>	Enter the name of the trigger, if any, to apply when a protection rule is violated. For details, see log trigger-policy on page 96. The maximum length is 63 characters. To display the list of existing triggers, enter: <pre>set trigger ?</pre> Note: This is not a single setting. You can configure a different trigger for each signature category.	No default.
<code>"<signature-id_str>"</code>	Enter 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, enter: <pre>edit ?</pre>	No default.

Variable	Description	Default
"<alert-only-list_signature-id_str>"	Enter 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>"	Enter 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>"	Enter the ID of a specific signature that will not be affected by the threat weight settings, if any. When traffic violates specified signature, FortiWeb takes the local action specified for that signature.	No default.
"<score-grade-list_signature-id_str>"	Enter the ID of a specific signature to configure its threat weight. Specify the <code>scoring-grade</code> to set the threat weight of the specified signature.	No default.
scoring-grade {low critical informational moderate substantial severe}	Specify the threat weight that the signature adds to the combined threat weight. Global threat weight risk level values can be modified using server-policy pattern threat-weight on page 132 .	No default.
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–128. You can create up to 128 exceptions for each signature.	No default.
signature_id "<signature-id_str>"	Enter 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 HTTP_HEADER JSON_ELEMENTS}	Enter the type of object that FortiWeb examines for matching values: - HTTP_METHOD—One or more HTTP methods specified by HTTP-method {get post head options trace connect delete put others patch} on page 619. - CLIENT_IP—The IP address or IP range specified by ip {<ipv4> <ipv6>} on page 619. - HOST—The <code>Host:</code> field value specified by value {"<value_str>" "<value_pattern>"} on page 620. - URI—The URL value specified by <code>value</code>. The value does not include parameters. - FULL_URL—The URL value specified by <code>value</code>. The value includes parameters to match. - PARAMETER—A parameter specified by name {"<name_str>" "<name_pattern>"} on page 619. To match a specific parameter value, enable value-check {enable disable} on page 620,	

Variable	Description	Default
	and then specify <code>value</code>. COOKIE—A cookie specified by <code>name</code>. To match a specific cookie value, enable <code>value-check</code>, and then specify <code>value</code>.	
operator {STRING_MATCH REGEXP_MATCH EQ NE INCLUDE EXCLUDE}	Enter the type of values to match. The <code>match-target</code> value determines which types are available. STRING_MATCH—<code>value</code> is a literal value (for example, a literal host name). REGEXP_MATCH—<code>value</code> is a regular expression that matches the object the exception applies to. EQ—When <code>match-target</code> is <code>CLIENT_IP</code>, FortiWeb only performs a signature scan for requests with a client IP address that matches the value of <code>ip</code>. NE—When <code>match-target</code> is <code>CLIENT_IP</code>, FortiWeb does not perform a signature scan for requests with a client IP address that matches the value of <code>ip</code>. INCLUDE—When <code>match-target</code> is <code>HTTP_METHOD</code>, FortiWeb does not perform a signature scan for requests that include the HTTP methods specified by <code>HTTP-method</code>. EXCLUDE—When <code>match-target</code> is <code>HTTP_METHOD</code>, FortiWeb only performs a signature scan for requests that include the HTTP methods specified by <code>HTTP-method</code>.	
HTTP-method {get post head options trace connect delete put others patch}	When <code>match-target</code> {HTTP_METHOD CLIENT_IP HOST URI FULL_URL PARAMETER COOKIE HTTP_HEADER JSON_ELEMENTS} on page 618 is <code>HTTP_METHOD</code>, specifies one or more HTTP methods to match.	No default.
ip {<ipv4> <ipv6>}	When <code>match-target</code> {HTTP_METHOD CLIENT_IP HOST URI FULL_URL PARAMETER COOKIE HTTP_HEADER JSON_ELEMENTS} on page 618 is <code>CLIENT_IP</code>, specifies the IP address or IP range to match.	No default.
name {"<name_str>" "<name_pattern>"}	Enter 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 <code>operator</code> {STRING_MATCH REGEXP_MATCH EQ NE INCLUDE EXCLUDE} on page 619. Available when <code>match-target</code> {HTTP_METHOD CLIENT_IP HOST URI FULL_URL PARAMETER COOKIE HTTP_HEADER JSON_ELEMENTS} on page 618 is <code>PARAMETER</code> or <code>COOKIE</code>.	No default.

Variable	Description	Default
value-check {enable disable}	Enable to specify 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>"}	Enter the value to match (for example, a <code>Host :</code> field value). Whether the value is a literal value or a regular expression is determined by the value of <code>operator</code> .	No 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>"	Enter 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

- [waf web-protection-profile inline-protection on page 696](#)
- [waf web-protection-profile offline-protection on page 706](#)
- [system snmp community on page 375](#)
- [waf custom-protection-group on page 485](#)
- [log trigger-policy on page 96](#)

waf signature_update_policy

Use this command to deploy new signature updates in alert mode.

Syntax

```
config waf signature_update_policy
    set status {enable | disable}
end
```

Variable	Description	Default
status {enable disable}	Enable to list new signatures from the FDS update.	disable

Example

This example shows how to enable the option to show the new signature list from the FDS update.

```
config waf signature_update_policy
    set status enable
end
```

Related topics

- [waf signature on page 612](#)

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 details, see [Permissions on page 46](#).

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>"	Enter the name of a new or existing authentication server pool. The maximum length is 63 characters. To display the list of existing pools, enter: <code>edit ?</code>	No default.
<entry_index>	Enter 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>. Enter <code>ldap</code> for a LDAP server or <code>radius</code> 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. For details, see user ldap-user on page 397 .	No 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. For details, see user radius-user on page 407 .	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} on page 622 is <code>radius</code> and client-auth-method {html-form-auth HTTP-auth client-cert-auth saml-auth ntlm-auth} on page 629 is <code>html-form-auth</code> .	disable

Example

For an example, see [waf site-publish-helper rule on page 626](#).

Related topics

- [waf site-publish-helper rule on page 626](#)

waf site-publish-helper form-based-delegation

Use this command to create a Form Based Delegation rule.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf site-publish-helper form-based-delegation
edit waf site-publish-helper form-based-delegation
    set url-type { plain | regular}
    set logon-url <URL>
    set form-action <URL>
    set additional-cookies
    set username-field
    set password-field
    set waf site-publish-helper form-based-delegation
next
end
```

Variable	Description	Default
form-based-delegation_ name	Enter a name for the Form based Delegation rule.	No default.
url-type { plain regular}	<code>plain</code> —Enter a literal URL, such as <code>/folder1/index.htm</code> that the HTTP request must contain in order to match the rule, or use wildcards to match multiple URLs, such as <code>/folder1/*</code> or <code>/folder1/*/index.htm</code> . The URL must begin with a slash (<code>/</code>). <code>regular</code> —A regular expression, such as <code>^/*.php</code> , matching the URLs to which the rule should apply. The pattern does not require a slash (<code>/</code>).	plain
logon-url <URL>	Enter the logon URL in simple string or regular expression.	No default.
form-action <URL>	The URL of the form.	No default.
method { PUT GET}	Select whether to use GET or POST method to initiate the	POST

Variable	Description	Default
	authentication requests to the server.	
additional-cookies	Configure to add cookie in the authentication request.	disable
username-field	The keyword of the username field.	No default.
password-field	The keyword of the password field.	No default.
additional-field-list	Enter additional fields to add in the authentication request. field-entry: field content The format must be "key=value"	No default.

To use the **Form Based Delegation**, you need to create a **Site Publish** rule, select **HTML Form Authentication** for **Client Authentication Method**, select **Form Based Delegation** for **Authentication Delegation**, then choose the Form Based Delegation you have created. See [waf site-publish-helper rule on page 626](#).

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 [waf site-publish-helper rule on page 626](#).

To apply this policy, include it in an inline web protection profile. For details, see [waf web-protection-profile inline-protection on page 696](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf site-publish-helper policy
edit "<site-publish-policy_name>"
    set account-lockout {enable | disable}
    set max-login-failures <failures_int>
    set account-block-period <account-block-period_int>
    set within <within_int>
    set limit-users {enable | disable}
    set maximum-users <integer>
    set session-idle-timeout <integer>
    set credential-stuffing-protection {enable | disable}
    set action {alert | alert_deny | block-period | deny_no_log}
    set block-period <block_period_int>
    set severity {high | medium | low | Info}
    set trigger "<trigger_policy>"
config rule
    edit <entry_index>
        set rule-name "<site-publish-rule_name>"
    next
end
next
```


end

Variable	Description	Default
"<site-publish-policy_name>"	Enter the name of a new or existing policy. The maximum length is 63 characters. To display the list of existing policies, enter: edit ?	No default.
account-lockout {enable disable}	Enable to prevent account cracking by locking an account out after several failures logging into FortiWeb.	disable
max-login-failures <failures_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 (within <within_int> on page 625).	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
within <within_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
limit-users {enable disable}	Enable to limit the number of concurrent logins per account.	disable
maximum-users <integer>	Specify the maximum number of concurrent logins using the same account.	1
session-idle-timeout <integer>	When a session is idle for the specified period of time, the Concurrent Users count will be renewed. The user who is timed-out needs to re-log in.	30
credential-stuffing-protection {enable disable}	Enable to use FortiGuard's Credential Stuffing Defense database to prevent against credential stuffing attacks.	disable
action {alert alert_deny block-period deny_no_log}	Set the action. The options are: <code>alert</code>—Accept the request and generate an alert email and/or log message. <code>alert_deny</code>—Block the request (or reset the connection) and generate an alert email and/or log message <code>block-period</code>—Block subsequent requests from the client for a number of seconds. <code>deny_no_log</code>—Deny a request. Do not generate a log message. You can customize the web page that returns to the client with the HTTP status code.	No default.

Variable	Description	Default
block-period <block_period_int>	If the action {alert alert_deny block-period deny_no_log} on page 625 is <code>block-period</code> , set amount of time (in seconds) FortiWeb will block subsequent requests from the client. The valid range is 1–3600 seconds.	600
severity {high medium low Info}	Set the severity of credential stuffing attacks.	No default.
trigger "<trigger_policy>"	Select the trigger policy, if any, to apply in the Site Publish policy. For details, see log trigger-policy on page 96 .	No default.
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999,999.	No default.
rule-name "<site-publish-rule_name>"	Enter the name of an existing rule.	No default.

Example

For an example, see [waf site-publish-helper rule on page 626](#).

Related topics

- [waf site-publish-helper rule on page 626](#)
- [waf web-protection-profile inline-protection on page 696](#)

waf site-publish-helper rule

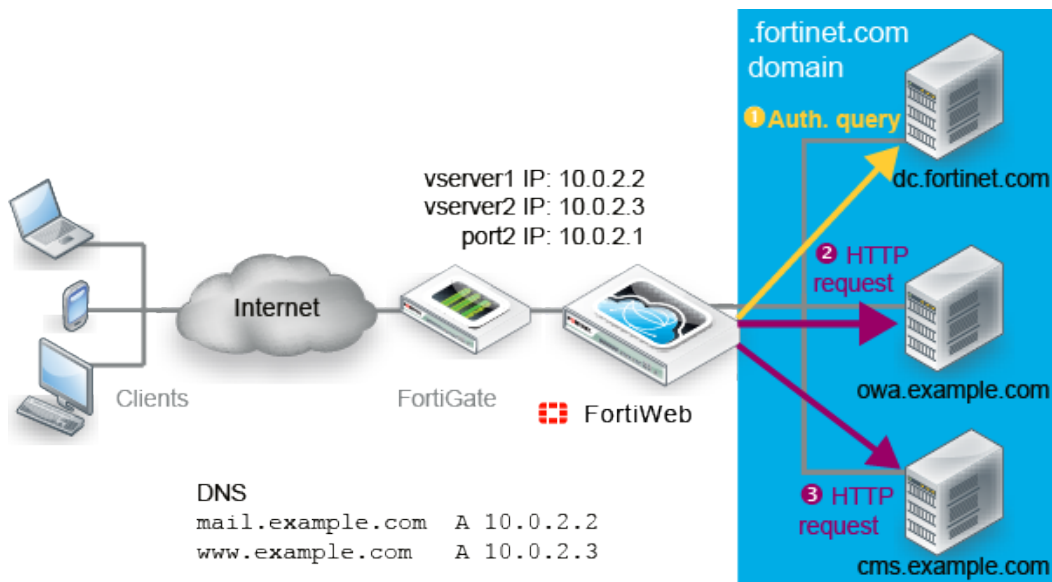
Use this command to configure access control, authentication, and, optionally, SSO for your web applications.

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 if:

- Your users access multiple web applications on your domain
- You have defined accounts centrally on an LDAP (such as Microsoft Active Directory) or RADIUS server

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 [user ldap-user on page 397](#) and ["server-policy custom-application application-policy" on page 1](#).

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 details about these options, see the descriptions of the individual site publishing rule settings and the *FortiWeb Administration Guide*:

<https://docs.fortinet.com/document/fortiweb>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf site-publish-helper rule
edit "<site-publish-rule_name>"
    set status {enable | disable}
    set req-type {plain | regular}
    set cookieless {enable | disable}
    set cookieless-cache <int>
    set saml-server "<server_name>"
    set service-principal-name-pool "<pool_name>"
    set published-site "<host_fqdn>"
    set path "<url_str>"
```

```

set client-auth-method {html-form-auth | HTTP-auth | client-cert-auth | saml-
    auth | ntlm-auth}
set logoff-path-type {plain | regular}
set Published-Server-Logoff-Path "<url_str>"
set cookie-timeout <timeout_int>
set kerberos-type {krb5 | spnego} on page 637
set auth-server-pool "<authentication-server-pool_name>"
set auth-delegation {HTTP-basic | kerberos | kerberos-constrained-delegation |
    radius-constrained-delegation | no-delegation | ntlm | form-based-
    delegation}
set form-based-delegation <form-based-delegation_name>
set field-name {subject | SAN}
set attribution-name {email | UPN}
set pass-failed-auth {enable | disable}
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>"
set cookieless {enable | disable}
set append-custom-header {enable | disable}
set custom-header-name <custom-header-name_str>
set custom-header-value-format <custom-header-value-format_str>
set pass-failed-auth {enable | disable}
set cache-tgs-ticket {enable | disable}
next
end

```

Variable	Description	Default
"<site-publish-rule_name>"	Enter the name of a new or existing rule. The maximum length is 63 characters. To display the list of existing rules, enter: 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>" on page 629 contains a literal FQDN (<code>plain</code>), or a regular expression designed to match multiple host names or fully qualified domain names (<code>regular</code>).	plain
cookieless {enable disable}	Enable to authenticate clients without using cookies. For cookieless authentication, FortiWeb uses credential cache to avoid frequent requests to the authentication server.	disable

Variable	Description	Default
cookieless-cache <int>	You can set the cache timeout value for the cookieless authentication. The valid range is 0-86,400. When it's set to 0, FortiWeb will send authentication requests to the authentication server every time the user logs in.	3600
saml-server "<server_name>"	Select the SAML server that FortiWeb uses to authenticate clients. Available only when client-auth-method {html-form-auth HTTP-auth client-cert-auth saml-auth ntlm-auth} on page 629 is set to <code>saml-auth</code>.	No default.
service-principal-name-pool "<pool_name>"	Select the SPN pool for the application that clients access using this site publish rule. Available only when auth-delegation {HTTP-basic kerberos kerberos-constrained-delegation radius-constrained-delegation no-delegation ntlm form-based-delegation} on page 631 is <code>kerberos</code> or <code>kerberos-constrained-delegation</code>.	No default.
published-site "<host_fqdn>"	Depending on your selection in req-type {plain regular} on page 628, enter either: - The literal <code>Host: name</code>, such as <code>sharepoint.example.com</code>, that the HTTP request must contain in order to match the rule. - A regular expression, such as <code>^*\..example\..edu</code>, matching only the host names to which the rule should apply. The maximum length is 255 characters. Note: Regular expressions beginning with an exclamation point (<code>!</code>) are not supported. For information on language and regular expression matching, see the <i>FortiWeb Administration Guide</i>: https://docs.fortinet.com/document/fortiweb	No default.
path "<url_str>"	Enter the URL of the request for the web application, such as <code>/owa</code>. It must begin with a forward slash (<code>/</code>).	No default.
client-auth-method {html-form-auth HTTP-auth client-cert-auth saml-auth ntlm-auth}	Specify one of the following options: <code>html-form-auth</code>—FortiWeb authenticates clients by presenting an HTML web page with an authentication form. When the authentication cookie expires, FortiWeb replies to the first request without a valid authentication cookie with a 200 (OK) status code and injects HTML into the response, showing the user the login page. <code>HTTP-auth</code>—FortiWeb authenticates clients by	<code>html-form-auth</code>

Variable	Description	Default
	replying to the request with a 401 (Unauthorized) status code, and the browser displays a traditional, browser-specific authentication prompt. <code>client-cert-auth</code>—FortiWeb validates the HTTP client's personal certificate using the certificate verifier specified in the associated server policy or server pool configuration. <code>saml-auth</code>—FortiWeb uses a SAML server to pass identity information to a service provider via a signed XML document for client authentication. When the authentication cookie expires, FortiWeb replies to the first request without a valid authentication cookie with a 301 (Moved Temporarily) status code, forcing the browser to direct to the authentication page. <code>ntlm-auth</code>—FortiWeb uses a NTLM server for client authentication. FortiWeb replies to the first request from the client with a 401 (Unauthorized) status code, and the browser displays a traditional, browser-specific authentication prompt. If waf site-publish-helper rule on page 626 is enable, only <code>HTTP_auth</code> is allowed here.	
<code>logoff-path-type {plain regular}</code>	Specify whether <code>Published-Server-Logoff-Path</code> contains a literal URL (<code>plain</code>), or a regular expression designed to match multiple URLs (<code>regular</code>).	
<code>Published-Server-Logoff-Path "<url_str>"</code>	This setting appears only if client-auth-method {html-form-auth HTTP-auth client-cert-auth saml-auth ntlm-auth} on page 629 is <code>html-form-auth</code>. Depending on the value of <code>logoff-path-type</code>, enter one of the following values: - The literal URL of the request that a client sends to log out of the application (for example, <code>/owa/auth/logoff.aspx</code>). - 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 <code>path</code> value. For example, if <code>path</code> is <code>/owa</code>, <code>/owa/auth/logoff.aspx</code> 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 (<code>!</code>) are not supported. For information on language and regular expression matching, see the <i>FortiWeb Administration Guide</i>: https://docs.fortinet.com/document/fortiweb	No default.

Variable	Description	Default
cookie-timeout <timeout_int>	Specify the length of time (in minutes) that passes before the cookie that the site publish rule adds expires and the client must re-authenticate. The valid range is 0–216,000. To disable the limit, enter 0. If waf site-publish-helper rule on page 626 is enable, this must be 0. If you enter a value of 0, 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. For details, see waf site-publish-helper authentication-server-pool on page 622.	No default.
auth-delegation {HTTP-basic kerberos kerberos-constrained-delegation radius-constrained-delegation no-delegation ntlm form-based-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 saml-auth ntlm-auth} on page 629 is <code>html-form-auth</code> or <code>HTTP-auth</code>. 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 <code>client-auth-method</code> is <code>html-form-auth</code> or <code>HTTP-auth</code>. 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 <code>client-auth-method</code> is <code>client-cert-auth</code>. radius-constrained-delegation—After it authenticates the client's certificate, FortiWeb sends a RADIUS access-request to the RADIUS server, using the RFC822 name (email address) of the certificate's Subject Alternative Name.	no-delegation

Variable	Description	Default
	For some applications a prefix should be added to the mail address sent to the RADIUS server (example: "app1/forename.surname@org.com"). Use <code>field-name</code> to define the format of the extracted user name. Available only if <code>client-auth-method</code> is <code>client-cert-auth</code>. • <code>no-delegation</code>—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. • <code>ntlm</code>—FortiWeb uses NT LAN Manager (NTLM) for authentication delegation. This is a challenge/response authentication protocol that FortiWeb uses to verify the identify of clients attempting to connect to the server(s). Note: If the <code>POST</code> method request triggers NTLM authentication, the request body cannot exceed 100M. • <code>form-based-delegation</code>—FortiWeb uses Form Based Delegation to forward the client's credentials to the server. Available only when <code>client-auth-method</code> is <code>html-form-auth</code>. If waf site-publish-helper rule on page 626 is enable, only <code>no_delegation</code> or <code>HTTP-basic</code> is allowed here. Not available when <code>rsa-securig {enable disable}</code> on page 622 is set to enable.	
field-name	Enter the username format that FortiWeb uses to send the user email address to the RADIUS server for authorization. For example, let's say the email address of the user account is <code>example@abc.com</code>. If the format is <code>USERNAME</code>, FortiWeb will send <code>example</code> to RADIUS server. If the format is <code>RAWNAME</code>, FortiWeb will send <code>example@abc.com</code> to RADIUS server.	No default.

Variable	Description	Default
	You can add any letter before or/and after USERNAME/RAWNAME. FortiWeb will combine them together and send it to RADIUS server. So, to send <code>app1/example@abc.com</code>, you can enter either <code>app1/USERNAME@abc.com</code> or <code>app1/RAWNAME</code>. Note: USERNAME and RAWNAME should be exactly as is, and in upper case. This option is available only when <code>auth-delegation</code> is <code>radius-constrained-delegation</code>.	
<code>form-based-delegation</code> <code><form-based-delegation_name></code>	Select the Form Based Delegation you have created. See waf site-publish-helper form-based-delegation.	No default.
<code>field-name {subject SAN}</code>	Specify one of the following options to specify the certificate information that FortiWeb uses to determines the client username: <code>subject</code>—The email address value in the certificate's Subject information. For attribution-name {email UPN} on page 633, select <code>email</code>. <code>SAN</code>—The certificate's <code>subjectAltName</code> (Subject Alternative Name or SAN) and either the User Principal Name (UPN) or the email address value in the certificate's Subject information. For <code>attribution-name</code>, enter <code>UPN</code> or <code>email</code>. In certificates issued in a Windows environment, the certificate's SAN and UPN contain the username. For example: <code>username@domain</code> Available only when auth-delegation {HTTP-basic kerberos kerberos-constrained-delegation radius-constrained-delegation no-delegation ntlm form-based-delegation} on page 631 is <code>kerberos-constrained-delegation</code>.	SAN
<code>attribution-name {email UPN}</code>	Specify one of the following options to specify the certificate information that FortiWeb uses to determines the client username: <code>email</code>—The email address value in the certificate's Subject information. For field-name {subject SAN} on page 633, enter <code>subject</code> or <code>SAN</code>. <code>UPN</code>—The User Principal Name (UPN) value. For <code>field-name</code>, enter <code>SAN</code>.	UPN

Variable	Description	Default
	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 radius-constrained-delegation no-delegation ntlm form-based-delegation} on page 631 is <code>kerberos-constrained-delegation</code>.	
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: <pre><service_type >/<instance_name>:<port_number>/<service_name></pre> For example, for an Exchange server that belongs to the domain <code>dc1.com</code> and has the hostname <code>USER-U3LOJFPLH1</code>, the SPN is <code>HTTP/USER-U3LOJFPLH1.dc1.com@DC1.COM</code>. Available only when auth-delegation {HTTP-basic kerberos kerberos-constrained-delegation radius-constrained-delegation no-delegation ntlm form-based-delegation} on page 631 is <code>kerberos</code> or <code>kerberos-constrained-delegation</code>.	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. For details, see "waf site-publish-helper keytab file" on page 1. Available only when auth-delegation {HTTP-basic kerberos kerberos-constrained-delegation radius-constrained-delegation no-delegation ntlm form-based-delegation} on page 631 is <code>kerberos-constrained-delegation</code>.	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> on page 634. 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 radius-constrained-delegation no-delegation ntlm form-based-delegation} on page 631 is <code>kerberos-constrained-delegation</code>.	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 <code>prefix-domain "<prefix-domain_str>"</code> on page 635. In some environments, the domain controller requires users to log in with the username format <code>domain\username</code>. For example, if the domain is <code>example.com</code> and the username is <code>user1</code>, the user enters <code>EXAMPLE\user1</code>. Alternatively, enable this option and enter <code>EXAMPLE</code> for <code>prefix-domain "<prefix-domain_str>"</code> on page 635. The user enters <code>user1</code> for the username value and FortiWeb automatically adds <code>EXAMPLE\</code> to the HTTP Authorization: header before it forwards it to the web application. Available only when <code>auth-delegation {HTTP-basic kerberos kerberos-constrained-delegation radius-constrained-delegation no-delegation ntlm form-based-delegation}</code> on page 631 is <code>HTTP-basic</code>, <code>kerberos</code>, or <code>ntlm</code>.	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 <code>prefix-support {enable disable}</code> on page 635 is enabled. If <code>auth-delegation {HTTP-basic kerberos kerberos-constrained-delegation radius-constrained-delegation no-delegation ntlm form-based-delegation}</code> on page 631 is <code>kerberos</code>, ensure that the string is the full domain name (for example, <code>example.com</code>).	No default.
sso-domain "<domain_str>"	Enter the domain suffix of <code>Host :</code> names that will be allowed to share this rule's authentication sessions, such as <code>.example.com</code>. Include the period (<code>.</code>) that precedes the host's name.	No default.
sso-support {enable disable}	Enable for single sign-on support. For example, if this website is <code>www1.example.com</code> and the SSO domain is <code>.example.com</code>, once a client has authenticated with that site, it can access <code>www2.example.com</code> without authenticating a second time.	disable

Variable	Description	Default
	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. If waf site-publish-helper rule on page 626 is enable, this must be disable.	
alert-type {all fail none success}	Specify 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. For details, see log disk on page 66 and log alertMail on page 60.	none
cookieless {enable disable}	Enable to allow Android clients to access to Microsoft Exchange servers through Exchange ActiveSync protocol. Note: If this is enabled, these are restrictions are put in place: • Only HTTP_auth is allowed for client-auth-method {html-form-auth HTTP-auth client-cert-auth saml-auth ntlm-auth} on page 629. • sso-support {enable disable} on page 635 must be disable. • cookie-timeout <timeout_int> on page 631 must be 0. • Only no_delegation, HTTP-basic or kerberos is allowed for auth-delegation {HTTP-basic kerberos kerberos-constrained-delegation radius-constrained-delegation no-delegation ntlm form-based-delegation} on page 631.	disable

Variable	Description	Default
kerberos-type {krb5 spnego}	Two kinds of authorization mechanisms are available, which are used by web servers to retrieve the Kerberos tickets. Available only when Authentication Delegation is Kerberos.	spnego
pass-failed-auth {enable disable}	Enable it so that FortiWeb can be configured when Kerberos Constrained Delegation fails. Available only when client-auth-method {html-form-auth HTTP-auth client-cert-auth saml-auth ntlm-auth} on page 629 is <code>client-cert-auth</code> , and auth-delegation {HTTP-basic kerberos kerberos-constrained-delegation radius-constrained-delegation no-delegation ntlm form-based-delegation} on page 631 is <code>kerberos-constrained-delegation</code> .	disable
append-custom-header {enable disable}	Enable this option to forward the username to the back-end server in HTTP header.	disable
custom-header-name <custom-header-name_str>	Enter a name for the HTTP header. You can change it to any name as you desire, e.g. X-FortiWeb-Uname, useraccount. Special characters are not supported.	X-FortiWeb-Username
custom-header-value-format <custom-header-value-format_str>	Enter the format for the value, such as aaa-USERNAME-bbb, xxx-USERNAME, or USERNAME. Special characters are not supported. It must contain "USERNAME" in the value format. FortiWeb replaces the "USERNAME" with the actual username when forwarding the HTTP header to the back-end server.	xxx-USERNAME-XXX
pass-failed-auth {enable disable}	This option is enabled automatically when the Authentication Delegation is Kerberos Constrained Delegation. When it is disabled and Kerberos Constrained Delegation fails, 500 and Account Failed Authentication pages will be returned.	enable
cache-tgs-ticket {enable disable}	This option is enabled automatically when the Authentication Delegation is Kerberos Constrained Delegation or Kerberos to control whether caching kerberos tgs ticket. When pass-failed-auth {enable disable} on page 637 is disabled, this option will also be disabled.	enable

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

- [waf site-publish-helper policy on page 624](#)
- [waf site-publish-helper authentication-server-pool on page 622](#)
- [log trigger-policy on page 96](#)

- [server-policy allow-hosts on page 106](#)
- [waf web-protection-profile inline-protection on page 696](#)

waf site-publish-helper saml-spool

Use this command to create a pool of SAML servers. For how to create a SAML server, see [user saml-user on page 410](#)

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf site-publish-helper saml-spool
  edit "<saml-server-pool_name>"
    edit <entry_index>
      set server-name <string>
      set saml-server "<string>" on page 639
    next
  end
next
end
```

Variable	Description	Default
"<saml-server-pool_name>"	Enter a name for the SAML server pool that can be referenced by other parts of the configuration. The maximum length is 63 characters. To display the list of existing pools, enter: <code>edit ?</code>	No default.
<entry_index>	Enter the index number of a new or existing server entry in the SAML server pool.	No default.
server-name <string>	Set a name for the SAML server. This name will be shown in the SAML server pool table.	No default.
saml-server "<string>"	Enter the name of the SAML server that you have created with <code>config user saml-user</code> .	No default.

Related topics

- [waf site-publish-helper rule on page 626](#)
- [user saml-user](#)

waf staged_signature_list

Use this command to update the status of the signatures.

Syntax

```
config waf staged_signature_list
  edit signature_id <signature_id_int>
    set status {unapplied | applied | disabled}
  end
```

Variable	Description	Default
signature_id <signature_id_int>	Select the ID that corresponds to the signature.	No default.
status {unapplied applied disabled}	Enable to select an action for the signature. disabled: disable the signature across all the web protection policies. If this signature related rule brings multiple blocks, you can confirm the false positive and enable this option. applied: change the Alert mode of the signature to normal status, with the action as configured in signature protection policy. Unapplied: use this option to cancel the "Disable" and "Approve" operations for a signature.	No default.

Example

This example shows how to update the status of signatures from the FDS update.

```
config waf staged_signature_list
  edit 3
    set status applied
  end
```

Related topics

- [waf signature_update_policy on page 621](#)

waf syntax-based-attack-detection

Using regular expression-based signatures to detect SQL/XSS injection attacks is core to a WAF solution. However, it is a continuous and tedious process to maintain and update the signatures to address new evasion techniques and to tune

false positives and negatives for some attacks. To address this, syntax-based SQL/XSS injection detection is introduced.

Syntax

```
config waf syntax-based-attack-detection
edit "<policy_name>"
    set sql-arithmetic-operation-action {alert | redirect | deny_no_log | alert_deny |
        block_period | send_HTTP_response}
    set detection-target-sql { ARGS_NAMES | ARGS_VALUE | REQUEST_COOKIES | REQUEST_USER_
        AGENT | REQUEST_REFERER | OTHER_REQUEST_HEADERS }
    set sql-arithmetic-operation-block-period <period_int>
    set sql-arithmetic-operation-severity {High | Medium | Low | Info}
    set sql-arithmetic-operation-status {enable | disable}
    set sql-arithmetic-operation-threat-weight {low | critical | informational | moderate |
        substantial | severe}
    set sql-arithmetic-operation-trigger <trigger_policy_name>
    set sql-condition-based-action {alert | redirect | deny_no_log | alert_deny | block_
        period | send_HTTP_response}
    set sql-condition-based-block-period <period_int>
    set sql-condition-based-severity {High | Medium | Low | Info}
    set sql-condition-based-status {enable | disable}
    set sql-condition-based-threat-weight {low | critical | informational | moderate |
        substantial | severe}
    set sql-condition-based-trigger <trigger_policy_name>
    set sql-embedded-queries-action {alert | redirect | deny_no_log | alert_deny | block_
        period | send_HTTP_response}
    set sql-embedded-queries-block-period <period_int>
    set sql-embedded-queries-severity {High | Medium | Low | Info}
    set sql-embedded-queries-status {enable | disable}
    set sql-embedded-queries-threat-weight {low | critical | informational | moderate |
        substantial | severe}
    set sql-embedded-queries-trigger <trigger_policy_name>
    set sql-function-based-action {alert | redirect | deny_no_log | alert_deny | block_
        period | send_HTTP_response}
    set sql-function-based-block-period <period_int>
    set sql-function-based-severity {High | Medium | Low | Info}
    set sql-function-based-status {enable | disable}
    set sql-function-based-threat-weight {low | critical | informational | moderate |
        substantial | severe}
    set sql-function-based-trigger <trigger_policy_name>
    set sql-line-comments-action {alert | redirect | deny_no_log | alert_deny | block_
        period | send_HTTP_response}
    set sql-line-comments-block-period <period_int>
    set sql-line-comments-severity {High | Medium | Low | Info}
    set sql-line-comments-status {enable | disable}
    set sql-line-comments-threat-weight {low | critical | informational | moderate |
        substantial | severe}
    set sql-line-comments-trigger <trigger_policy_name>
    set sql-stacked-queries-action {alert | redirect | deny_no_log | alert_deny | block_
        period | send_HTTP_response}
    set sql-stacked-queries-block-period <period_int>
    set sql-stacked-queries-severity {High | Medium | Low | Info}
    set sql-stacked-queries-status {enable | disable}
    set sql-stacked-queries-threat-weight {low | critical | informational | moderate |
        substantial | severe}
```

```
set sql-stacked-queries-trigger <trigger_policy_name>
set xss-html-attribute-based-action {alert | redirect | deny_no_log | alert_deny |
    block_period | send_HTTP_response}
set detection-target-xss { ARGS_NAMES | ARGS_VALUE | REQUEST_COOKIES | REQUEST_USER_
    AGENT | REQUEST_REFERER | OTHER_REQUEST_HEADERS }
set xss-html-attribute-based-block-period <period_int>
set xss-html-attribute-based-severity {High | Medium | Low | Info}
set xss-html-attribute-based-status {enable | disable}
set xss-html-attribute-based-threat-weight {low | critical | informational | moderate
    | substantial | severe}
set xss-html-attribute-based-trigger <trigger_policy_name>
set xss-html-css-based-action {alert | redirect | deny_no_log | alert_deny | block_
    period | send_HTTP_response}
set xss-html-css-based-block-period <period_int>
set xss-html-css-based-severity {High | Medium | Low | Info}
set xss-html-css-based-status {enable | disable}
set xss-html-css-based-threat-weight {low | critical | informational | moderate |
    substantial | severe}
set xss-html-css-based-trigger <trigger_policy_name>
set xss-html-tag-based-action {alert | redirect | deny_no_log | alert_deny | block_
    period | send_HTTP_response}
set xss-html-tag-based-block-period <period_int>
set xss-html-tag-based-check-level {strict | moderate}
set xss-html-tag-based-severity {High | Medium | Low | Info}
set xss-html-tag-based-status {enable | disable}
set xss-html-tag-based-threat-weight {low | critical | informational | moderate |
    substantial | severe}
set xss-html-tag-based-trigger <trigger_policy_name>
set xss-javascript-function-based-action {alert | redirect | deny_no_log | alert_deny
    | block_period | send_HTTP_response}
set xss-javascript-function-based-block-period <period_int>
set xss-javascript-function-based-severity {High | Medium | Low | Info}
set xss-javascript-function-based-status {enable | disable}
set xss-javascript-function-based-threat-weight {low | critical | informational |
    moderate | substantial | severe}
set xss-javascript-function-based-trigger <trigger_policy_name>
set xss-javascript-variable-based-action {alert | redirect | deny_no_log | alert_deny
    | block_period | send_HTTP_response}
set xss-javascript-variable-based-block-period <period_int>
set xss-javascript-variable-based-severity {High | Medium | Low | Info}
set xss-javascript-variable-based-status {enable | disable}
set xss-javascript-variable-based-threat-weight {low | critical | informational |
    moderate | substantial | severe}
set xss-javascript-variable-based-trigger <trigger_policy_name>
config exception-element-list
    edit "<list-id>"
        set match-target {HOST | URI | FULL-URL | PARAMETER | COOKIE}
        set operator {STRING_MATCH| REGEXP_MATCH}
        set value-name <name_str>
        set value-check {enable | disable}
        set value <value_str>
        set concatenate-type {AND | OR}
        set attack-type {arithmetic_operation_based_boolean_injection | condition_based_
            boolean_injection | embeded_queries_sql_injection | html_attr_based_xss_
            injection | html_css_based_xss_injection | html_tag_based_xss_injection |
            js_func_based_xss_injection | js_var_based_xss_injection | line_comments |
            invalid | sql_function_based_boolean_injection | stacked_queries_sql_
            injection}
```

```

        next
    end
    next
end

```

Variable	Description	Default
"<policy_name>"	Enter a name for the syntax based detection policy.	No default
sql-arithmetic-operation-action {alert redirect deny_no_log alert_deny block_period send_HTTP_response}	Select the action FortiWeb takes when this injection type attack is identified. 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. For details, see system replacemsg-image on page 366. deny_no_log—Block the request (or reset the connection). redirect—Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. block_period—Block subsequent requests from the client for a number of seconds. Also configure sql-arithmetic-operation-block-period <period_int> on page 644. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see system replacemsg-image on page 366. send_HTTP_response—Block and reply to the client with an HTTP error message and generate an alert email and/or log message. Note: Logging and/or alert email will occur only if enabled and configured. See log on page 784 and log alertMail on page 60.	alert_deny
detection-target-sql { ARGS_NAMES ARGS_VALUE REQUEST_COOKIES REQUEST_USER_AGENT REQUEST_REFERER OTHER_REQUEST_HEADERS }	Select the elements in the request that you want FortiWeb to scan: - Parameter Name - Parameter Value - Request Cookie - Request User-Agent - Request Referer - Other Request Header You can select multiple elements, for example, set <code>detection-target-sql ARGS_NAMES REQUEST_COOKIES ARGS_VALUE</code>.	Parameter Name/Parameter Value/Request Cookie

Variable	Description	Default
sql-arithmetic-operation-block-period <period_int>	Enter the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects this injection type attack.	600
sql-arithmetic-operation-severity {High Medium Low Info}	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs an injection attack: - High - Medium - Low - Info	High
sql-arithmetic-operation-status {enable disable}	Enable or disable the attack type detection for this rule.	enable
sql-arithmetic-operation-threat-weight {low critical informational moderate substantial severe}	Set the threat weight for Arithmetic Operation Based Boolean Injection attack.	severe
sql-arithmetic-operation-trigger <trigger_policy_name>	Enter the name of the trigger to apply when this policy is violated. For details, see log trigger-policy on page 96 . To display the list of existing triggers, enter: <code>set trigger ?</code>	No default
sql-condition-based-action {alert redirect deny_no_log alert_deny block_period send_HTTP_response}	Select the action FortiWeb takes when this injection type attack is identified. <code>alert</code>—Accept the request and generate an alert email and/or log message. <code>alert_deny</code>—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. For details, see system replacemsg-image on page 366. <code>deny_no_log</code>—Block the request (or reset the connection). <code>redirect</code>—Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. <code>block_period</code>—Block subsequent requests from the client for a number of seconds. Also configure sql-condition-based-block-period <period_int> on page 645.	alert_deny

Variable	Description	Default
	You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see system replacemsg-image on page 366. <code>send_HTTP_response</code>—Block and reply to the client with an HTTP error message and generate an alert email and/or log message. Note: Logging and/or alert email will occur only if enabled and configured. See log on page 784 and log alertMail on page 60.	
<code>sql-condition-based-block-period <period_int></code>	Enter the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects this injection type attack.	600
<code>sql-condition-based-severity {High Medium Low Info}</code>	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs an injection attack: - High - Medium - Low - Info	High
<code>sql-condition-based-status {enable disable}</code>	Enable or disable the attack type detection for this rule.	enable
<code>sql-condition-based-threat-weight {low critical informational moderate substantial severe}</code>	Set the threat weight for Arithmetic Operation Based Boolean Injection attack.	severe
<code>sql-condition-based-trigger <trigger_policy_name></code>	Enter the name of the trigger to apply when this policy is violated. For details, see log trigger-policy on page 96. To display the list of existing triggers, enter: <pre>set trigger ?</pre>	No default
<code>sql-embedded-queries-action {alert redirect deny_no_log alert_deny block_period send_HTTP_response}</code>	Select the action FortiWeb takes when this injection type attack is identified. <code>alert</code>—Accept the request and generate an alert email and/or log message. <code>alert_deny</code>—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. For details, see system replacemsg-image on page 366.	alert_deny

Variable	Description	Default
	<code>deny_no_log</code>—Block the request (or reset the connection). <code>redirect</code>—Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. <code>block_period</code>—Block subsequent requests from the client for a number of seconds. Also configure sql-embedded-queries-block-period <period_int> on page 646. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see system replacemsg-image on page 366. <code>send_HTTP_response</code>—Block and reply to the client with an HTTP error message and generate an alert email and/or log message. Note: Logging and/or alert email will occur only if enabled and configured. See log on page 784 and log alertMail on page 60.	
<code>sql-embedded-queries-block-period <period_int></code>	Enter the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects this injection type attack.	600
<code>sql-embedded-queries-severity</code> {High Medium Low Info}	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs an injection attack: - High - Medium - Low - Info	High
<code>sql-embedded-queries-status</code> {enable disable}	Enable or disable the attack type detection for this rule.	enable
<code>sql-embedded-queries-threat-weight</code> {low critical informational moderate substantial severe}	Set the threat weight for Embedded Queries SQL Injection attack.	severe
<code>sql-embedded-queries-trigger <trigger_policy_name></code>	Enter the name of the trigger to apply when this policy is violated. For details, see log trigger-policy on page 96. To display the list of existing triggers, enter: <code>set trigger ?</code>	No default

Variable	Description	Default
sql-function-based-action {alert redirect deny_no_log alert_deny block_period send_HTTP_response}	Select the action FortiWeb takes when this injection type attack is identified. 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. For details, see system_replacemsg-image on page 366. deny_no_log—Block the request (or reset the connection). redirect—Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. block_period—Block subsequent requests from the client for a number of seconds. Also configure sql-function-based-block-period <period_int> on page 647. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see system_replacemsg-image on page 366. send_HTTP_response—Block and reply to the client with an HTTP error message and generate an alert email and/or log message. Note: Logging and/or alert email will occur only if enabled and configured. See log on page 784 and log alertMail on page 60.	alert_deny
sql-function-based-block-period <period_int>	Enter the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects this injection type attack.	600
sql-function-based-severity {High Medium Low Info}	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs an injection attack: - High - Medium - Low - Info	High
sql-function-based-status {enable disable}	Enable or disable the attack type detection for this rule.	enable

Variable	Description	Default
sql-function-based-threat-weight {low critical informational moderate substantial severe}	Set the threat weight for SQL Function Based Boolean Injection attack.	severe
sql-function-based-trigger <trigger_policy_name>	Enter the name of the trigger to apply when this policy is violated. For details, see log trigger-policy on page 96 . To display the list of existing triggers, enter: <code>set trigger ?</code>	No default
sql-line-comments-action {alert redirect deny_no_log alert_deny block_period send_HTTP_response}	Select the action FortiWeb takes when this injection type attack is identified. <code>alert</code>—Accept the request and generate an alert email and/or log message. <code>alert_deny</code>—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. For details, see system replacemsg-image on page 366. <code>deny_no_log</code>—Block the request (or reset the connection). <code>redirect</code>—Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. <code>block_period</code>—Block subsequent requests from the client for a number of seconds. Also configure sql-line-comments-block-period <period_int> on page 648. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see system replacemsg-image on page 366. <code>send_HTTP_response</code>—Block and reply to the client with an HTTP error message and generate an alert email and/or log message. Note: Logging and/or alert email will occur only if enabled and configured. See log on page 784 and log alertMail on page 60.	alert_deny
sql-line-comments-block-period <period_int>	Enter the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects this injection type attack.	600

Variable	Description	Default
sql-line-comments-severity {High Medium Low Info}	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs an injection attack: - High - Medium - Low - Info	High
sql-line-comments-status {enable disable}	Enable or disable the attack type detection for this rule.	enable
sql-line-comments-threat-weight {low critical informational moderate substantial severe}	Set the threat weight for Line Comments attack.	severe
sql-line-comments-trigger <trigger_policy_name>	Enter the name of the trigger to apply when this policy is violated. For details, see log trigger-policy on page 96 . To display the list of existing triggers, enter: <code>set trigger ?</code>	No default
sql-stacked-queries-action {alert redirect deny_no_log alert_deny block_period send_HTTP_response}	Select the action FortiWeb takes when this injection type attack is identified. <code>alert</code>—Accept the request and generate an alert email and/or log message. <code>alert_deny</code>—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. For details, see system replacemsg-image on page 366. <code>deny_no_log</code>—Block the request (or reset the connection). <code>redirect</code>—Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. <code>block_period</code>—Block subsequent requests from the client for a number of seconds. Also configure sql-stacked-queries-block-period <period_int> on page 650. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see system replacemsg-image on page 366. <code>send_HTTP_response</code>—Block and reply to the	alert_deny

Variable	Description	Default
	client with an HTTP error message and generate an alert email and/or log message. Note: Logging and/or alert email will occur only if enabled and configured. See log on page 784 and log alertMail on page 60.	
sql-stacked-queries-block-period <period_int>	Enter the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects this injection type attack.	600
sql-stacked-queries-severity {High Medium Low Info}	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs an injection attack: • High • Medium • Low • Info	High
sql-stacked-queries-status {enable disable}	Enable or disable the attack type detection for this rule.	enable
sql-stacked-queries-threat-weight {low critical informational moderate substantial severe}	Set the threat weight for Stacked Queries SQL Injection attack.	severe
sql-stacked-queries-trigger <trigger_policy_name>	Enter the name of the trigger to apply when this policy is violated. For details, see log trigger-policy on page 96. To display the list of existing triggers, enter: <pre>set trigger ?</pre>	No default
xss-html-attribute-based-action {alert redirect deny_no_log alert_deny block_period send_HTTP_response}	Select the action FortiWeb takes when this injection type attack is identified. • <code>alert</code>—Accept the request and generate an alert email and/or log message. • <code>alert_deny</code>—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. For details, see system replacemsg-image on page 366. • <code>deny_no_log</code>—Block the request (or reset the connection). • <code>redirect</code>—Redirect the request to the URL that you specify in the protection profile and generate an alert	alert_deny

Variable	Description	Default
	email and/or log message. <code>block_period</code>—Block subsequent requests from the client for a number of seconds. Also configure <code>xss-html-attribute-based-block-period <period_int></code> on page 651. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see system replacemsg-image on page 366. <code>send_HTTP_response</code>—Block and reply to the client with an HTTP error message and generate an alert email and/or log message. Note: Logging and/or alert email will occur only if enabled and configured. See log on page 784 and log alertMail on page 60.	
<code>detection-target-xss {</code> <code> ARGS_NAMES </code> <code> ARGS_VALUE </code> <code> REQUEST_</code> <code> COOKIES </code> <code> REQUEST_USER_</code> <code> AGENT REQUEST_</code> <code> REFERER OTHER_</code> <code> REQUEST_</code> <code> HEADERS }</code>	Select the elements in the request that you want FortiWeb to scan: - Parameter Name - Parameter Value - Request Cookie - Request User-Agent - Request Referer - Other Request Header You can select multiple elements, for example, set <code>detection-target-xss ARGS_NAMES REQUEST_COOKIES ARGS_VALUE</code>.	Parameter Name/Parameter Value/Request Cookie
<code>xss-html-attribute-based-block-period <period_int></code>	Enter the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects this injection type attack.	600
<code>xss-html-attribute-based-severity {High Medium Low Info}</code>	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs an injection attack: - High - Medium - Low - Info	High
<code>xss-html-attribute-based-status {enable disable}</code>	Enable or disable the attack type detection for this rule.	enable

Variable	Description	Default
xss-html-attribute-based-threat-weight {low critical informational moderate substantial severe}	Set the threat weight for HTML Attribute Based XSS Injection attack.	severe
xss-html-attribute-based-trigger <trigger_policy_name>	Enter the name of the trigger to apply when this policy is violated. For details, see log trigger-policy on page 96 . To display the list of existing triggers, enter: set trigger ?	No default
xss-html-css-based-action {alert redirect deny_no_log alert_deny block_period send_HTTP_response}	Select the action FortiWeb takes when this injection type attack is identified. • 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. For details, see system replacemsg-image on page 366. • deny_no_log—Block the request (or reset the connection). • redirect—Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. • block_period—Block subsequent requests from the client for a number of seconds. Also configure xss-html-css-based-block-period <period_int> on page 652. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see system replacemsg-image on page 366. • send_HTTP_response—Block and reply to the client with an HTTP error message and generate an alert email and/or log message. Note: Logging and/or alert email will occur only if enabled and configured. See log on page 784 and log alertMail on page 60.	alert_deny
xss-html-css-based-block-period <period_int>	Enter the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects this injection type attack.	600

Variable	Description	Default
xss-html-css-based-severity {High Medium Low Info}	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs an injection attack: - High - Medium - Low - Info	High
xss-html-css-based-status {enable disable}	Enable or disable the attack type detection for this rule.	enable
xss-html-css-based-threat-weight {low critical informational moderate substantial severe}	Set the threat weight for HTML CSS Based XSS Injection attack.	severe
xss-html-css-based-trigger <trigger_policy_name>	Enter the name of the trigger to apply when this policy is violated. For details, see log trigger-policy on page 96 . To display the list of existing triggers, enter: set trigger ?	No default
xss-html-tag-based-action {alert redirect deny_no_log alert_deny block_period send_HTTP_response}	Select the action FortiWeb takes when this injection type attack is identified. <code>alert</code>—Accept the request and generate an alert email and/or log message. <code>alert_deny</code>—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. For details, see system replacemsg-image on page 366. <code>deny_no_log</code>—Block the request (or reset the connection). <code>redirect</code>—Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. <code>block_period</code>—Block subsequent requests from the client for a number of seconds. Also configure xss-html-tag-based-block-period <period_int> on page 654. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see system replacemsg-image on page 366. <code>send_HTTP_response</code>—Block and reply to the	alert_deny

Variable	Description	Default
	client with an HTTP error message and generate an alert email and/or log message. Note: Logging and/or alert email will occur only if enabled and configured. See log on page 784 and log alertMail on page 60.	
xss-html-tag-based-block-period <period_int>	Enter the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects this injection type attack.	600
xss-html-tag-based-check-level {strict moderate}	<code>moderate</code>—An injection attack will be reported when tags besides body/head/html are detected. <code>strict</code>—No injection attack will be reported when tags besides body/head/html are detected. Note: It is not advised to set it as <code>moderate</code> as false positives may occur.	strict
xss-html-tag-based-severity {High Medium Low Info}	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs an injection attack: - High - Medium - Low - Info	High
xss-html-tag-based-status {enable disable}	Enable or disable the attack type detection for this rule.	enable
xss-html-tag-based-threat-weight {low critical informational moderate substantial severe}	Set the threat weight for HTML Tag Based XSS Injection attack.	severe
xss-html-tag-based-trigger <trigger_policy_name>	Enter the name of the trigger to apply when this policy is violated. For details, see log trigger-policy on page 96. To display the list of existing triggers, enter: <pre>set trigger ?</pre>	No default
xss-javascript-function-based-action {alert redirect deny_no_log alert_deny block_period send_HTTP_response}	Select the action FortiWeb takes when this injection type attack is identified. <code>alert</code>—Accept the request and generate an alert email and/or log message. <code>alert_deny</code>—Block the request (or reset the connection) and generate an alert email and/or log message.	alert_deny

Variable	Description	Default
	You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see system replacemsg-image on page 366. • <code>deny_no_log</code>—Block the request (or reset the connection). • <code>redirect</code>—Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. • <code>block_period</code>—Block subsequent requests from the client for a number of seconds. Also configure xss-javascript-function-based-block-period <period_int> on page 655. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see system replacemsg-image on page 366. • <code>send_HTTP_response</code>—Block and reply to the client with an HTTP error message and generate an alert email and/or log message. Note: Logging and/or alert email will occur only if enabled and configured. See log on page 784 and log alertMail on page 60.	
<code>xss-javascript-function-based-block-period <period_int></code>	Enter the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects this injection type attack.	600
<code>xss-javascript-function-based-severity {High Medium Low Info}</code>	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs an injection attack: • High • Medium • Low • Info	High
<code>xss-javascript-function-based-status {enable disable}</code>	Enable or disable the attack type detection for this rule.	enable
<code>xss-javascript-function-based-threat-weight {low critical informational moderate substantial severe}</code>	Set the threat weight for Javascript Function Based XSS Injection attack.	severe

Variable	Description	Default
xss-javascript-function-based-trigger <trigger_policy_name>	Enter the name of the trigger to apply when this policy is violated. For details, see log trigger-policy on page 96 . To display the list of existing triggers, enter: <pre>set trigger ?</pre>	No default
xss-javascript-variable-based-action {alert redirect deny_no_log alert_deny block_period send_HTTP_response}	Select the action FortiWeb takes when this injection type attack is identified. 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. For details, see system replacemsg-image on page 366. deny_no_log—Block the request (or reset the connection). redirect—Redirect the request to the URL that you specify in the protection profile and generate an alert email and/or log message. block_period—Block subsequent requests from the client for a number of seconds. Also configure xss-javascript-variable-based-block-period <period_int> on page 656. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see system replacemsg-image on page 366. send_HTTP_response—Block and reply to the client with an HTTP error message and generate an alert email and/or log message. Note: Logging and/or alert email will occur only if enabled and configured. See log on page 784 and log alertMail on page 60.	alert_deny
xss-javascript-variable-based-block-period <period_int>	Enter the number of seconds that you want to block subsequent requests from the client after the FortiWeb appliance detects this injection type attack.	600
xss-javascript-variable-based-severity {High Medium Low Info}	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs an injection attack: - High - Medium - Low - Info	High

Variable	Description	Default
xss-javascript-variable-based-status {enable disable}	Enable or disable the attack type detection for this rule.	enable
xss-javascript-variable-based-threat-weight {low critical informational moderate substantial severe}	Set the threat weight for Javascript Variable Based XSS Injection attack.	severe
xss-javascript-variable-based-trigger <trigger_policy_name>	Enter the name of the trigger to apply when this policy is violated. For details, see log trigger-policy on page 96 . To display the list of existing triggers, enter: set trigger ?	No default
"<list-id>"	Enter an ID for the exception list.	No default
match-target {HOST URI FULL-URL PARAMETER COOKIE}	Select the type of request element to exempt from this rule.	URI
operator {STRING_MATCH REGEXP_MATCH}	- STRING_MATCH—Name is the literal name of a parameter. - REGEXP_MATCH— Name is a regular expression that matches all and only the name of the parameter that the exception applies to.	REGEXP_MATCH
value-name <name_str>	Specify the name of the parameter to match.	
value-check {enable disable}	Enable to specify a parameter value to match in addition to the parameter name.	disable
value <value_str>	Specify a HOST/URI/FULL-URL/PARAMETER/COOKIE value to match.	No default
concatenate-type {AND OR}	- AND—A matching request matches this entry in addition to other entries in the exemption list. - OR—A matching request matches this entry instead of other entries in the exemption list. Later, you can use the exception list options to adjust the matching sequence for entries.	AND

Variable	Description	Default
attack-type {arithmetic_ operation_based_ boolean_injection condition_based_ boolean_injection embedded_queries_ sql_injection html_ attr_based_xss_ injection html_css_ based_xss_injection html_tag_based_ xss_injection js_ func_based_xss_ injection js_var_ based_xss_injection line_comments invalid sql_function_ based_boolean_ injection stacked_ queries_sql_ injection}	Select the attack type you want to create the exception for.	No default

Related topics

- [waf web-protection-profile inline-protection on page 696](#)

waf threshold-based-detection

Use this command to configure threshold based detection rules to define occurrence, time period, severity, and trigger policy, etc of the following suspicious behaviors, and thus FortiWeb judges whether the request comes from a human or a bot.

- Crawler
- Vulnerability Scanning
- Slow Attack
- Content Scraping
- Illegal User Scan

Syntax

```
config waf threshold-based-detection
edit "<policy_name>"
```

```

set bot-recognition {disabled | real-browser-enforcement | captcha-enforcement |
    recaptcha-enforcement}
set recaptcha <recaptcha_server_name>
set mobile-app-identification {disabled | mobile-token-validation}
set bot-confirmation {enable | disable}
set validation-timeout <validation-timeout_int>
set set set set max-attempt-times <max-attempt-times_int>
set crawler-detection {enable | disable}
set crawler-action {alert | deny_no_log | alert_deny | block-period}
set crawler-severity {High | Medium | Low | Info}
set crawler-trigger <crawler-trigger-policy_name>
set crawler-occurrence-num <crawler-occurrence-num_int>
set crawler-within <crawler-within_int>
set crawler-block-period <crawler-block-period_int>
set scanner-detection {enable | disable}
set scanner-action {alert | deny_no_log | alert_deny | block-period}
set scanner-severity {High | Medium | Low | Info}
set crawler-trigger <crawler-trigger-policy_name>
set scanner-occurrence-num <scanner-occurrence-num_int>
set scanner-within <scanner-within_int>
set scanner-block-period <scanner-block-period_int>
set slow-attack-detection {enable | disable}
set slow-attack-action {alert | deny_no_log | alert_deny | block-period}
set slow-attack-severity {High | Medium | Low | Info}
set slow-attack-trigger <slow-attack-trigger-policy_name>
set slow-attack-occurrence-num <slow-attack-occurrence-num_int>
set slow-attack-within <slow-attack-within_int>
set slow-attack-HTTP-transaction-timeout <slow-attack-HTTP-transaction-timeout_
    int>
set slow-attack-packet-interval-timeout <slow-attack-packet-interval-timeout_int>
set slow-attack-block-period <slow-attack-block-period_int>
set content-scraping-detection {enable | disable}
set content-scraping-action {alert | deny_no_log | alert_deny | block-period}
set content-scraping-severity {High | Medium | Low | Info}
set content-scraping-trigger <content-scraping-trigger-policy_name>
set content-scraping-occurrence-num <content-scraping-occurrence-num_int>
set content-scraping-within <content-scraping-within_int>
set content-scraping-block-period <content-scraping-block-period_int>
set keep-occurrence-count {enable | disable}
next
end

```

Variable	Description	Default
"<policy_name>"	Enter a name for the threshold based detection rule that can be referenced in bot mitigation policy.	No default.
bot-recognition {disabled real-browser-enforcement captcha-enforcement recaptcha-enforcement}	Select between: - captcha-enforcement—Requires the client to successfully fulfill a CAPTCHA request. If the client cannot successfully fulfill the request within the , or doesn't fulfill the request within the validation-timeout <validation-timeout_int>, FortiWeb applies the action and sends the CAPTCHA block page. - real-browser-enforcement—Enable to return a	disabled

Variable	Description	Default
	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 waf threshold-based-detection on page 658, FortiWeb applies the specified action. If the client appears to be a web browser, FortiWeb allows the client to violate the rule. <code>recaptcha-enforcement</code>—Requires the client to successfully fulfill a reCAPTCHA request. If the client cannot successfully fulfill the request within the , or doesn't fulfill the request within the validation-timeout <validation-timeout_int>, FortiWeb applies the action and sends the CAPTCHA block page. <code>disable</code>—Not to carry out the bot verification.	
<code>recaptcha <recaptcha_server_name></code>	Enter the reCAPTCHA server you have created through user recaptcha-user	No default.
<code>mobile-app-identification {disabled mobile-token-validation}</code>	<code>disabled</code>—Not to carry out the mobile token verification. <code>mobile-token-validation</code>—Requires the client to use mobile token to verify whether the traffic is from mobile devices. To apply mobile token validation, you must enable mobile-app-identification in waf web-protection-profile inline-protection.	disabled
<code>bot-confirmation {enable disable}</code>	Enable to confirm if the client is indeed a bot. The system sends RBE (Real Browser Enforcement) JavaScript or CAPTCHA to the client to double check if it's a bot.	disable
<code>validation-timeout <validation-timeout_int></code>	Enter the maximum amount of time (in seconds) that FortiWeb waits for results from the client. Available only when the bot-recognition {disabled real-browser-enforcement captcha-enforcement recaptcha-enforcement} is browser-enforcement or captcha-enforcement.	20
<code>crawler-detection {enable disable}</code>	Enable to detect tools that browse your web site for indexing purposes.	enable
<code>crawler-action {alert deny_no_log alert_deny block-period}</code>	Select which action FortiWeb will take when it detects a crawler: <code>alert</code>—Accept the connection and generate an alert email and/or log message. <code>alert_deny</code>—Block the request (or reset the connection) and generate an alert and/or log message. <code>deny_no_log</code>—Block the request (or reset the connection).	alert

Variable	Description	Default
	<code>block-period</code>—Block subsequent requests from the client for a number of seconds. Also configure <code>crawler-block-period <crawler-block-period_int></code>.	
<code>crawler-severity {High Medium Low Info}</code>	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs a crawler: - Informative - Low - Medium - High	Medium
<code>crawler-trigger <crawler-trigger-policy_name></code>	Select the trigger, if any, that FortiWeb will use when it logs and/or sends an alert email about a crawler. For details, see "Viewing log messages" on page 1.	No default.
<code>crawler-occurrence-num <crawler-occurrence-num_int></code>	Define the frequency that FortiWeb detects 403 and 404 response codes returned by the web server.	100
<code>crawler-within <crawler-within_int></code>	Specify the time period, in seconds, during which FortiWeb detects the 403 and 404 response codes.	10
<code>crawler-block-period <crawler-block-period_int></code>	Enter the number of seconds that you want to block subsequent requests from a client after FortiWeb detects a crawler. The valid range is 1–3,600 seconds. Available only if <code>crawler-action {alert deny_no_log alert_deny block-period}</code> is set to <code>block-period</code>.	600
<code>scanner-detection {enable disable}</code>	Enable to detect tools that scan your web site for vulnerabilities.	disable
<code>scanner-action {alert deny_no_log alert_deny block-period}</code>	Select which action FortiWeb will take when it detects attack signatures: <code>alert</code>—Accept the connection and generate an alert email and/or log message. <code>alert_deny</code>—Block the request (or reset the connection) and generate an alert and/or log message. <code>deny_no_log</code>—Block the request (or reset the connection). <code>block-period</code>—Block subsequent requests from the client for a number of seconds. Also configure <code>scanner-block-period <scanner-block-period_int></code>.	alert
<code>scanner-severity {High Medium Low Info}</code>	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs attack signatures: Informative	Medium

Variable	Description	Default
	- Low - Medium - High	
scanner-trigger <scanner-trigger-policy_name>	Select the trigger, if any, that FortiWeb will use when it logs and/or sends an alert email about attack signatures. For details, see "Viewing log messages" on page 1.	No default.
scanner-occurrence-num <scanner-occurrence-num_int>	Define the frequency that FortiWeb detects attack signatures.	100
scanner-within <scanner-within_int>	Specify the time period, in seconds, during which FortiWeb monitors the attack signatures.	10
scanner-block-period <scanner-block-period_int>	Enter the number of seconds that you want to block subsequent requests from a client after FortiWeb detects attack signatures. The valid range is 1–3,600 seconds. Available only if scanner-action {alert deny_no_log alert_deny block-period} is set to <code>block-period</code> .	600
slow-attack-detection {enable disable}	Enable to detect Denial of Service tools that try to go undetected by generating a small stream of traffic.	disable
slow-attack-action {alert deny_no_log alert_deny block-period}	Select which action FortiWeb will take when it detects slow attack activities: <code>alert</code>—Accept the connection and generate an alert email and/or log message. <code>alert_deny</code>—Block the request (or reset the connection) and generate an alert and/or log message. <code>deny_no_log</code>—Block the request (or reset the connection). <code>block-period</code>—Block subsequent requests from the client for a number of seconds. Also configure slow-attack-block-period <slow-attack-block-period_int>.	
slow-attack-severity {High Medium Low Info}	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs slow attack activities: - Informative - Low - Medium - High	Medium
slow-attack-trigger <slow-attack-trigger-policy_name>	Select the trigger, if any, that FortiWeb will use when it logs and/or sends an alert email about slow attack activities. For details, see "Viewing log messages" on page 1.	No default.

Variable	Description	Default
slow-attack-occurrence-num <slow-attack-occurrence-num_int>	Define the frequency that FortiWeb detects slow attack activities.	5
slow-attack-within <slow-attack-within_int>	Specify the time period, in seconds, during which FortiWeb detects slow attack activities.	100
slow-attack-HTTP-transaction-timeout <slow-attack-HTTP-transaction-timeout_int>	Specify a timeout value, in seconds, for the HTTP transaction.	60
slow-attack-packet-interval-timeout <slow-attack-packet-interval-timeout_int>	Specify the timeout value, in seconds, for interval between packets arriving from either the client or server (request or response packets).	10
slow-attack-block-period <slow-attack-block-period_int>	Enter the number of seconds that you want to block subsequent requests from a client after FortiWeb detects slow attack activities. The valid range is 1–3,600 seconds. Available only if slow-attack-action {alert deny_no_log alert_deny block-period} is set to <code>block-period</code> .	600
content-scraping-detection {enable disable}	Enable to detect bots that illegally copy contents from your web site.	disable
content-scraping-action {alert deny_no_log alert_deny block-period}	Select which action FortiWeb will take when it detects content scraping activities: <code>alert</code>—Accept the connection and generate an alert email and/or log message. <code>alert_deny</code>—Block the request (or reset the connection) and generate an alert and/or log message. <code>deny_no_log</code>—Block the request (or reset the connection). <code>block-period</code>—Block subsequent requests from the client for a number of seconds. Also configure content-scraping-block-period <content-scraping-block-period_int>.	alert
content-scraping-severity {High Medium Low Info}	When policy violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb will use when it logs content scraping activities: - Informative - Low - Medium - High	Medium

Variable	Description	Default
content-scraping-trigger <content-scraping-trigger-policy_name>	Select the trigger, if any, that FortiWeb will use when it logs and/or sends an alert email about content scraping activities. For details, see "Viewing log messages" on page 1.	No default.
content-scraping-occurrence-num <content-scraping-occurrence-num_int>	Define the frequency that FortiWeb detects content scraping activities.	100
content-scraping-within <content-scraping-within_int>	Specify the time period, in seconds, during which FortiWeb detects content scraping activities.	30
content-scraping-block-period <content-scraping-block-period_int>	Enter the number of seconds that you want to block subsequent requests from a client after FortiWeb detects content scraping activities. The valid range is 1–3,600 seconds. Available only if content-scraping-action {alert deny_no_log alert_deny block-period} is set to <code>block-period</code> .	600
keep-occurrence-count {enable disable}	Enable this option so that the threshold counter will not be reset throughout the Within (Seconds) timeframe. FortiWeb can continue denying or period-blocking the client as long as it has ever reached the threshold within the "Within (Seconds)" timeframe.	disable

Related Topics

- [waf bot-mitigation-policy](#) on page 459
- [waf biometrics-based-detection](#) on page 442
- [waf bot-deception](#) on page 1

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. For details, see [waf url-access url-access-rule](#) on page 669.

To apply URL access policies, select them within an inline or Offline Protection profile. For details, see [waf web-protection-profile inline-protection](#) on page 696 or [waf web-protection-profile offline-protection](#) on page 706.

You can use SNMP traps to notify you when a URL access rule is enforced. For details, see [system snmp community](#) on page 375.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions](#) on page 46.

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>"	Enter the name of the new or existing URL access policy. The maximum length is 63 characters. To display the list of existing policies, enter: edit ?	No default.
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999.	No default.
url-access-rule-name "<url-access-rule_name>"	Enter the name of the existing URL access rule to add to the policy. The maximum length is 63 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

- [waf url-access url-access-rule on page 669](#)
- [waf web-protection-profile inline-protection on page 696](#)
- [waf web-protection-profile offline-protection on page 706](#)

waf url-encryption

To prevent users from forceful browsing, you can now encrypt the URLs, which can ensure that the internal directory structure of the web application is not revealed to users.

Use this command to create URL encryption rules and policies.

Syntax

```
config waf url-encryption url-encryption-rule
  edit "<encryption-rule_name>"
    set host-status {enable | disable}
    set host <host_str>
    set allow-unencrypted {enable | disable}
    set action {alert | deny_no_log | alert_deny | block-period}
    set block-period <block-period_int>
    set severity {High | Medium | Low | Info}
    set trigger <trigger_str>
    config url-list
      edit "<url-list_id>"
        set url-type {plain | regular}
        set url-pattern <url-pattern_str>
      end
    config exceptions
      edit "<exceptions-item_id>"
        set url-type {plain | regular}
        set url-pattern <url-pattern_str>
      end
    end
  next
end

config waf url-encryption url-encryption-policy
  edit "<url-encryption-policy_name>"
    set full-mode {enable | disable}
    config rule-list
      edit "<rule-list_id>"
        set rule <rule_str>
      end
    end
  next
end
```

Variable	Description	Default
"<encryption-rule_name>"	Enter a name for the encryption rule.	No default.
host-status {enable disable}	Enable to require that the <code>Host:</code> field of the HTTP request match a protected host names entry in order to match the URL acceleration rule. Also configure host <host_str> .	disable
host <host_str>	Select which protected host names entry (either a web host name or IP address) that the <code>Host:</code> field of the HTTP	No default.

Variable	Description	Default
	request must be in to match the URL acceleration rule.	
allow-unencrypted {enable disable}	When enabled, unencrypted URL requests will be allowed. Unencrypted URL requests are the valid requests from the client that FortiWeb failed to decrypt. When disabled, if the URL can match the rule, and FortiWeb detects unencrypted URLs, the action will be triggered.	enable
action {alert deny_no_log alert_deny block-period}	Select which action the FortiWeb appliance will take when it detects a violation. alert—Accept the connection and generate an alert email and/or log message. alert_deny—Block the request (or reset the connection) and generate an alert and/or log message. deny_no_log—Block the request (or reset the connection). block-period—Blocks the request for a certain period of time.	Alert
block-period <block-period_int>	Enter the number of seconds that you want to block the requests. The valid range is 1–3,600 seconds. This option only takes effect when you choose Period Block in <code>action {alert deny_no_log alert_deny block-period}</code>.	60
severity {High Medium Low Info}	When FortiWeb records rule violations in the attack log, each log message contains a Severity Level field. Select the severity level that FortiWeb will record when the rule is violated: • Low • Medium • High • Informative The default value is High.	High
trigger <trigger_str>	Select the trigger, if any, that FortiWeb carries out when it logs and/or sends an alert email about a rule violation. For details, see "Viewing log messages" on page 1.	No default.
"<url-list_id>"	Enter the ID for the URL request.	No default.
url-type {plain regular}	Select whether the URL Pattern field will contain a literal URL (plain), or a regular expression designed to match multiple URLs (regular).	plain
url-pattern <url-pattern_str>	Depending on the <code>url-type</code>, enter either: • plain—The literal URL, such as <code>/index.php</code>, that	No default.

Variable	Description	Default
	the HTTP request must contain in order to match the rule. The URL must begin with a slash (/). regular—A regular expression, such as <code>^/*\.php</code>, matching the URLs to which the rule should apply. The pattern does not require a slash (/), but it must match URLs that begin with a slash, such as <code>/index.cfm</code>.	
"<exceptions-item_id>"	Enter the exception URL ID.	No default.
url-type {plain regular}	Select whether the URL Pattern field will contain a literal URL (plain), or a regular expression designed to match multiple URLs (regular).	plain
url-pattern <url-pattern_str>	Depending on the <code>url-type</code>, enter either: plain—The literal URL, such as <code>/index.php</code>, that the HTTP request must contain in order to match the rule. The URL must begin with a slash (/). regular—A regular expression, such as <code>^/*\.php</code>, matching the URLs to which the rule should apply. The pattern does not require a slash (/), but it must match URLs that begin with a slash, such as <code>/index.cfm</code>.	No default.
"<url-encryption-policy_name>"	Enter an encryption policy name.	No default.
full-mode {enable disable}	When enabled, Script Events, Embedded non-HTML content - scripts, js files, and Embedded non-HTML content - stylesheets that match the rule will be encrypted.	enable
"<rule-list_id>"	Enter the URL encryption rule ID.	No default.
rule <rule_str>	Select the URL encryption rule name.	No default.

Related topics

- [waf web-protection-profile inline-protection on page 696](#)

waf url-access-parameter

Use this command to add URL access parameter rules. It should be referred in an URL 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 details, see [Permissions on page 46](#).

Syntax

```
config waf url-access-parameter
  edit waf url-access-parameter
    config waf url-access-parameter-list
      edit <index>
        set argument-name <string>
        set data-type
      next
    end
  next
end
```

Variable	Description	Default
"<url-access-parameter-rule_name>"	Enter the name of a new or existing rule. The maximum length is 63 characters. To display the list of existing rules, enter: edit ?	No default.
argument-name <string>	Depending on your selection in Type , enter either: - The literal name that the HTTP request must contain in order to match the rule. - A regular expression. To create and test a regular expression, click the >> (test) icon. This opens the Regular Expression Validator window where you can fine-tune the expression. For details, see "Regular expression syntax" on page 1.	No default.
data-type	Specify the data type of the parameter value.	No default.

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, [waf url-access url-access-policy on page 664](#).

You can use SNMP traps to notify you when a URL access rule is enforced. For details, see [system snmp community on page 375](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```

config waf url-access url-access-rule
edit "<url-access-rule_name>"
    set action {alert_deny | continue | pass | deny_no_log}
    set host "<protected-hosts_name>"
    set host-status {enable | disable}
    set severity {Informative | Low | Medium | High | Info}
    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 reverse-dns-timeout <int>
            set type {regex-expression | simple-string}
            set reg-exp "<object_pattern>"
            set url-access-parameter
            set only-method {get | post | head | options | trace | connect | delete | put
                | patch | webdav | rpc | others}
            set only-protocol {http | https | ws | wss}
            set reverse-match {yes | no}
        next
    end
next
end

```

Variable	Description	Default
"<url-access-rule_name>"	Enter the name of a new or existing rule. The maximum length is 63 characters. To display the list of existing rules, enter: edit ?	No default.
action {alert_deny continue pass deny_no_log}	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. For details, see "system_replacemsg" on page 1. • continue—Generate an alert and/or log message, then continue by evaluating any subsequent rules defined in the web protection profile. If no other rules are violated, allow the request. If multiple rules are violated, a single request will generate multiple attack log messages. For details, see debug flow trace on	pass

Variable	Description	Default
	page 759. • <code>pass</code>—Allow the request. Do not generate an alert and/or log message. • <code>deny_no_log</code>—Deny a request. Do not generate a log message. Caution: This setting will be ignored if monitor-mode {enable disable} on page 163 is enabled. Note: Logging and/or alert email will occur only if enabled and configured. For details, see log disk on page 66 and log alertMail on page 60. Note: If an auto-learning profile will be selected in the policy with Offline Protection profiles that use this rule, you should select <code>pass</code>. If the action is <code>alert_deny</code>, the FortiWeb appliance will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For details about auto-learning requirements, see "waf web-protection-profile autolearning-profile" on page 1.	
<code>host "<protected-hosts_name>"</code>	Enter the name of a protected host that the <code>Host :</code> 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 {enable disable} on page 671 is <code>enable</code>.	No default.
<code>host-status {enable disable}</code>	Enable to require that the <code>Host :</code> field of the HTTP request match a protected hosts entry in order to match the rule. Also configure host "<protected-hosts_name>" on page 671.	<code>disable</code>
<code>severity {Informative Low Medium High Info}</code>	When rule violations are recorded in the attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level the FortiWeb appliance will use when a blocklisted IP address attempts to connect to your web servers: • Informative • Low • Medium • High • Info	Low
<code>trigger "<trigger-policy_name>"</code>	Select which trigger, if any, that the FortiWeb appliance will use when it logs and/or sends an alert email about a blocklisted IP address's attempt to connect to your web servers. The maximum length is 63 characters. For details, see log trigger-policy on page 96. To display the list of existing trigger policies, enter:	No default.

Variable	Description	Default
	set trigger ?	
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999,999.	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} on page 672 and the specific settings for each source address type.	disable
sip-address-type {sip sdomain source-domain}	- sip—Configure sip-address-value "<client_ip>" on page 672. - sdomain—Configure sdomain-type {"<ipv4>" "<ipv6>"} on page 672 and sip-address-domain "<fqdn_str>" on page 672. - source-domain—Configure source-domain-type {simple-string regex-expression} on page 672 and source-domain "<source-domain_str>" on page 672.	sip
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 (e.g. 1.2.3.4,2001::1,1.2.3.4-1.2.3.40,2001::1-2001::100). Available only if sip-address-type {sip sdomain source-domain} on page 672 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>" on page 672. Available only if sip-address-type {sip sdomain source-domain} on page 672 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} on page 672 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} on page 672 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.	No default.

Variable	Description	Default
	Available only if <code>sip-address-type {sip sdomain source-domain}</code> on page 672 is <code>sdomain</code> .	
<code>reverse-dns-timeout <int></code>	To avoid the process hanging for a long time, you can set this option to limit the time (in millisecond) when FortiWeb performs the reverse DNS lookup for an IP address. The unit is 0.01 second. For example, if you set the value to 10, it means 0.1 second. The valid value range is 0-600. 0 means the process will not be blocked by reverse dns lookup. This option is available only when sip-address-check is enabled and the sip-address-type is source-domain.	10
<code>type {regex-expression simple-string}</code>	Select how to use the text in <code>reg-exp "<object_pattern>"</code> on page 673 to determine whether or not a request URL meets the conditions for this rule. <code>simple-string</code>—The text is a string that request URLs must match exactly. <code>regular-expression</code>—The text is a regular expression that defines a set of matching URLs.	No default.
<code>reg-exp "<object_pattern>"</code>	Depending on your selection in <code>type {regex-expression simple-string}</code> on page 673 and <code>reverse-match {yes no}</code> on page 673, type a regular expression that defines either all matching or all non-matching URLs. Then, also configure <code>reverse-match {yes no}</code> on page 673. For example, for the URL access rule to match all URLs that begin with <code>/wordpress</code>, you could enter <code>^/wordpress</code>, then, for <code>reverse-match</code>, enter <code>no</code>. 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 <code>reverse-match {yes no}</code>.	No default.
<code>url-access-parameter</code>	Enter the URL Access Parameter rule you have created by <code>config waf url-access-parameter</code> .	No default.
<code>only-method {get post head options trace connect delete put patch webdav rpc others}</code>	Select the HTTP methods. Only the requests with the specified HTTP methods will match.	No default.
<code>only-protocol {http https ws wss}</code>	Select the HTTP protocols. Only the requests with the specified HTTP protocols will match.	No default.
<code>reverse-match {yes no}</code>	Indicate how to use <code>reg-exp "<object_pattern>"</code> on page 673 when determining whether or not this rule's condition has been met.	no

Variable	Description	Default
	<code>no</code>—If the simple string or regular expression does match the request URL, the condition is met. <code>yes</code>—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 (<code>!</code>).	

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

- [waf web-protection-profile inline-protection on page 696](#)
- [waf web-protection-profile offline-protection on page 706](#)
- [waf url-access url-access-policy on page 664](#)

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 [waf url-rewrite url-rewrite-rule on page 676](#).

To apply a URL rewriting group, select it in an inline protection profile. For details, see [waf web-protection-profile inline-protection on page 696](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

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>"	Enter the name of the URL rewriting rule group. The maximum length is 63 characters. To display the list of existing group, enter: <code>edit ?</code>	No default.
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999.	No default.
url-rewrite-rule-name "<url-rewrite-rule_name>"	Enter the name of an existing URL rewriting rule that you want to include in the group. The maximum length is 63 characters.	No default.
continue-execution {enable disable}	Enable to run this rule together with the next rule, for instance, inserting a custom header together with rewriting a header. If disabled, only the first matched rule in the table will be executed.	disable

Related topics

- [waf url-rewrite url-rewrite-rule on page 676](#)
- [waf web-protection-profile inline-protection on page 696](#)

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 website 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 website
- 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. For details, see the *FortiWeb Administration Guide*:

<https://docs.fortinet.com/document/fortiweb>

To use a URL rewriting rule, add it to a policy. For details, see [waf url-rewrite url-rewrite-policy](#) on page 675.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf url-rewrite url-rewrite-rule
  edit "<url-rewrite-rule_name>"
    set action {403-forbidden | redirect | redirect-301 | HTTP-request-body-
      rewrite | HTTP-response-body-rewrite | HTTP-header-rewrite | HTTP-
      response-header-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 referer-status {enable | disable}
    set referer "<referrer-url_str>"
    set referer-use-pserver {enable | disable}
    set http-method-status {enable | disable}
    set http-method <string>
    set status-code-status {enable | disable}
    set status-code <int>
    set request-replace-existing-headers {enable | disable}
    set response-replace-existing-headers {enable | disable}
    set request-remove-duplicate-headers {enable | disable}
    set response-remove-duplicate-headers {enable | disable}
  config header-insert
    edit <entry_index>
      set header-name "<header-name_str>"
      set header-value "<header-value_str>"
    next
  end
  set http-request-body-rewrite <string>
  set waf url-rewrite url-rewrite-rule
  set location "<location_str>"
  set location-status {enable | disable}
  set location_replace "<location_str>"
  set header-response-status {enable | disable}
  config response-header-removal
    edit <entry_index>
      set response-removal-header-name <string>
    next
  end
  config response-header-insert
    edit <entry_index>
      set response-header-name <string>
      set response-header-value <string>
    next
  end
  config match-condition
    edit <entry_index>
      set object {HTTP-host | HTTP-reference | HTTP-url}
      set protocol-filter {enable | disable}
      set protocol {HTTP | HTTPS}
      set reg-exp "<object_pattern>"
      set reverse-match {yes | no}
```

```

        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 is-essential {yes | no}
    next
end
    next
end
next
end

```

Variable	Description	Default
"<url-rewrite-rule_name>"	Enter the name of a new or existing rule. The maximum length is 63 characters. To display the list of existing rules, enter: edit ?	No default.
action {403-forbidden redirect redirect-301 HTTP-request-body-rewrite HTTP-response-body-rewrite HTTP-header-rewrite HTTP-response-header-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-request-body-rewrite—Replace the specific HTTP content in the body of requests. - HTTP-response-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. - HTTP-response-header-rewrite—Rewrite the HTTP header or body in the response packet. The following rows list the configurations when different actions are selected.	HTTP-header-rewrite
HTTP-header-rewrite		
header-name "<header-name_str>"	Enter the name of the header field that you want to insert to a request, such as "Myheader." You can add up to 10 headers in the insertion list.	No default.
header-value "<header-value_str>"	Enter the value of the header field that you specified in header-name "<header-name_str>", such as "123." Then, the customized header Myheader: 123 will be inserted to the matched HTTP requests.	No default.

Variable	Description	Default
host {<server_fqdn> <server_ipv4> <host_pattern>}	Type the FQDN of the host, such as <code>store.example.com</code>, to which the request will be redirected. The maximum length is 255 characters. This option is available only when host-status {enable disable} on page 679 is enabled. This field supports back references such as <code>\$0</code> to the parts of the original request that matched any capture groups that you entered in reg-exp "<object_pattern>" on page 683 for each object in the condition table. (A capture group is a regular expression, or part of one, surrounded in parentheses.) Use <code>\$n</code> ($0 \leq n \leq 9$) to invoke a substring, where <code>n</code> 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: <pre>(a) (b) (c (d)) (e) (f)</pre> would result in invokable variables with the following values: • <code>\$0</code>—a • <code>\$1</code>—b • <code>\$2</code>—cd • <code>\$3</code>—d • <code>\$4</code>—e • <code>\$5</code>—f	No default.
host-status {enable disable}	Enable to rewrite the <code>Host:</code> field or host name part of the <code>Referer:</code> field. When disabled, the FortiWeb appliance preserves the value from the client's request when rewriting it.	disable
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 {enable disable} on page 679 is enabled. Any setting you make for <code>host</code> is ignored.	disable
url "<replacement-url_str>"	Enter the string, such as <code>/catalog/item1</code>, that will replace the request URL. The maximum length is 255 characters. This option is available only when url-status {enable disable} on page 680 is enabled.	No default.

Variable	Description	Default
	Do not include the name of the web host, such as <code>www.example.com</code>, nor the protocol, which are configured separately in <code>host {<server_fqdn> <server_ipv4> <host_pattern>}</code> on page 679. Like <code>host</code>, this field supports back references such as <code>\$0</code> to the parts <code>reg-exp "<object_pattern>"</code> on page 683 for each object in the condition table. For an example, see the <i>FortiWeb Administration Guide</i>: https://docs.fortinet.com/document/fortiweb	
<code>url-status {enable disable}</code>	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.	disable
<code>referer-status {enable disable}</code>	Enable to rewrite the <code>Referer :</code> field in the HTML header. Also configure <code>referer "<referer-url_str>"</code> on page 680 and <code>referer-use-pserver {enable disable}</code> on page 680.	disable
<code>referer-use-pserver {enable disable}</code>	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 <code>referer-status {enable disable}</code> on page 680 is enabled. Any setting you make for <code>referer "<referer-url_str>"</code> on page 680 is ignored.	disable
<code>referer "<referer-url_str>"</code>	Enter the replacement value for the <code>Referer :</code> field in the HTML header. The maximum length is 255 characters. This option is available only when <code>referer-status {enable disable}</code> on page 680 is enabled.	No default.
<code>http-method-status {enable disable}</code>	Enable to replace the original HTTP methods in a request with the specified method.	disable
<code>http-method <string></code>	Specify the HTTP method to replace the original one. Please avoid changing the method on the fly unless absolutely necessary. It is important to consider the potential implications and ensure that the server can handle the new method correctly.	get
<code>status-code-status {enable disable}</code>	Enable to replace the original status code in a response with the specified code.	disable
<code>status-code <int></code>	Enter a status code to replace the original one in HTTP response.	404

Variable	Description	Default
request-replace-existing-headers {enable disable}	If there is already a header with the same name existing in the request, enabling this option will overwrite the value of the existing header with your specified header value. On the other hand, if this option is disabled, the system will insert the header directly without checking if there is an existing header with the same header name.	enable
response-replace-existing-headers {enable disable}	If there is already a header with the same name existing in the response, enabling this option will overwrite the value of the existing header with your specified header value. On the other hand, if this option is disabled, the system will insert the header directly without checking if there is an existing header with the same header name.	enable
request-remove-duplicate-headers {enable disable}	If the system finds multiple items in the HTTP request that match your specified header name, enabling this option will remove all of them. However, if this option is disabled, only the first matching item will be removed.	enable
response-remove-duplicate-headers {enable disable}	If the system finds multiple items in the HTTP response that match your specified header name, enabling this option will remove all of them. However, if this option is disabled, only the first matching item will be removed.	enable
redirect redirect-301		
location "<location_str>"	Enter the URL string that provides a location for use in a 301 or 302 HTTP redirection when the HTTP request matches. The maximum length is 255 characters.	No default.
HTTP-response-header-rewrite		
location-status {enable disable}	Enable to configure the <code>location_replace</code> .	disable
location_replace "<location_str>"	Enter the replacement value for the <code>Location:</code> field in the HTTP header for the response. The maximum length is 255 characters.	No default.
header-response-status {enable disable}	Enable to configure HTTP header insertion when the HTTP response matches.	disable
response-header-name <string>	Type the Header name that you want to insert into the HTTP response. You can add up to 10 headers in the insertion list.	No default.
response-header-value <string>	Type the value of the Header field.	No default.

Variable	Description	Default
<entry_index>	The index number of the header removal item.	No default.
response-removel-header-name <string>	The name of the header that you want to remove. Up to 10 header names can be added in the removal list.	No default.
HTTP-request-body-rewrite		
http-request-body-rewrite <string>	Enter the value that will replace matching HTTP content in the body of requests. The maximum is 255 characters.	No default.
HTTP-request-body-rewrite		
http-response-body-rewrite <string>	Enter the value that will replace matching HTTP content in the body of responses. The maximum is 255 characters.	No default.
Match Conditions		
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999.	No default.
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 <code>Referer:</code> field) If the request must match multiple conditions (for example, it must contain both a matching <code>Host:</code> 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 waf url-rewrite url-rewrite-rule on page 676. 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
protocol {HTTP HTTPS}	Select the protocol to use.	HTTP

Variable	Description	Default
reg-exp "<object_pattern>"	Depending on your selection in object {HTTP-host HTTP-reference HTTP-url} on page 682 and reverse-match {yes no} on page 683, type a regular expression that defines either all matching or all non-matching <code>Host :</code> fields, URLs, or <code>Referer :</code> fields. Then, also configure <code>reverse-match {yes no}</code>. For example, for the URL rewriting rule to match all URLs that begin with <code>/wordpress</code>, you could enter <code>^/wordpress</code>, then, in <code>reverse-match {yes no}</code>, select <code>no</code>. The pattern is not required to begin with a slash (<code>/</code>). The maximum length is 255 characters. Note: Regular expressions beginning with an exclamation point (<code>!</code>) are not supported. Instead, use <code>reverse-match {yes no}</code>.	No default.
reverse-match {yes no}	Indicate how to use reg-exp "<object_pattern>" on page 683 when determining whether or not this URL rewriting condition has been met. <code>no</code>—If the regular expression does match the request object, the condition is met. <code>yes</code>—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 (<code>!</code>). If all conditions are met, the FortiWeb appliance will do your selected action {403-forbidden redirect redirect-301 HTTP-request-body-rewrite HTTP-response-body-rewrite HTTP-header-rewrite HTTP-response-header-rewrite}.	no
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 <code>text/html</code>, as indicated in the <code>Content-Type :</code> 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 application/json application/rss+xml multipart/form-data application/x-www-form-urlencoded} on page 684.	disable

Variable	Description	Default
content-type-set {text/html text/plain text/javascript application/xml(or)text/xml application/javascript application/soap+xml application/x-javascript application/json application/rss+xml multipart/form-data application/x-www-form-urlencoded}	Enter 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.
is-essential {yes no}	Select what to do if there is no <code>Referer</code> field, either: - no—Meet this condition. - yes—Do not meet this condition. Requests can lack a <code>Referer</code> field for several reasons, such as if the user manually types the URL, and the request does not result from a hyperlink from another website, or if the URL resulted from an HTTPS connection. In those cases, the field cannot be tested for a matching value. For details, see the RFC 2616 section on the <code>Referer</code> field (http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html). This option appears only if <code>object {HTTP-host HTTP-reference HTTP-url}</code> on page 682 is <code>HTTP-reference</code>.	yes

Related topics

- [waf url-rewrite url-rewrite-policy on page 675](#)

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. For details, see [waf user-tracking rule on page 685](#).

To apply a user tracking policy, you select it in an inline or Offline Protection profile. For details, see [waf web-protection-profile inline-protection on page 696](#) and [waf web-protection-profile offline-protection on page 706](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

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>"	Enter the name of a new or existing policy. The maximum length is 63 characters. To display the list of existing policies, enter: edit ?	No default.
<entry_index>	Enter the index number of the individual entry in the table. The valid range is 1–9,999,999,999,999,999.	No default.
input-rule "<input-rule_name>"	Enter 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. For details, see [waf user-tracking policy on page 684](#).

You can apply a user tracking policy using either an inline or Offline Protection profile. However, Session Fixation Protection, Session Timeout, Limit Concurrent Users per Account, and Credential Stuffing Defense are not supported in Offline Protection mode.

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. For details, see [waf custom-access rule on page 469](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

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>"
  end
end

```

```

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 limit-users {enable | disable}
set maximum-users <maximum-users_int>
set session-idle-timeout <session-idle-timeout_int>
set session-timeout-enable {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 | deny_no_log}
set session-frozen-block-period <block-period_int>
set session-frozen-severity {High | Medium | Low | Info}
set session-frozen-trigger "<trigger-policy_name>"
set default-action {failed | success}
set credential-stuffing-protection {enable | disable}
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. You will use this name to reference the rule in other parts of the configuration. The maximum length is 63 characters.	No default.
hostname-ip "<hostname-ip_str>"	Select which protected host names entry (either a web host name or IP address) that the <code>Host: field</code> of the HTTP request must be in to match the rule. Available only when <code>host-status { enable disable }</code> is enable.	No default.
host-status { enable disable }	Enable to require that the <code>Host: field</code> of the HTTP request match a protected host names entry in order to match the URL access rule. Also configure <code>hostname-ip "<hostname-ip_str>"</code> .	disable
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.

Variable	Description	Default
password-parameter "<password_str>"	Enter the password field value to match in authorization requests.	No default.
session-id-name "<session-id_str>"	Enter the name of the session ID that is used to identify each session. Examples of session ID names are <code>sid</code>, <code>PHPSESSID</code>, and <code>JSESSIONID</code>. To track users with JSON format login credentials, here you need to type the API token in response data that users will use to access server resource in API queries.	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 <code>enable</code> 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
limit-users {enable disable}	Enable to limit the number of concurrent logins per account.	disable
maximum-users <maximum-users_int>	Specify the maximum number of concurrent logins using the same account.	1
session-idle-timeout <session-idle-timeout_int>	When a session is idled for the specified period of time, the Concurrent Users count will be renewed. The user who is timed-out needs to re-log in. The valid range is 1-1440.	30
session-timeout-enable {enable disable}	Enable to set the time in minutes that FortiWeb waits before it stops tracking an inactive user session.	disable

Variable	Description	Default
session-timeout-enforcement {enable disable}	Enter <code>enable</code> to configure FortiWeb to remove the session ID for user sessions that are idle for longer than the length of time specified by <code>session-timeout</code>. 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 <code>session-frozen-time</code>.	disable
session-timeout <timeout_int>	Enter the length of time in minutes that FortiWeb waits before it stops tracking an inactive user session. The valid range is 1–60.	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 <code>session-timeout-enforcement {enable disable}</code> on page 688 is <code>enable</code>.	30
session-frozen-action {alert alert_deny redirect block-period deny_no_log}	When <code>session-timeout-enforcement {enable disable}</code> on page 688 is <code>enable</code>, enter the action that FortiWeb takes against requests with the ID of a timed-out session during the specified time period, or when <code>credential-stuffing-protection {enable disable}</code> on page 690 is enabled enter the action that FortiWeb takes against spilled username/password pairs: <code>alert</code>—Accept the request and generate an alert email and/or log message. <code>alert_deny</code>—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. For details, see "<code>system replacemsg</code>" on page 1. Note: In Offline Protection mode, because the deny action is not supported, this option has the same effect as <code>alert</code>. <code>redirect</code> — Redirect the request to the URL that you specify in the protection profile and generate an alert and/or log message. Also configure <code>redirect-url <redirect_fqdn></code> and <code>rdt-reason {enable disable}</code>. Caution: This option is not supported in Offline Protection mode	alert

Variable	Description	Default
	<code>block-period</code>—Block subsequent requests from the client for a specified number of seconds. <code>deny_no_log</code>—Deny a request. Do not generate a log message. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see "system replacemsg" on page 1. Caution: This option is not supported in Offline Protection mode When the action generates a log message, the message field value is <code>Session Timeout Enforcement: triggered by user <username></code>. Available only when session-timeout-enforcement {enable disable} on page 688 or credential-stuffing-protection {enable disable} on page 690 is set to <code>enable</code>.	
<code>session-frozen-block-period</code> <code><block-period_int></code>	Enter the number of seconds to block requests with the ID of a timed-out session or when credential-stuffing-protection {enable disable} on page 690 is enabled and detects spilled username/password pairs. This setting is available only if session-frozen-action {alert alert_deny redirect block-period deny_no_log} on page 688 is <code>block-period</code>. The valid range is 1–3,600 seconds.	600
<code>session-frozen-severity</code> {High Medium Low Info}	When the session timeout settings generate an attack log, each log message contains a Severity Level (<code>severity_level</code>) field. Select which severity level FortiWeb uses when it takes the specified action: - Low - Medium - High Available only when session-timeout-enforcement {enable disable} on page 688 or credential-stuffing-protection {enable disable} on page 690 is set to <code>enable</code>.	Low
<code>session-frozen-trigger</code> <code>"<trigger-policy_name>"</code>	Enter the name of the trigger, if any, to apply when FortiWeb detects requests with the ID of a timed-out session or when credential-stuffing-protection is enabled and FortiWeb detects spilled username/password pairs. The maximum length is 63 characters. For details, see log trigger-policy on page 96. To display the list of existing triggers, enter: <pre>set trigger ?</pre>	No default.

Variable	Description	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
credential-stuffing-protection {enable disable}	Enable to use FortiGuard's Credential Stuffing Defense database to prevent against Credential Stuffing attacks. For details, see the <i>FortiWeb Administration Guide</i> : https://docs.fortinet.com/document/fortiweb	disable
<entry_index>	Enter 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 {failed success} on page 690.	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

- [server-policy allow-hosts on page 106](#)
- [waf web-protection-profile inline-protection on page 696](#)
- [waf web-protection-profile offline-protection on page 706](#)

waf waiting-room policy

You can use Waiting Room to manage visitor traffic and avoid server overload delays, you can enable a virtual holding space and queuing system, allowing new users to enter a Waiting Room where they can view estimated wait times before accessing your application.

This feature may be configured for your entire website, or specific URL paths.

Use this command to create waiting room policies.

Syntax

```
config waf waiting-room-policy
  edit <waiting-room-policy_name>
    set path-type {plain | regular}
    set path <string>
    set total-active-users <integer>
    set new-users-per-min <integer>
    set session-duration <integer>
    set description <string>
  config bypass-rules
    edit <bypass-rules_id>
      set type source-ip
```

```

        set value <string>
    next
end
next
end

```

Variable	Description	Default
<waiting-room-policy-name>	Enter a 40-character string for the name, for example e1947036-alfa-489e-8434-c8a401a75f78.	No default
path-type {plain regular}	Select whether to use a Simple String or a Regular Expression to specify the URLs for the Waiting Room. When users access the URL, FortiWeb will queue their requests according to the Waiting Room policy.	plain
path <string>	The waiting room will only be enabled for the configured URL. Use /. * to match all. - If Path Type is Simple String, enter the literal URL. - If Path Type is Regular Expression, enter a regular expression to match the URLs. This value cannot be empty.	No default
total-active-users <integer>	Control the size of traffic accessing your application. If the number of active users reaches the configured value, additional users will enter the Waiting Room.	0
new-users-per-min <integer>	Prevent your application from being flooded by new users in a short time span. If the number of new users per minute reaches the configured value, additional users will enter the Waiting Room. At least specify one of <code>total-active-users</code> and <code>new-users-per-min</code> . If you choose to configure both, make sure that <code>total-active-users</code> is set to a value greater than or equal to <code>new-users-per-min</code> .	0
session-duration <integer>	Users who have remained idle for the configured time will be considered as a new user. Users who have ended and restarted the session will also be considered as a new user. This value cannot be empty.	5
description <string>	Enter a brief description for the Waiting Room Policy.	No default
<bypass-rules_id>	Add bypass rules to allow users with certain IP addresses to access your application directly, even if they trigger the above limiting conditions.	No default
value <string>	Enter an IP address or range in the Value field to configure a new Bypass rule.	No default

Related topics

- [server-policy policy on page 150](#)

waf web-cache-rule/policy

To improve performance of your back-end network and servers by reducing their traffic and processing load, you can configure FortiWeb to cache responses from your servers.



To configure the web caching, you must enable it in [system feature-visibility](#).

Syntax

```
config waf web-cache-policy
  edit "<server_policy_id>"
  next
end
```

Variable	Description	Default
<web-cache-policy_name>	Enter the ID of the server policy that has enabled this web cache.	No default.

```
config waf web-cache-rule
  edit "<rule-name_entry>"
    set host-status {enable | disable}
    set host <host_str>
    set path <path_str>
    set HTTP-method {get-head | get-head-options | all-methods}
    set request-file-type {text | picture | media | binary | other}
    set allow-return-code {allow-200 | allow-200-206 | allow-200-206-301-302}
    set cache-inactive-time <cache-inactive-time_int>
    set inactive-time-type {minutes | hours}
    set client-cache-expire <client-cache-expire_int>
    set client-cache-expire-type {minutes | hours}
    set key-factor {method | protocol | host | url | arguments | cookies}
    set enable-client-expire {enable | disable}
    set policy-id <entry_index>
    config cookie-name-list
      edit <cookie-name-list_id>
        set cookie-name "<cookie-name_str>"
      end
    config bypass-sub-url
      edit "<bypass-sub-url_id>"
        set HTTP-method {get | post | head | options | trace | connect | delete | put | patch | any}
        set type {plain | regular}
      end
    end
  end
```

```

        set url-expression <url-expression_str>
        set enable-bypass-args {enable | disable}
        set bypass-args <bypass-args_str>
        set enable-bypass-cookies {enable | disable}
        set bypass-cookies <bypass-cookies_str>
        set block-return-code {block-none|block-200|block-206|block-301|block-302}
    next
end
next
end

```

Variable	Description	Default
"<rule-name_entry>"	Enter a 40-character string for the name, for example e1947036-a1fa-489e-8434-c8a401a75f78.	No default.
host-status {enable disable}	Enable to require that the <code>Host: field</code> of the HTTP request match a protected host names entry in order to match the web cache rule. Also configure <code>host <host_str></code> .	No default.
host <host_str>	Select which protected host names entry (either a web host name or IP address) that the <code>Host: field</code> of the HTTP request must be in to match the web cache rule.	No default.
path <path_str>	Enter a path for your web pages, for example <code>/test</code> , a prefix of a set of URLs.	No default.
HTTP-method {get-head get-head-options all-methods}	Select whether to cache the response contents according to the HTTP method you use.	get-head
request-file-type {text picture media binary other}	Select whether to cache the response contents according to the content type.	All values
allow-return-code {allow-200 allow-200-206 allow-200-206-301-302}	Select whether to cache the response contents according to the response code.	200
cache-inactive-time <cache-inactive-time_int>	Specify a timeout threshold that the cache becomes invalid and needs to be refreshed. After the timeout, the cached web contents will be removed automatically.	60 minutes
inactive-time-type {minutes hours}	Select the time unit for the cache inactive time.	minutes
client-cache-expire <client-cache-expire_int>	Enter a period specified by max-age so that if the client requests the same contents again in the period, the client can obtain the web content from local cache directly.	10 minutes
client-cache-expire-type {minutes hours}	Select the time unit for the cache expiration time.	minutes
key-factor {method protocol host url arguments cookies}	Select the protocol variable that you want to use to generate the cache key.	All values except cookies.

Variable	Description	Default
enable-client-expire {enable disable}	Enable to clear the cache based on the specified period.	disable
policy-id <server-policy_name>	Enter the ID of the server policy that has enabled this web cache.	No default.
"<cookie-name-list_id>"	Enter the cookie name ID if you specify cookie in key-factor {method protocol host url arguments cookies}	No default.
cookie-name "<cookie-name_str>"	Enter a cookie name related to the ID.	No default.
"<bypass-sub-url_id>"	Enter the bypass sub URL list ID.	No default.
HTTP-method {get post head options trace connect delete put patch any}	Select the HTTP method in which the request sub URL is included.	any
type {plain regular}	Select whether the url-expression <url-expression_str> field must contain either: - plain—The field is a string that the request sub URL must match exactly. - regular—The field is a regular expression that defines a set of matching sub URLs.	plain
url-expression <url-expression_str>	Depending on your selection in type {plain regular} , enter either: - The literal URL, such as <code>/index.php</code>, that the HTTP request must contain in order to match the web cache rule. The URL must begin with a slash (/). - A regular expression, such as <code>^/* .php</code>, matching all and only the URLs to which the web cache 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 <code>/index.cfm</code>. Note: Regular expressions beginning with an exclamation point (!) are not supported. For information on language and regular expression matching, see the <i>FortiWeb Administration Guide</i>: https://docs.fortinet.com/document/fortiweb	No default.
enable-bypass-args {enable disable}	Enable this option so that the request matches the bypass URL only when the request brings the specific arguments.	disable
bypass-args <bypass-args_str>	Enter the bypass arguments.	No default.
enable-bypass-cookies {enable disable}	Enable this option so that the request matches the bypass URL only when the request brings the specific cookies.	disable

Variable	Description	Default
bypass-cookies <bypass-cookies_str>	Enter the bypass arguments.	No default.
block-return-code {block-none block-200 block-206 block-301 block-302}	Select the HTTP return code so that the request matches the bypass URL only when the request triggers one of the selected return codes.	block-none

Related topics

- [server-policy policy on page 150](#)

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 [server-policy policy on page 150](#).

Before configuring an inline protection profile, first configure any of the following that you want to include in the profile:

- Parameter validation rule (see [waf parameter-validation-rule on page 610](#))
- URL access policy (see [waf url-access url-access-policy on page 664](#))
- Hidden field rule group (see [waf hidden-fields-protection on page 522](#))
- Parameter restriction constraint (see [waf HTTP-protocol-parameter-restriction on page 543](#))
- Authentication policy and/or site publisher (see [waf HTTP-authen HTTP-authen-policy on page 527](#) and [waf site-publish-helper policy on page 624](#))
- Allowed method exception (see [waf allow-method-exceptions on page 423](#))
- List of manually trusted and block-listed IPs, FortiGuard IP reputation category-based blocklisted IPs, and/or a geographically-based IP blocklist (see [waf ip-intelligence-ignore-x-forwarded-for on page 560](#), ["server-policy custom-application application-policy" on page 1](#), and [waf geo-block-list on page 511](#))
- Attack signatures (see [waf signature on page 612](#))
- File security policy (see ["server-policy custom-application application-policy" on page 1](#))
- Web Shell Detection (see [waf webshell-detection-policy on page 712](#))
- URL rewriting policy (see [waf url-rewrite url-rewrite-policy on page 675](#))
- XML protection policy ([waf xml-validation on page 727](#))
- DoS protection policy (see [waf application-layer-dos-prevention on page 440](#))
- Compression rules (see [waf file-compress-rule on page 495](#))
- Policy that protects vulnerable block cipher implementations for web applications that selectively encrypt inputs without using HTTPS ([waf padding-oracle on page 606](#))
- FortiGate that provides a list of quarantined source IPs ([system fortigate-integration on page 304](#))
- Cross-site request forgery (CSRF) protection rule (see [waf csrf-protection on page 464](#))
- Cookie security policy (see [waf cookie-security on page 460](#))
- User tracking policy (see [waf user-tracking policy on page 684](#))

- JSON protection policy (see [waf json-validation rule on page 566](#))
- OpenAPI Validation (see [waf openapi-validation-policy on page 605](#))
- Mobile API protection policy (see [waf mobile-api-protection on page 602](#))
- Bot mitigation policy (see [waf bot-detection-policy on page 446](#))
- API gateway policy (see [waf api-rules on page 432](#))
- Syntax-based attack detection policy (see [waf syntax-based-attack-detection on page 640](#))

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf web-protection-profile inline-protection
edit "<inline-protection-profile_name>"
    set client-management {enable | disable}
    set threat-score-profile <name>
    set http-session-cookie {enable | disable}
    set http-session-timeout <days_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 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 url-access-policy "<policy_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 url-rewrite-policy "<group_name>"
    set HTTP-authen-policy "<policy_name>"
    set HTTP-header-security "<policy_name>"
    set site-publisher-helper "<policy_name>"
    set file-compress-rule "<rule_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>"
    set profile-id "<profile-id_str>"
    set mitb-protection "<mitb-protection_name>"
    set openapi-validation-policy "<openapi-validation-policy_name>"
    set websocket-security-policy "<websocket-security-policy_name>"
    set json-validation-policy "<json-validation-policy_name>"
```

```

set cors-protection-policy "<cors-protection-policy>"
set mobile-app-identification {enable | disable}
set token-secret <token-secret_str>
set token-header <token-header_str>
set mobile-api-protection <mobile-api-protection_name>
set bot-mitigate-policy <bot-mitigate-policy_name>
set api-management-policy <api-management-policy_name>
set url-encryption-policy <url-encryption-policy_str>
set syntax-based-attack-detection <detection_name>
set advanced-bot-protection <policy_name>
set owasp_api_top10_log_field {enable/disable}
next
end

```

Variable	Description	Default
"<inline-protection-profile_name>"	Enter the name of the inline protection profile. The maximum length is 63 characters. To display the list of existing profiles, enter: <pre>edit ?</pre>	No default.
client-management {enable disable}	Enable to add an implementation of HTTP sessions, and track their states, using a cookie such as <code>cookiesession1</code>. Also configure http-session-timeout <days_int> on page 699. 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? 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: If you want to include this profile's traffic in the traffic log, in addition to enabling traffic logs in general. For details, see log attack-log on page 61.	enable

Variable	Description	Default
threat-score-profile <name>	Select the Threat Score Profile so that FortiWeb can take action on IPs or clients when their threat score accumulates to a certain value. The threat score profile is configured in <code>config server-policy pattern threat-score-profile</code>. If you have enabled client-management, but does not configure <code>threat-score-profile</code>, the system will by default applies the configurations in <code>config server-policy pattern threat-weight</code>. This option is available only when client-management is enabled.	
http-session-cookie {enable disable}	If enabled, <code>cookiesession1</code> will expire upon the termination of the user's session. If disabled, <code>cookiesession1</code> will not expire upon the termination of the session. In this case, you can specify its expiration time through <code>http-session-timeout <days_int></code>. The default expiration time is 365 days. Note: FortiWeb uses <code>cookiesession1</code> for user tracking, ensuring consistent user identification as long as the <code>cookiesession1</code> remains unexpired. For more information, see this FAQ in Troubleshooting part: Why is the cookiesession1 generated by Client Management persistent cookie?	disable
http-session-timeout <days_int>	Specify the expiration time for <code>cookiesession1</code>. The valid range is 1-365. This setting is available only if <code>http-session-management</code> is enabled and <code>http-session-cookie</code> is disabled.	365
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. The maximum length is 63 characters. For details, see waf x-forwarded-for on page 721. To display the list of existing rules, enter: <pre>set x-forwarded-for-rule ?</pre>	No default.
signature-rule {"High Level Security" "Medium Level Security" "Alert Only" <signature-set_name>}	Specify a signature policy to include in the profile. The maximum length is 63 characters. For details, see waf signature on page 612. To display the list of existing rules, enter: <pre>set server-protection-rule ?</pre> The type of attack that FortiWeb detects determines the attack log messages for this feature. For a list, see waf signature on page 612.	No default.

Variable	Description	Default
amf3-protocol-detection {enable disable}	Enable to scan requests that use action message format 3.0 (AMF3) for these attacks if you have enabled those in the signature set specified by signature-rule {"High Level Security" "Medium Level Security" "Alert Only" <signature-set_name>} on page 699: • Cross-site scripting (XSS) attacks • SQL injection attacks • Common exploits 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
json-validation-policy "<json-validation-policy_name>"	Enter the JSON protection policy name.	No default.
cors-protection-policy "<cors-protection-policy>"	Enter the CORS protection policy name.	No default.
mobile-app-identification {enable disable}	Enable to configure the JWT token secret and token header to verify a request from a mobile application. Refer to the Approov documentation for how to get the token.	disable
token-secret <token-secret_str>	Enter the token secret that you have got from Approov. Available only when mobile-app-identification {enable disable} is enable.	No default
token-header <token-header_str>	Specify the header where the token is carried. Available only when mobile-app-identification {enable disable} is enable.	No default
mobile-api-protection <mobile-api-protection_name>	Select the name of an existing API protection policy. For details, see waf mobile-api-protection .	No default
bot-mitigate-policy <bot-mitigate-policy_name>	Select the name of a bot mitigation policy. For details, see waf mobile-api-protection .	No default.
api-management-policy <api-management-policy_name>	Select the name of an API gateway policy. For details, see waf api-rules .	No default.
custom-access-policy "<combo-access_name>"	Select the name of a custom access policy. The maximum length is 63 characters. For details, see waf custom-access policy on page 468. To display the list of existing policies, enter: <pre>set custom-access-policy ?</pre>	No default.

Variable	Description	Default
padding-oracle "<rule_name>"	Select the name of a padding oracle protection rule. The maximum length is 63 characters. For details, see waf padding-oracle on page 606. To display the list of existing rules, enter: <pre>set padding-oracle ?</pre>	No default.
csrf-protection "<rule_name>"	Select the name of cross-site request forgery protection rule, if any, to apply to matching requests. For details, see waf csrf-protection on page 464. Available only when client-management {enable disable} on page 698 is enabled.	No default.
cookie-security-policy "<cookie-security_name>"	Select the name of a cookie security policy. For details, see waf cookie-security on page 460. To display the list of existing policies, enter: <pre>set cookie-security-policy ?</pre>	
parameter-validation-rule "<rule_name>"	Select the name of a parameter validation rule. The maximum length is 63 characters. For details, see waf parameter-validation-rule on page 610. To display the list of existing rules, enter: <pre>set parameter-validation-rule ?</pre>	No default.
hidden-fields-protection "<group_name>"	Select the name of a hidden field rule group that you want to apply, if any. The maximum length is 63 characters. For details, see waf hidden-fields-protection on page 522. To display the list of existing groups, enter: <pre>set hidden-fields-protection ?</pre>	No default.
file-upload-policy "<policy_name>"	Select the name of a file upload security policy to use, if any. The maximum length is 63 characters. For details, see "server-policy custom-application application-policy" on page 1. To display the list of existing policies, enter: <pre>set file-upload-policy ?</pre>	No default.
HTTP-protocol-parameter-restriction "<constraint_name>"	Select the name of an HTTP protocol constraint that you want to apply, if any. The maximum length is 63 characters. For details, see waf HTTP-protocol-parameter-restriction on page 543. To display the list of existing profiles, enter: <pre>set HTTP-protocol-parameter-restriction ?</pre>	No default.
url-access-policy "<policy_name>"	Select the name of a URL access policy. The maximum length is 63 characters. For details, see waf url-access url-access-policy on page 664. To display the list of existing policies, enter:	No default.

Variable	Description	Default
	<code>set url-access-policy ?</code>	
allow-method-policy " <code><policy_name></code> "	Select the name of an allowed method policy. The maximum length is 63 characters. For details, see "server-policy custom-application application-policy" on page 1. To display the list of existing policies, enter: <code>set allow-method-policy ?</code>	No default.
ip-list-policy " <code><policy_name></code> "	Select the name of a trusted IP or blocklisted IP policy. The maximum length is 63 characters. For details, see "server-policy custom-application application-policy" on page 1. To display the list of existing policies, enter: <code>set ip-list-policy ?</code>	No default.
geo-block-list-policy " <code><policy_name></code> "	Select the name of a geographically-based client IP block list that you want to apply, if any. The maximum length is 63 characters. For details, see waf geo-block-list on page 511 . To display the list of existing groups, enter: <code>set geo-block-list-policy ?</code>	No default.
application-layer-dos-prevention " <code><policy_name></code> "	Select the name of an existing DoS protection policy to use with this profile, if any. The maximum length is 63 characters. For details, see waf application-layer-dos-prevention on page 440 . To display the list of existing profiles, enter: <code>set application-layer-dos-prevention ?</code>	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 waf ip-intelligence-ignore-x-forwarded-for on page 560 .	disable
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 FortiOS and FortiWeb, see system fortigate-integration on page 304 .	disable
quarantined-ip-action {alert alert_deny}	Specify the action that FortiWeb takes if it detects a quarantined IP address: <code>alert</code>—Accept the request and generate an alert email, log message, or both. <code>alert_deny</code>—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

Variable	Description	Default
quarantined-ip-trigger "<trigger-policy_name>"	Select the name of the trigger to apply when FortiWeb detects a quarantined IP. For details, see log trigger-policy on page 96. To display the list of existing trigger policies, enter: <pre>set trigger ?</pre>	No default.
url-rewrite-policy "<group_name>"	Select the name of a URL rewriting rule set, if any, that will be applied to matching HTTP requests. The maximum length is 63 characters. To display the list of existing policies, enter: <pre>set url-rewrite-policy ?</pre> For details, see waf url-access url-access-policy on page 664.	No default.
HTTP-authen-policy "<policy_name>"	Select the name of an HTTP authentication policy, if any, that will be applied to matching HTTP requests. The maximum length is 63 characters. For details, see waf HTTP-authen HTTP-authen-policy on page 527. To display the list of existing profiles, enter: <pre>set HTTP-authen-policy ?</pre> If the HTTP client fails to authenticate, it will receive an HTTP 403 (Access Forbidden) error message.	No default.
HTTP-header-security "<policy_name>"	Select the name of an HTTP Header Security Policy, if any. For details, see waf HTTP-header-security on page 540. To display the list of existing policies, enter: <pre>set HTTP-header-security ?</pre>	No default.
site-publisher-helper "<policy_name>"	Select the name of a site publishing policy, if any, that will be applied to matching HTTP requests. The maximum length is 63 characters. For details, see waf site-publish-helper policy on page 624. To display the list of existing profiles, enter: <pre>set site-publisher-policy ?</pre> If the HTTP client fails to authenticate, it will receive an HTTP 403 (Access Forbidden) error message.	No default.
file-compress-rule "<rule_name>"	Select the name of an existing file compression rule to use with this profile, if any. The maximum length is 63 characters. For details, see waf file-compress-rule on page 495. To display the list of existing rules, enter: <pre>set file-compress-rule ?</pre>	No default.
user-tracking-policy "<user-tracking-policy_name>"	Select the name of a user tracking policy. The maximum length is 63 characters. For details, see waf user-tracking policy on page 684.	No default.

Variable	Description	Default
	To display the list of existing policies, enter: <code>set user-tracking-policy ?</code>	
<code>redirect-url "<redirect_ fqdn>"</code>	Enter 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 <code>www.example.com/products/</code> . 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.
<code>rdt-reason {enable disable}</code>	Enable to include the reason for URL redirection as a parameter in the URL, such as <code>reason=DETECT_PARAM_RULE_FAILED</code> , when traffic has been redirected using <code>redirect-url "<redirect_fqdn>"</code> on page 704. The FortiWeb appliance also adds <code>fortiwaf=1</code> 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.
<code>data-analysis {enable disable}</code>	Enable this to collect data for servers covered by this profile.	disable
<code>comment "<comment_str>"</code>	Enter 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.
<code>xml-validation-policy "<xml_ policy_name>"</code>	Select the name of an XML protection policy, if any. The maximum length is 63 characters. For details, see waf xml-validation on page 727 . To display the list of existing policies, enter: <code>set xml-validation-policy ?</code>	No default.
<code>profile-id "<profile-id_str>"</code>	Enter the inline profile ID.	No default.
<code>mitb-protection "<mitb- protection_name>"</code>	Select the MiTB protection policy name. For details, see waf mitb-policy on page 600 .	No default.
<code>openapi-validation-policy "<openapi-validation-policy_ name>"</code>	Select the openapi validation policy name. For details, see waf openapi-validation-policy on page 605 .	No default.

Variable	Description	Default
websocket-security-policy "<websocket-security-policy_name>"	Select the websocket security policy name. For details, see waf websocket-security policy on page 717 .	No default.
grpc-security-policy <grpc-security-policy_name>	Select the grpc security policy name. For details, see waf grpc-security policy .	No default.
url-encryption-policy <url-encryption-policy_str>	Select the URL encryption policy name. For details, see waf url-encryption on page 666 .	No default.
syntax-based-attack-detection <detection_name>	Select the name of an existing SQL/XSS syntax based detection policy. For details, see waf syntax-based-attack-detection .	No default.
advanced-bot-protection <policy_name>	Select the name of an existing Advanced Bot Protection policy. For details, see waf advanced-bot-protection on page 420 .	No default.
owasp_api_top10_log_field {enable/disable}	Enable to record the OWASP API Top10 attack categories in attack logs so that you can filter the attack logs by OWASP API Top10.	enable

Related topics

- [log trigger-policy on page 96](#)
- [server-policy pattern custom-global-white-list-group on page 126](#)
- [server-policy policy on page 150](#)
- [waf signature on page 612](#)
- [waf padding-oracle on page 606](#)
- [waf parameter-validation-rule on page 610](#)
- [waf HTTP-protocol-parameter-restriction on page 543](#)
- [waf url-access url-access-policy on page 664](#)
- [waf allow-method-exceptions on page 423](#)
- [waf application-layer-dos-prevention on page 440](#)
- [waf file-compress-rule on page 495](#)
- [waf geo-block-list on page 511](#)
- [waf hidden-fields-protection on page 522](#)
- [waf HTTP-authen HTTP-authen-policy on page 527](#)
- [waf HTTP-protocol-parameter-restriction on page 543](#)
- [waf ip-intelligence-ignore-x-forwarded-for on page 560](#)
- ["server-policy custom-application application-policy" on page 1](#)
- [waf syntax-based-attack-detection on page 640](#)

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, or cookie poisoning detection.

To apply detection profiles, select them within a server policy. For details, see [server-policy policy on page 150](#).

Before configuring an Offline Protection profile, first configure any of the following that you want to include in the profile:

- File security policy (see ["server-policy custom-application application-policy" on page 1](#))
- Web Shell Detection policy (see [waf webshell-detection-policy on page 712](#))
- Server protection rule (see [waf signature on page 612](#))
- List of manually trusted and block-listed IPs, FortiGuard IRIS category-based blocklisted IPs, and/or a geographically-based IP blocklist (see [waf ip-intelligence-ignore-x-forwarded-for on page 560](#), ["server-policy custom-application application-policy" on page 1](#) and [waf geo-block-list on page 511](#))
- Parameter validation rule (see [waf parameter-validation-rule on page 610](#))
- URL access policy (see [waf url-access url-access-policy on page 664](#))
- Allowed method exception (see [waf allow-method-exceptions on page 423](#))
- Hidden field rule group (see [waf hidden-fields-protection on page 522](#))
- Parameter restriction constraint (see [waf HTTP-protocol-parameter-restriction on page 543](#))
- Policy that protects vulnerable block cipher implementations for web applications that selectively encrypt inputs without using HTTPS ([waf padding-oracle on page 606](#))
- User tracking policy (see [waf user-tracking policy on page 684](#))
- XML protection policy (see [waf xml-validation on page 727](#))
- JSON protection policy (see [waf json-validation rule on page 566](#))
- OpenAPI Validation (see [waf openapi-validation-policy on page 605](#))
- Mobile API protection policy (see [waf mobile-api-protection on page 602](#))
- Syntax-based attack detection policy (see [waf syntax-based-attack-detection on page 640](#))

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf web-protection-profile offline-protection
edit "<offline-protection-profile_name>"
set client-management {enable | disable}
```

```

set threat-score-profile <name>
set waf web-protection-profile offline-protection
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 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 ip-list-policy "<policy_name>"
set geo-block-list-policy "<policy_name>"
set ip-intelligence {enable | disable}
set csrf-protection "<rule_name>"
set user-tracking-policy "<user-tracking-policy_name>"
set data-analysis {enable | disable}
set comment "<comment_str>"
set openapi-validation-policy "<openapi-validation-policy_name>"
set json-validation-policy "<json-validation-policy_name>"
set mobile-app-identification {enable | disable}
set token-secret <token-secret_str>
set token-header <token-header_str>
set mobile-api-protection <mobile-api-protection_name>
set syntax-based-attack-detection <detection_name>
set owasp_api_top10_log_field {enable/disable}
next
end

```

Variable	Description	Default
"<offline-protection-profile_name>"	Enter the name of the Offline Protection profile. The maximum length is 63 characters. To display the list of existing profiles, enter: edit ?	No default.
client-management {enable disable}	Enable to track the states of HTTP sessions. Also configure waf web-protection-profile offline-protection on page 706 . 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.	disable

Variable	Description	Default
	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 details, see log attack-log on page 61.	
threat-score-profile <name>	Select the Threat Score Profile so that FortiWeb can take action on IPs or clients when their threat score accumulates to a certain value. The threat score profile is configured in <code>config server-policy pattern threat-score-profile</code>. If you have enabled client-management, but does not configure <code>threat-score-profile</code>, the system will by default applies the configurations in <code>config server-policy pattern threat-weight</code>. This option is available only when client-management is enabled.	
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. For details, see waf x-forwarded-for on page 721. To display a list of existing rules, enter: <pre>set forwarded-for-rule ?</pre>	No default.
HTTP-session-keyword "<key_str>"	If you want to use an HTTP header other than <code>Session-Id</code>: to track separate HTTP sessions, enter the key portion of the HTTP header that you want to use, such as <code>Session-Num</code>. The maximum length is 63 characters.	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. The maximum length is 63 characters. For details, see waf signature on page 612. To display the list of existing rules, enter: <pre>set server-protection-rule ?</pre> The type of attack that FortiWeb detects determines the attack log messages for this feature. For a list, see waf signature on page 612.	No default.
amf3-protocol-detection {enable disable}	Enable to scan requests that use the action message format 3.0 (AMF3) for these attacks 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>"} on page 709: • Cross-site scripting (XSS) attacks • SQL injection attacks • Common exploits 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
custom-access-policy "<combo-access_name>"	Enter the name of a custom access policy. The maximum length is 63 characters. For details, see waf custom-access policy on page 468. To display the list of existing policies, enter: <pre>set custom-access-policy ?</pre>	No default.
padding-oracle "<rule_name>"	Enter the name of a padding oracle protection rule. The maximum length is 63 characters. For details, see waf padding-oracle on page 606. To display the list of existing rules, enter: <pre>set padding-oracle ?</pre>	No default.
parameter-validation-rule "<rule_name>"	Enter the name of a parameter validation rule. The maximum length is 63 characters. For details, see waf parameter-validation-rule on page 610. To display the list of existing rules, enter: <pre>set parameter-validation-rule ?</pre>	No default.
hidden-fields-protection "<group_name>"	Enter the name of a hidden field rule group that you want to apply, if any. The maximum length is 63 characters. For details, see waf hidden-fields-protection on page 522. To display the list of existing groups, enter: <pre>set hidden-fields-protection ?</pre>	No default.

Variable	Description	Default
file-upload-policy "<policy_name>"	Enter the name of a file security policy. The maximum length is 63 characters. For details, see "server-policy custom-application application-policy" on page 1. To display the list of existing policies, enter: <pre>set file-upload-policy ?</pre>	No default.
HTTP-protocol-parameter-restriction "<constraint_name>"	Enter the name of an HTTP protocol constraint that you want to apply, if any. The maximum length is 63 characters. For details, see waf HTTP-protocol-parameter-restriction on page 543. To display the list of existing constraints, enter: <pre>set HTTP-protocol-parameter-restriction ?</pre>	No default.
url-access-policy "<policy_name>"	Enter the name of a URL access policy. The maximum length is 63 characters. For details, see waf url-access url-access-policy on page 664. To display the list of existing policies, enter: <pre>set url-access-policy ?</pre>	No default.
allow-method-policy "<policy_name>"	Enter the name of an allowed method policy. The maximum length is 63 characters. For details, see "server-policy custom-application application-policy" on page 1. To display the list of existing policies, enter: <pre>set allow-method-policy ?</pre>	No default.
ip-list-policy "<policy_name>"	Enter the name of a trusted IP or blocklisted IP policy. The maximum length is 63 characters. For details, see "server-policy custom-application application-policy" on page 1. To display the list of existing policies, enter: <pre>set ip-list-policy ?</pre>	No default.
geo-block-list-policy "<policy_name>"	Enter the name of a geographically-based client IP block list that you want to apply, if any. The maximum length is 63 characters. For details, see waf geo-block-list on page 511. To display the list of existing policies, enter: <pre>set geo-block-list-policy ?</pre>	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 waf ip-intelligence-ignore-x-forwarded-for on page 560.	disable
csrf-protection "<rule_name>"	Select the name of cross-site request forgery protection rule, if any, to apply to matching requests. See waf csrf-protection on page 464. To display the list of existing rules, enter: <pre>set csrf-protection ?</pre>	

Variable	Description	Default
	Available only when client-management {enable disable} on page 707 is enabled.	
user-tracking-policy "<user-tracking-policy_name>"	Select the name of a user tracking policy. The maximum length is 63 characters. For details, see waf user-tracking policy on page 684 . To display the list of existing policies, enter: <code>set user-tracking-policy ?</code>	No default.
data-analysis {enable disable}	Enable this to collect data for servers covered by this profile.	disable
comment "<comment_str>"	Enter 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.
openapi-validation-policy "<openapi-validation-policy_name>"	Select the openapi validation policy name.	No default.
json-validation-policy "<json-validation-policy_name>"	Select the JSON protection policy name.	No default.
mobile-app-identification {enable disable}	Enable to configure the JWT token secret and token header to verify a request from a mobile application. Refer to the Approov documentation for how to get the token.	disable
token-secret <token-secret_str>	Enter the token secret that you have got from Approov. Available only when mobile-app-identification {enable disable} is enable.	No default
token-header <token-header_str>	Specify the header where the token is carried. Available only when mobile-app-identification {enable disable} is enable.	No default
mobile-api-protection <mobile-api-protection_name>	Select the name of an existing API protection policy. For details, see waf mobile-api-protection . Available only when mobile-app-identification {enable disable} is enable.	No default
syntax-based-attack-detection <detection_name>	Select the name of an existing SQL/XSS syntax based detection policy. For details, see waf syntax-based-attack-detection .	No default
owasp_api_top10_log_field {enable/disable}	Enable to record the OWASP API Top10 attack categories in attack logs so that you can filter the attack logs by OWASP API Top10.	enable

Related topics

- [server-policy policy on page 150](#)
- [waf signature on page 612](#)
- [waf padding-oracle on page 606](#)
- [waf parameter-validation-rule on page 610](#)
- [waf url-access url-access-rule on page 669](#)
- [waf allow-method-exceptions on page 423](#)
- [system settings on page 372](#)
- [waf geo-block-list on page 511](#)
- [waf hidden-fields-protection on page 522](#)
- [waf HTTP-protocol-parameter-restriction on page 543](#)
- [waf ip-intelligence-ignore-x-forwarded-for on page 560](#)
- ["server-policy custom-application application-policy" on page 1](#)
- [waf syntax-based-attack-detection on page 640](#)

waf webshell-detection-policy

Use this command to set Web Shell Detection policies that FortiWeb will use to Trojans in the files that can be uploaded to your web servers.

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.

Web Shell Detection detects Trojan in the uploaded files. In addition to the traditional method which detects Trojan based on tags and keywords, Web Shell Detection can perform fuzzy hash based detection as well, where it determines the similarity by comparing the hash value of the file and the Trojan sample library. In this way, no matter how the attacker modifies the script, as long as the similarity meets the threshold, it can be identified as a Trojan.

Web Shell Detection is divided into two categories: Fuzzy Hash Based Detection and Known Web Shells. And each category is divided into five categories according to the type, namely PHP, ASP, JSP, Perl, and Python.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf webshell-detection-policy
edit "<file-upload-restriction-policy_name>"
    set action {alert | alert_deny | block-period | deny_no_log}
    set block-period <seconds_int>
    set severity {High | Medium | Low | Info}
    set trigger <trigger-policy_name>
    set fuzzy-similarity-threshold <threshold>
    set fuzzy-asp-status {enable | disable} on page 714
    set fuzzy-jsp-status {enable | disable}
    set fuzzy-php-status {enable | disable}
    set fuzzy-perl-status {enable | disable}
    set fuzzy-python-status {enable | disable}
```



```

set known-asp-status {enable | disable}
set known-jsp-status {enable | disable}
set known-php-status {enable | disable}
set known-php-short-open-tag {enable | disable}
set known-perl-status {enable | disable}
set known-python-status {enable | disable}
config fuzzy-disable-list
    edit edit <webshell-name>
end
end
end

```

Variable	Description	Default
"<file-upload-restriction-policy_name>"	Enter the name of an existing or new Web Shell Detection policy. The maximum length is 63 characters. To display the list of existing policies, enter: <pre>edit ?</pre>	No default.
action {alert alert_deny block-period deny_no_log}	Enter 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. For details, see "system replacemsg" on page 1 and the <i>FortiWeb Administration Guide</i>: http://docs.fortinet.com/fortiweb/admin-guides block-period—Block subsequent requests from the client for a number of seconds. Also configure block-period <seconds_int> on page 714. deny_no_log—Deny a request. Do not generate a log message. Note: If FortiWeb is deployed behind a NAT load balancer, when using this option, you must also define an X-header that indicates the original client's IP. Failure to do so may cause FortiWeb to block all connections when it detects a violation of this type. For details, see waf x-forwarded-for on page 721. Caution: This setting will be ignored if monitor-mode {enable disable} on page 163 is enabled. Note: Logging and/or alert email will occur only if enabled and configured. For details, see log disk on page 66 and log alertMail on page 60.	alert_deny

Variable	Description	Default
	Note: If an auto-learning profile will be selected in the policy with Offline Protection profiles that use this rule, you should select <code>alert</code> . If the action is <code>alert_deny</code> , the FortiWeb appliance will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. For details about auto-learning requirements, see " waf web-protection-profile autolearning-profile " on page 1.	
<code>block-period</code> <seconds_ int>	If action {alert alert_deny block-period deny_no_log} on page 713 is <code>block-period</code> , type the number of seconds that violating requests will be blocked. The valid range is 1–3,600 seconds.	600
<code>severity</code> {High Medium Low Info}	Select the severity level to use in logs and reports generated when a violation of the rule occurs.	medium
<code>trigger</code> <trigger- policy_name>	Enter the name of the trigger to apply when this policy is violated. For details, see log trigger-policy on page 96 . The maximum length is 63 characters. To display the list of existing triggers, enter: <code>set trigger ?</code>	No default
<code>fuzzy- similarity- threshold</code> <threshold>	Web Shell Detection can perform fuzzy hash based detection to determines the similarity by comparing the hash value of the file and the Trojan sample library. In this way, no matter how the attacker modifies the script, as long as the similarity meets the threshold, it can be identified as a Trojan. Specify the Fuzzy Similarity Threshold. A file will be identified as a Trojan when it resembles the Trojan sample library by the specified percentage. The valid range is 1-100 (%).	80
<code>fuzzy-asp- status {enable disable}</code>	Enable or disable fuzzy hash based detection for ASP script type.	enable
<code>fuzzy-jsp- status {enable disable}</code>	Enable or disable fuzzy hash based detection for JSP script type.	enable
<code>fuzzy-php- status {enable disable}</code>	Enable or disable fuzzy hash based detection for PHP script type.	enable
<code>fuzzy-perl- status {enable disable}</code>	Enable or disable fuzzy hash based detection for Perl script type.	enable
<code>fuzzy-python-</code>	Enable or disable fuzzy hash based detection for Python script type.	enable

Variable	Description	Default
status {enable disable}		
known-asp-status {enable disable}	Enable or disable FortiWeb to detect ASP script type according to known signatures.	enable
known-jsp-status {enable disable}	Enable or disable FortiWeb to detect JSP script type according to known signatures.	enable
known-php-status {enable disable}	Enable or disable FortiWeb to detect PHP script type according to known signatures.	enable
known-php-short-open-tag {enable disable}	By default, FortiWeb uses both the <code><?ph</code> and <code><?</code> tags to identify the start of a PHP file. However, if you find that the short open tag <code><?</code> does not consistently indicate the beginning of a PHP file in your specific files (for instance, a PDF file begins with <code><?</code>), you can disable this option to ensure that <code><?</code> is not considered, and only <code><?ph</code> will be recognized as the indication of a PHP file beginning.	enable
known-perl-status {enable disable}	Enable or disable FortiWeb to detect Perl script type according to known signatures.	enable
known-python-status {enable disable}	Enable or disable FortiWeb to detect Python script type according to known signatures.	enable
edit <webshell-name>	Enter the web shell name to exclude it. The uploaded file containing the specified script will not be identified as an attack.	No default

Related topics

- [server-policy custom-application application-policy on page 1](#)
- [log trigger-policy on page 96](#)
- [system fortisandbox on page 305](#)

waf websocket-security rule

Use this command to configure WebSocket rule related settings.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```

config waf websocket-security rule
edit websocket-security_rule_name
    set host-status {enable | disable}
    set host <host_str>
    set url-type {plain | regular}
    set url <url_str>
    set block-websocket-traffic {enable | disable}
    set action {alert | deny_no_log | alert_deny}
    set max-frame-size <max-frame-size_int>
    set max-message-size <max-message-size_int>
    set block-extensions {enable | disable}
    set enable-attack-signatures {enable | disable}
    set allow-plain-text {enable | disable}
    set allow-binary-text {enable | disable}
config allowed-origin-list
    edit allowed-origin-list <allowed-origin-list_id> on page 717
        set origin <origin_str> on page 717
    next
end
next
end

```

Variable	Description	Default
websocket-security_rule_name	Enter the WebSocket security rule name.	No default.
host-status {enable disable}	Enable to compare the WebSocket security rule to the <code>Host :</code> field in the HTTP header.	No default.
host <host_str>	Select the IP address or fully qualified domain name (FQDN) of the protected host to which this rule applies. This option is available only if Host Status is enabled.	No default.
url-type {plain regular}	Select whether the URL Pattern field will contain a literal URL (Simple String), or a regular expression designed to match multiple URLs (Regular Expression).	Plain
url <url_str>	The URL which hosts the web page containing the user input fields you want to protect.	No default.
block-websocket-traffic {enable disable}	Enable to deny the WebSocket traffic, and FortiWeb will not check any WebSocket related traffic. This option is disabled by default.	Disable
action {alert deny_no_log alert_deny}	Select which action the FortiWeb appliance will take when it detects a violation. Alert—Accept the connection and generate an alert email and/or log message. Alert & Deny—Block the request (or reset the connection) and generate an alert and/or log message. Deny (no log)—Block the request (or reset the	Alert

Variable	Description	Default
	connection).	
max-frame-size <max-frame-size_int>	Specifies the maximum acceptable frame header and body size in bytes. The valid range is 0–2147483647 bytes.	64
max-message-size <max-message-size_int>	Specifies the maximum acceptable message header and body size in bytes. The valid range is 0–2147483647 bytes.	1024
block-extensions {enable disable}	Enable to not check the extension header in WebSocket handshake packet. By default, this option is disabled.	Disable
enable-attack-signatures {enable disable}	Enable to detect attack in WebSocket message body. But if WebSocket traffic has extension header and allow extension header in WebSocket security rule, FortiWeb can not detect attack signatures. When attack signature is detected, the actions FortiWeb will take follow those of related signatures.	Disable
allow-plain-text {enable disable}	Enable to allow detecting the plain text.	Enable
allow-binary-text {enable disable}	Enable to allow detecting the binary text.	Enable
allowed-origin-list <allowed-origin-list_id>	Enter the origin list ID in WebSocket handshake packet.	No default.
origin <origin_str>	Enter the allowed origin.	No default.

Related topics

- [waf HTTP-constraints-exceptions on page 534](#)
- [waf HTTP-protocol-parameter-restriction on page 543](#)

waf websocket-security policy

Use this command to create WebSocket policy.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf websocket-security policy
edit "<"<policy_name>"
    config rule-list
        edit rule-list_id on page 718
```

```

        set rule "<rule_name>"
    next
end
next
end

```

Variable	Description	Default
"<policy_name>"	Enter the WebSocket Security policy name.	No default.
rule-list_id	Enter the sequence number of the rule in the rule list.	
rule "<rule_name>"	Select the created WebSocket security rule name.	No default.

Related topics

- [waf websocket-security rule on page 715](#)

waf ws security

Use this command to create WS-security rules.

You can use WS-Security rules to do the following:

- Encrypt and decrypt parts of SOAP messages
- Digitally sign parts of SOAP messages
- Verify parts of SOAP messages using digital signatures

Syntax

```

config waf ws-security rule
edit "<ws-security_rule_name>"
    set encryption-algorithm {3EDS | AES-128 | AES-256}
    set encryption-part {Element Value | Element Markup}
    set key-transport-algorithm {RSA-15 | RSA-OAEP}
    set request-operation {Sign Verify & Decrypt | Decrypt | Sign Verify}
    set request-security-status {enable | disable}
    set response-operation {Sign | Encrypt | Sign & Encrypt | Encrypt & Sign}
    set response-security-status {enable | disable}
    set signature-algorithm {RSA-SHA-1 | HMAC-SHA-1}
    set xml-client-certificate-group <xml-client-certificate_group_str>
    set xml-server-certificate <xml-server-certificate_str>
    config namespace-mapping
        edit waf ws security
            set prefix <prefix_str>
            set namespace <namespace_str>
        next
    end
    config element-list
        edit waf ws security

```

```

        set xpath <xpath_str>
        set direction {request | response}
    next
end
next
end

```

Variable	Description	Default
"<ws-security_rule_name>"	Enter a name that can be referenced by other parts of the configuration.	No default.
encryption-algorithm {3EDS AES-128 AES-256}	Select the encryption algorithm. • 3EDS • AES-128 • AES-256 Available only when response-security-status {enable disable} is enable, and response-operation {Sign Encrypt Sign & Encrypt Encrypt & Sign} is Encrypt, Sign & Encrypt, or Encrypt & Sign.	3EDS
encryption-part {Element Value Element Markup}	Select which part of the SOAP messages to encrypt. • Element Value • Element Markup	Element Value
key-transport-algorithm {RSA-15 RSA-OAEP}	Select the key transport algorithm. • RSA-15 • RSA-OAEP	RSA-15
request-operation {Sign Verify & Decrypt Decrypt Sign Verify}	Select the operation that FortiWeb performs for the encrypted SOAP messages from the client. • Sign Verify & Decrypt • Decrypt • Sign Verify	Sign Verify
request-security-status {enable disable}	Enable to configure FortiWeb to decrypt, sign and verify the encrypted SOAP messages from the client.	disable
response-operation {Sign Encrypt Sign & Encrypt Encrypt & Sign}	Select the operation that FortiWeb performs for the SOAP messages returned from the server. • Sign • Encrypt • Sign & Encrypt • Encrypt & Sign	Sign
response-security-status {enable disable}	Enable to configure FortiWeb to encrypt , and sign the SOAP messages returned from the server.	disable
signature-algorithm {RSA-SHA-1 HMAC-SHA-1}	Select the signature algorithm. • RSA-SHA-1 • HMAC-SHA-1	RSA-SHA-1

Variable	Description	Default
xml-client-certificate-group <xml-client-certificate_group_str>	Select the XML client certificate group created from XML Certificate > Client Certificate Group. Available only when request-operation {Sign Verify & Decrypt Decrypt Sign Verify} is <code>enable</code>, and the request-operation {Sign Verify & Decrypt Decrypt Sign Verify} is Sign Verify & Decrypt or Sign Verify. Or Available only when response-security-status {enable disable} is <code>enable</code>, and the response-operation {Sign Encrypt Sign & Encrypt Encrypt & Sign} is Encrypt, Sign & Encrypt or Encrypt & Sign.	No default.
xml-server-certificate <xml-server-certificate_str>	Select the XML server certificate uploaded from XML Certificate> Server Certificate. Available only when request-security-status {enable disable} is <code>enable</code>, and the request-operation {Sign Verify & Decrypt Decrypt Sign Verify} is Sign Verify & Decrypt or Decrypt . Or Available only when response-security-status {enable disable} is <code>enable</code>, and the response-operation {Sign Encrypt Sign & Encrypt Encrypt & Sign} is Sign, Sign & Encrypt, or Encrypt & Sign.	No default.
"<namespace-mapping_name_id>"	Enter the index number of an entry to create a namespace mapping.	No default.
namespace <namespace_str>	Enter the namespace.	No default.
prefix <prefix_str>	Enter a prefix for the namespace.	No default.
"<element-list_name_id>"	Enter the index number of an entry to create an element list.	No default.
xpath <xpath_str>	Enter an XPath to specify which part of the XML file to process.	No default.
direction {request response}	Select either Request or Response to define in which direction the XPath applies to.	<code>request</code>

Related topics

- [Configuring XML protection on page 1](#)
- [system certificate xml-client-certificate on page 266](#)
- [system certificate xml-client-certificate-group on page 270](#)
- [system certificate xml-server-certificate on page 393](#)

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 "Defining your proxies, clients, & X-headers" in *FortiWeb Administration Guide*:

<https://docs.fortinet.com/document/fortiweb/7.6>

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

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 merge-headers {enable | disable}
    set delete-headers {enable | disable}
    set x-forwarded-for-support {enable | disable}
    set ip-location-add {left | right}
    set x-real-ip {enable | disable}
    set skip-private-original-ip {enable | disable}
    set add-source-port {enable | disable}
    set x-forwarded-port {enable | disable}
    config ip-list
      edit <entry_index>
        set ip "<load-balancer_ip>"
      next
    end
  next
end
```

Variable	Description	Default
"<x-forwarded-for_name>"	Enter the name of the new or existing group. The maximum length is 63 characters. To display the list of existing groups, enter: 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

Variable	Description	Default
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. If there are multiple X-headers, "left" is the left location of the first x-header, and "right" is the right location of the last x-header. 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.	right
original-ip-header "<HTTP-header-key_str>"	Enter the key of the X-header, such as X-Forwarded-For X-Real-IP, without the colon (:), that contains the original source IP address of the client. Also configure tracing-original-ip {enable disable} on page 722 and, for security reasons, ip "<load-balancer_ip>" on page 724. 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>" on page 722 and, for security reasons, ip "<load-balancer_ip>" on page 724. 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 <i>FortiWeb Administration Guide</i>: https://docs.fortinet.com/document/fortiweb 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
merge-headers {enable disable}	Enable to merge all the previous X-Forward-For headers into one header to create an IP list. Headers are merged based on their location in the request, which means the IPs of the first header will be at the beginning of the new list followed by the IPs of the next header. The Delete Previous XFF Headers is executed before Merge Previous XFF Headers. If these two options are both enabled, Merge Previous XFF Headers actually takes no effect because all the previous XFF Headers have already been deleted.	disable

Variable	Description	Default
delete-headers {enable disable}	Enable to delete all the previous X-Forward-For headers. If x-forwarded-for-support is enabled, the request will only have one header and one IP which is created by FortiWeb.	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
ip-location-add {left right}	Left : Add IP address at the leftmost position of the first header. Right : Add IP address at the rightmost position of the last header. Available only when x-forwarded-for-support is enabled.	left
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. For details, see x-forwarded-for-support {enable disable} on page 723. 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 or True Transparent Proxy mode.	disable
skip-private-original-ip {enable disable}	Enable to skip the private original IP that indicates the service used in the client's original request.	enable

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>	Enter the index number of the individual entry in the table. The valid range is 1–9,223,372,036,854,775,807. 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>" on page 722 only if the packet arrived from one of the IP addresses you specify here. It regards original-ip-header "<HTTP-header-key_str>" on page 722 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.
add-source-port {enable disable}	Enable to add an X-Forwarded-For: header with the connection's source IP. If this field is enabled, the source port of the request will be added as well. Available only when FortiWeb operates in Reverse Proxy, True Transparent Proxy, or WCCP mode.	disable
x-forwarded-port {enable disable}	Enable to add an X-Forwarded-Port: header with the connection's destination port. Available only when FortiWeb operates in Reverse Proxy, True Transparent Proxy, or WCCP mode.	disable

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 192.0.2.105 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 "192.0.2.105"
        next
    end
    set block-based-on-original-ip enable
next
end
```

waf xml-dtd

Use this command to view DTD files that have already been uploaded to FortiWeb. You can upload DTD files only in the web UI through the **XML DTD** tab in **Web Protection > XML Protection**.

A Document Type Definition (DTD) is a specification that defines the structure, legal elements, and attributes of an XML document. By importing a DTD file, you can validate an XML request to ensure it adheres to the specified rules and constraints outlined in the DTD.

XML DTD files are included in XML protection rules. XML protection rules define acceptable parameters for XML content in HTTP requests. Groups of XML protection rules are grouped into XML protection policies. For details, see [waf xml-validation on page 727](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf xml-dtd file
    edit waf xml-dtd
end
```

Variable	Description	Default
"<xml_dtd_file_name>"	To display a list of existing XML DTD files, enter: edit ?	No default.

Related topics

- [waf xml-validation on page 727](#)

waf xml-exempted-urls

When you configure schema location to forbid using location field to perform malicious requests, you can use this command to exempt specific URLs from XML protection.

Syntax

```
config waf xml-exempted-urls
  edit "<xml-exempted-urls_name>"
    config exempted-url-list
      edit exempted-url-list <exempted-url-list_str>
        set url-type {plain | regular}
        set exempted-url <exempted-url_str>
      next
    end
  next
end
```

Variable	Description	Default
"<xml-exempted-urls_name>"	Enter the name for the Exempted URLs list.	No default.
exempted-url-list <exempted-url-list_str>	Enter the ID for the he Exempted URLs list.	No default.
url-type {plain regular}	Select whether the <code>exempted-url <exempted-url_str></code> on page 726 field must contain either <code>plain</code>—The field is a string that the request URL must match exactly. <code>regular</code>—The field is a regular expression that defines a set of matching URLs.	No default.
exempted-url <exempted-url_str>	Depending on your selection in <code>url-type {plain regular}</code> on page 726 , enter either: <code>plain</code>—The literal URL, such as <code>/index.php</code>, that the HTTP request must contain in order to match the rule. The URL must begin with a slash (/). <code>regular</code>—A regular expression, such as <code>^/*\.php</code>, matching the URLs to which the rule should apply. The pattern does not require a slash (/), but it must match URLs that begin with a slash, such as <code>/index.cfm</code>.	No default.

Related topics

- [waf xml-validation on page 727](#)
- [waf xml-wsdl on page 735](#)

waf xml-schema

Use this command to view XML schema files that have already been uploaded to FortiWeb. You can upload XML schema files only in the web UI.

XML schema files specify the acceptable structure of an elements in an XML document. When you use XML schema files to check XML content in HTTP requests, FortiWeb can determine whether content is allowed and validate that content is well-formed.

XML schema files are included in XML protection rules. XML protection rules define acceptable parameters for XML content in HTTP requests. Groups of XML protection rules are grouped into XML protection policies. For details, see [waf xml-validation on page 727](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf xml-schema file
  edit "<xml_schema_file_name>"
end
```

Variable	Description	Default
"<xml_schema_file_name>"	To display a list of existing XML schema files, enter: edit ?	No default.

Related topics

- [waf xml-validation on page 727](#)

waf xml-validation

Use this command to create XML protection rules and configure XML protection policies. You can create up to 256 rules per policy.

XML is commonly used for data exchange, and hackers sometimes try to exploit security holes in XML to attack web servers. Using this command, you can configure FortiWeb to examine lcient requests for anomalies in XML. Configuring XML protection can help ensure that the content of HTTP requests containing XML does not contain any potential attacks.

XML protection is available in Reverse Proxy, True Transparent Proxy, and WCCP operating modes.

Syntax

```
config waf xml-validation rule
```

```

edit "<xml_rule_name>"
  set action {alert | alert_deny | block-period | redirect | send_403_forbidden |
    deny_no_log}
  set block-period <period_int>
  set expansion-entity-check {enable | disable}
  set external-entity-check {enable | disable}
  set host "<host_name_str>"
  set host-status {enable | disable}
  set request-file "<file_str>"
  set request-type {plain | regular}
  set dtd-file <dtd_file_name>
  set schema-file "<schema_file_name>"
  set severity {High Low | Medium | Info}
  set trigger "<trigger_policy_name>"
  set xml-attributes-check {enable | disable}
  set xml-limit-attr-num <limit_int>
  set xml-limit-attrname-len <limit_int>
  set xml-limit-attrvalue-len <limit_int>
  set xml-limit-cdata-len <limit_int>
  set xml-limit-check {enable | disable}
  set xml-limit-element-depth <limit_int>
  set xml-limit-element-name-len <limit_int>
  set data-format {xml | soap}
  set wsdl-ip-port-override {enable | disable}
  set wsdl-file <wsdl-file_name>
  set ws-security <string>
  set xsw <string>
  set validate-soapaction {enable | disable}
  set validate-soap-headers {enable | disable}
  set allow-additional-soap-headers {enable | disable}
  set validate-soap-body {enable | disable}
  set x-include-check {enable | disable}
  set schema-location-check {enable | disable}
  set schema-location-exempted-urls <schema-location-exempted-urls_str>
  set soap-attachment {allow | disallow} on page 733
  set ws-i-basic-profile-assertion {WSI1001 | WSI1002 | WSI1003 | WSI1004 | WSI1006
    | WSI1007 | WSI1032 | WSI1033 | WSI1109 | WSI1110 | WSI1111 | WSI1201 |
    WSI1202 | WSI1204 | WSI1208 | WSI1301 | WSI1307 | WSI1308 | WSI1309 | WSI1318
    | WSI1601 | WSI1701} on page 733
  set ws-i-basic-profile-wsdl-assertion {WSI1008 | WSI1116 | WSI1211} on page 734
next
end
config waf xml-validation policy
  edit "<xml_policy_name>"
    set enable-signature-detection {enable | disable}
    config input-rule-list
      edit <entry_index>
        set "<xml_rule_1>"
      next
    end
  next
end

```


Variable	Description	Default
"<xml_rule_name>"	Enter a name that can be referenced by other parts of the configuration. You will use the name to select the rule in an XML protection policy. The maximum length is 63 characters.	No default.
action {alert alert_deny block-period redirect send_403_forbidden deny_no_log}	Select one of the following actions that FortiWeb performs when a request violates the rule: 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. For details, see "system replacemsg" on page 1. block-period—Block subsequent requests from the client for a number of seconds. Also configure waf xml-validation on page 727. 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>" on page 704 and rdt-reason {enable disable} on page 704. send_403_forbidden—Reply to the client with an HTTP 403 Access Forbidden error message and generate an alert email and/or log message. deny_no_log—Deny a request. Do not generate a log message. Caution: FortiWeb ignores this setting when monitor-mode {enable disable} on page 163 is enabled. Note: Logging and/or alert email will occur only if enabled and configured. For details, see log disk on page 66 and log alertMail on page 60.	alert
block-period <period_int>	Enter the amount of time (in seconds) that you want to block subsequent requests from a client after FortiWeb detects a rule violation. This setting is available only when waf xml-validation on page 727 is <code>block-period</code> . The valid range is 1–3,600 seconds.	600
expansion-entity-check {enable disable}	Enable to trigger the waf xml-validation on page 727 if an HTTP request contains an XML recursive entity expansion. To enable this option, you must first enable waf xml-validation on page 727.	disable
external-entity-check {enable disable}	Enable to trigger the waf xml-validation on page 727 if an HTTP request contains an external entity in XML. To enable this option, you must first enable waf xml-validation on page 727.	disable
host "<host_name_str>"	Enter the name of a protected host that the <code>Host :</code> field of an HTTP request must match in order for the rule to apply. For details, see server-policy allow-hosts on page 106 .	No default.

Variable	Description	Default
host-status {enable disable}	Enable to compare the XML rule to the Host: field in the HTTP header. If enabled, also configure waf xml-validation on page 727 .	disable
request-file "<file_str>"	Depending on your selection for waf xml-validation on page 727 , enter either: plain—The literal URL, such as <code>/index.php</code>, that the HTTP request must contain in order to match the rule. The URL must begin with a slash (/). regular—A regular expression, such as <code>^/*\.php</code>, matching the URLs to which the rule should apply. The pattern does not require a slash (/), but it must match URLs that begin with a slash, such as <code>/index.cfm</code>. Do not include the domain name, such as <code>www.example.com</code> , which is configured separately in waf xml-validation on page 727 .	No default.
request-type {plain regular}	Select whether waf xml-validation on page 727 must contain either: Simple String—The field is a string that the request URL must match exactly. Regular Expression—The field is a regular expression that defines a set of matching URLs.	No default.
dtd-file <dtd_file_name>	Select the DTD file uploaded in the web UI through the XML DTD tab in Web Protection > XML Protection . Available only when the data-format is XML . Note: If you upload an XML DTD file that refers to other DTD schema files, the other DTD files must also be uploaded to FortiWeb.	No default.
schema-file "<schema_file_name>"	Select an XML schema file. To display a list of existing XML schema files, enter: set schema-file ? Note, if you select an XML schema file that references other XML schema files, the other XML schema files must also be uploaded to FortiWeb.	No default.
severity {High Low Medium Info}	When rule violations are recorded in the attack log, each log message contains a Severity Level field. Select which severity level FortiWeb will use when it logs a violation of the rule: - Low - Medium - High - Info	Low
trigger "<trigger_policy_name>"	Enter the name of the trigger, if any, to apply when the rule is violated. The maximum length is 63 characters. For details, see log trigger-policy on page 96 . To display a list of existing triggers, enter: set trigger ?	No default.

Variable	Description	Default
xml-attributes-check {enable disable}	Enable to configure waf xml-validation on page 727 and waf xml-validation on page 727 .	disable
xml-limit-attr-num <limit_int>	Enter the maximum number of attributes for each element. The valid range is 1–256. To configure this option, you must first enable waf xml-validation on page 727 .	20
xml-limit-attrname-len <limit_int>	Enter the maximum attribute name length (in bytes) of each element. The valid range is 1–1,024. To configure this option, you must first enable waf xml-validation on page 727 .	64
xml-limit-attrvalue-len <limit_int>	Enter the maximum attribute value length (in bytes) of each element. The valid range is 1–2,048. To configure this option, you must first enable waf xml-validation on page 727 .	1,024
xml-limit-cdata-len <limit_int>	Enter the maximum Character Data (CDATA) length (in bytes) in XML. The valid range is 1–4,096. To configure this option, you must first enable waf xml-validation on page 727 .	4,096
xml-limit-check {enable disable}	Enable to configure XML limits.	disable
xml-limit-element-depth <limit_int>	Enter the maximum element depth in XML. The valid range is 1–256. To configure this option, you must first enable waf xml-validation on page 727 .	20
xml-limit-element-name-len <limit_int>	Enter the maximum element name length (in bytes) in XML. The valid range is 1–1,024. To configure this option, you must first enable waf xml-validation on page 727 .	64
"<xml_policy_name>"	Enter the name of an XML protection policy. You will use the name to select the policy in other parts of the configuration. The maximum length is 63 characters.	No default.
<entry_index>	Enter the index number of an entry to create or modify a rule for the policy. The valid range is 1–9,999,999,999,999,999,999.	No default.
"<xml_rule_1>"	Enter the sequence number of an XML protection rule to add to the XML protection policy. The maximum length is 63 characters.	No default.

Variable	Description	Default
data-format {xml soap}	Select the XML protection rule format.	No default.
wSDL-ip-port-override {enable disable}	When enabled, only the URL will be used to match the service in WSDL. If a URL corresponds to multiple services, the first service will be matched.	disable
wSDL-file <wSDL-file_name>	This field applies when the Data Format is SOAP. Enter a name for the WSDL file.	No default.
ws-security <string>	Select the WS-Security rule created with <code>config waf ws-security rule</code> . Available only when the <code>data-format</code> is SOAP.	
xsw <string>	Select the XSW Detection rule created with <code>config waf xsw-detection rule</code> .	No default.
validate-soapaction {enable disable}	Enable to validate whether the soapAction in SOAP protocol complies with that in WSDL file.	No default.
validate-soap-headers {enable disable}	Enable to validate whether the header elements in SOAP protocol comply with those in WSDL file.	No default.
allow-additional-soap-headers {enable disable}	Enable not to validate additional header elements.	No default.
validate-soap-body {enable disable}	Enable to validate whether the body elements in SOAP protocol comply with those in WSDL file.	No default.
x-include-check {enable disable}	Enable to trigger the action {alert alert_deny block-period redirect send_403_forbidden deny_no_log} on page 729 if other XML contents are included in XML.	No default.
schema-location-check {enable disable}	Enable to forbid using location field to perform malicious requests.	No default.

Variable	Description	Default
schema-location-exempted-urls <schema-location-exempted-urls_str>	Select the exempted URL you have created to configure allowed location URLs. Available only when schema-location-check {enable disable} on page 732 is enabled.	No default.
enable-signature-detection {enable disable}	Enable to scan for matches with attack and data leak signatures in Web 2.0 (XML AJAX), SOAP, and other XML submitted by clients in the bodies of HTTP POST requests.	disable
soap-attachment {allow disallow}	Specify whether the SOAP message can carry attachments. Available only when the data-format {xml soap} on page 732 is SOAP .	Allow
ws-i-basic-profile-assertion {WSI1001 WSI1002 WSI1003 WSI1004 WSI1006 WSI1007 WSI1032 WSI1033 WSI1109 WSI1110 WSI1111 WSI1201 WSI1202 WSI1204 WSI1208 WSI1301 WSI1307 WSI1308 WSI1309 WSI1318 WSI1601 WSI1701}	Select WSI rules that SOAP messages will adhere to. Available only when the data-format {xml soap} on page 732 is SOAP .	No default

Variable	Description	Default
ws-i-basic-profile-wsdl-assertion {WSI1008 WSI1116 WSI1211}	If you select these three rules, configure WSDL files first. Available only when the data-format {xml soap} on page 732 is SOAP .	No default

Example

The below example creates an XML protection rule and applies the rule to a new XML protection policy.

```
config waf xml-validation rule
  edit "example_rule_name_1"
    set action block-period
    set block-period 3000
    set severity Medium
    set trigger "example_trigger_policy_name"
    set host-status enable
    set host "example_host_name"
    set request-type plain
    set request-file "/index.php"
    set schema-file "example_schema_file_name"
    set xml-limit-check enable
    set xml-limit-attr-num 64
    set xml-limit-attrname-len 256
    set xml-limit-attrvalue-len 1024
    set xml-limit-cdata-len 2096
    set xml-limit-element-depth 128
    set xml-limit-element-name-len 128
    set xml-entity-check enable
    set expansion-entity-check enable
    set external-entity-check enable
  next
end
config waf xml-validation policy
  edit "example_policy_name"
    config input-rule-list
      edit "example_rule_1"
        set "example_rule_1"
      next
    end
  next
end
```

Related topics

- [waf xml-schema on page 727](#)
- [waf xml-wsdl on page 735](#)
- [waf web-protection-profile inline-protection on page 696](#)

waf xml-wsdl

Use this command to view XML wsdl files that have already been uploaded to FortiWeb. You can upload XML wsdl files only in the web UI.

WSDL files are XML files that describe how to use SOAP to invoke web service. To configure FortiWeb to verify legality of WSDL files and check the SOAP message against WSDL and SOAP protocol, create an XML protection rule and select a WSDL file for that rule. You can select only one WSDL file for each XML protection rule, but you can configure FortiWeb to enforce multiple rules in XML protection policies.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wafgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config waf xml-wsdl file
  edit "<xml_wsdl_file_name>"
end
```

Variable	Description	Default
"<xml_wsdl_file_name>"	To display a list of existing XML WSDL files, enter: edit ?	No default.

Related topics

- [waf xml-validation on page 727](#)

waf xsw-detection rule

Use this command to create XSW Detection rules.

XML Signature Wrapping (XSW) allows a malicious client to modify or forge a digitally signed document without breaking the included signature. This attack is accomplished by moving the original nodeset to another location within the document and replacing the contents.

To counter XSW attacks, FortiWeb will locate the signed node within the XML file and execute verification specifically at that location. Consequently, if a forged node is positioned at the original node's location or the original node is moved to another location, FortiWeb will be able to detect it. In the XSW Detection rule, XPath is employed to specify the correct location of the signed node, while a certificate is used to verify whether the content of the signed node is legitimate.

Syntax

```
config waf xsw-detection rule
  set xml-client-certificate-group
  config namespace-mapping
```

```

edit "<namespace-mapping_name>"
    set prefix <string>
    set namespace <string>
next
end
config element-list
edit "<element-list_name>"
    set xpath <xpath_str>
    set id-attr-name <string>
next
end
end

```



For more information on how to define namespace, XPath, and ID attribute name, please refer to "Creating XSW Detection rules" in *FortiWeb Administration Guide*.

Variable	Description	Default
"<xsw-detection_rule_name>"	Enter a name that can be referenced by other parts of the configuration.	No default.
xml-client-certificate-group <xml-client-certificate_group_str>	Select the XML client certificate group created from XML Certificate > Client Certificate Group.	No default.
"<namespace-mapping_name_id>"	Enter the index number of an entry to create a namespace mapping.	No default.
namespace <string>	Enter the namespace.	No default.
prefix <string>	Enter a prefix for the namespace.	No default.
"<element-list_name_id>"	Enter the index number of an entry to create an element list.	No default.
xpath <xpath_str>	Enter an XPath to specify which part of the XML file to process.	No default.
id-attr-name <string>	Enter the name of the attribute to be protected.	No default.

Related topics

- [Configuring XML protection on page 1](#)
- [system certificate xml-client-certificate on page 266](#)
- [system certificate xml-client-certificate-group on page 270](#)
- [system certificate xml-server-certificate on page 393](#)

wvs limit

Use this command to limit scanning related settings, such as the scanning report size, request interval, etc.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wvsgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config wvs limit
  set report-path-size <report-path-size_int>
  set request-interval <request-interval_int>
  set scan-cpu-usage <scan-cpu-usage_int>
  set scan-memory-usage <scan-memory-usage_int>
  set single-report-size <single-report-size_int>
  set verbose-output {enable | disable}
end
```

Variable	Description	Default
report-path-size <report-path-size_int>	Type the size of the folders that store all scanning reports of all policies (1024~51200 M)	10240
request-interval <request-interval_int>	Type the number of seconds between each request (1~1000 ms).	1
scan-cpu-usage <scan-cpu-usage_int>	Set the CPU limit. When the CPU of all scanning processes exceeds certain parentage of the total CPU, the scanning will be killed (10~80 percent).	70
scan-memory-usage <scan-memory-usage_int>	Set the memory limit. When the memory of all scanning processes exceeds certain parentage of the total memory , the scanning will be killed (10~80 percent).	40
single-report-size <single-report-size_int>	The size of the scanning report file for the first scanning in a single policy (1~5120 M).	512
verbose-output {enable disable}	Control the <code>output.txt</code> contents. Enable to output detailed debug information, which causes large <code>output.txt</code> file.	disable

Example

This example shows how to configure scanning related limitations.

```
config wvs limit
  set report-path-size 10500
  set request-interval 3
  set scan-cpu-usage 60
  set single-report-size 700
  set verbose-output disable
end
```

Related topics

- [wvs policy on page 738](#)
- [wvs schedule on page 743](#)
- [wvs profile on page 740](#)
- [wvs template on page 745](#)

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 [wvs schedule on page 743](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wvsgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
config wvs policy
  edit "<wvs-policy_name>"
    set type {runonce | schedule}
    set schedule "<wvs-schedule_name>"
    set profile "<wvs-profile_name>"
    set email "<email-policy_name>"
    set report_format {html pdf xml}
    set runtime <count_int>
  next
end
```

Variable	Description	Default
"<wvs-policy_name>"	Enter the name of a new or existing web vulnerability scan policy. The maximum length is 63 characters. To display the list of existing policies, enter: <code>edit ?</code>	No default.
type {runonce schedule}	Select either: • <code>runonce</code>—Run the scan immediately after you complete the policy. • <code>schedule</code>—Run the scan on a schedule. Also configure analyzer-policy "<fortianalyzer-policy_name>" on page 97.	runonce

Variable	Description	Default
schedule "<wvs-schedule_name>"	Enter the name of an existing web vulnerability scan schedule. The maximum length is 63 characters. For details, see wvs schedule on page 743. To display the list of existing schedules, enter: <pre>set schedule ?</pre> This setting is applicable only if type {runonce schedule} on page 738 is <code>schedule</code>.	No default.
profile "<wvs-profile_name>"	Enter the name of an existing web vulnerability scan profile. The maximum length is 63 characters. To display a list of the existing profiles, enter: <pre>set profile ?</pre>	No default.
email "<email-policy_name>"	Enter the name of an existing 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 63 characters. For details, see log email-policy on page 68. To display the list of existing policy, enter: <pre>set email ?</pre>	No default.
report_format {html pdf xml}	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: <pre>set runtime 0</pre>	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 xml
    set profile "wvs-profile1"
    set email "EmailPolicy1"
  next
end
```

Related topics

- [wvs profile on page 740](#)
- [wvs schedule on page 743](#)

wvs profile

Use this command to configure web vulnerability scan profiles.

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 details, see [Permissions on page 46](#).

Syntax

```
config wvs profile
edit "<wvs_profile_name>"
    set scan-target <scan-target_str>
    set scan-template <scan-template_id>
    set request-timeout <request-timeout_int>
    set ignore-session-cookies {enable | disable}
    set user-agent-type {custom | random}
    set custom-user-agent <custom-user-agent_str>
    set custom-header0 <custom-header0_str>
    set custom-header1 <custom-header1_str>
    set custom-header2 <custom-header2_str>
    set custom-header3 <custom-header3_str>
    set custom-header4 <custom-header4_str>
    set custom-header5 <custom-header5_str>
    set custom-header6 <custom-header6_str>
    set custom-header7 <custom-header7_str>
    set custom-header8 <custom-header8_str>
    set custom-header9 <custom-header9_str>
    set sub-path-limit <sub-path-limit_int>
    set max-scan-time <max-scan-time_int>
    set max-crawl-time <max-crawl-time_int>
    set max-params-limit <max-params-limit_int>
    set max-file-size <max-file-size_int>
    set max-HTTP-retries <max-HTTP-retries_int>
    set specify-urls-for-scanning {enable | disable}
    set follow-regex <follow-regex_int>
    set ignore-regex <ignore-regex_int>
    set HTTP-basic-authentication {enable | disable}
    set basic-username <basic-username_str>
    set basic-password <basic-password_str>
    set form-based-authentication {enable | disable}
    set form-based-username <form-based-username_str>
    set form-based-password <form-based-password_str>
    set form-based-auth-url <form-based-auth-url_str>
    set username-field <username-field_str>
    set password-field <password-field_str>
    set cookie-jar-file <cookie-jar-file_str>
    set session-check-url <session-check-url_str>
    set session-check-str <session-check-url_str> on page 743
    set data-format <data-format_str>
```

end

Variable	Description	Default
"<wvs_profile_name>"	Type a unique name for the profile name. The maximum length is 63 characters.	No default.
scan-target <scan-target_str>	Enter the URL that you want to scan, such as www.mytestwvs.com .	No default.
scan-template <scan-template_id>	Select an existing scan template that you want to use in the profile.	No default.
request-timeout <request-timeout_int>	Type the number of seconds for the vulnerability scanner to wait for a response from the website before it assumes that the request will not successfully complete, and continues with the next request in the scan. It will not retry timeout requests.	0
ignore-session-cookies {enable disable}	If enabled, the scanner will ignore all session cookies sent by the target web application.	disable
user-agent-type {custom random}	Custom: when there is no user-agent in custom headers, the actual user-agent sent is FortiWeb WVS; when user-agent is set in custom headers, the actual user-agent sent is the value set in custom-user-agent <custom-user-agent_str> on page 741 . random: When the user-agent-type is random, and there is no user-agent in custom headers, the actual user-agent sent is random; when user-agent is set in custom headers, the actual user-agent sent is random.	custom
custom-user-agent <custom-user-agent_str>	Enter the custom user-agent value.	No default.
custom-header0 <custom-header0_str>	You can define the host, user agent, and other common headers in the request.	No default.
custom-header1 <custom-header1_str>	You can define the host, user agent, and other common headers in the request.	No default.
custom-header2 <custom-header2_str>	You can define the host, user agent, and other common headers in the request.	No default.
custom-header3 <custom-header3_str>	You can define the host, user agent, and other common headers in the request.	No default.
custom-header4 <custom-header4_str>	You can define the host, user agent, and other common headers in the request.	No default.
custom-header5 <custom-header5_str>	You can define the host, user agent, and other common headers in the request.	No default.
custom-header6 <custom-header6_str>	You can define the host, user agent, and other common headers in the request.	No default.

Variable	Description	Default
custom-header7 <custom-header7_str>	You can define the host, user agent, and other common headers in the request.	No default.
custom-header8 <custom-header8_str>	You can define the host, user agent, and other common headers in the request.	No default.
custom-header9 <custom-header9_str>	You can define the host, user agent, and other common headers in the request.	No default.
sub-path-limit <sub-path-limit_int>	Enter the maximum number of requests for sub path of each URL.	75
max-scan-time <max-scan-time_int>	Enter the maximum scanning time.	120
max-crawl-time <max-crawl-time_int>	Enter the maximum crawling time (minutes).	60
max-params-limit <max-params-limit_int>	Enter the maximum number of requests for each URL, and parameter set.	25
max-file-size <max-file-size_int>	Indicate the maximum file size (in bytes) that the scanner will retrieve from the remote server.	400,000
max-HTTP-retries <max-HTTP-retries_int>	Indicate the maximum number of retries when requesting an URL. The valid value range is 1–10.	2
specify-urls-for-scanning {enable disable}	Enable to specify the URL to be scanned.	disable
follow-regex <follow-regex_int>	<code>follow-regex</code> is <code>.*</code> . When crawling, do not follow links that match this regular expression.	No default.
ignore-regex <ignore-regex_int>	An empty string (nothing to be ignored), when crawling, only follow that matches this regular expression. <code>ignore-regex</code> has precedence over <code>follow-regex</code> .	No default.
HTTP-basic-authentication {enable disable}	Enable the HTTP basic authentication.	disable
basic-username <basic-username_str>	Enter the username of the web application.	No default.
basic-password <basic-password_str>	Enter the password for the username.	No default.
form-based-authentication {enable disable}	Enable the form based authentication.	disable
form-based-username <form-based-username_str>	The username parameter name, for example, "uname" if the HTML looks like <code><input type="text" name="uname">...</code>	No default.

Variable	Description	Default
form-based-password <form-based-password_str>	The password parameter name, for example, "pwd" if the HTML looks like <code><input type="password" name="pwd">...</code>	No default.
form-based-auth-url <form-based-auth-url_str>	Enter the target URL for security auditing, and the URL shall include <code>HTTP</code> or <code>HTTPS</code> tag.	No default.
username-field <username-field_str>	Enter the username for using in the authentication process.	No default.
password-field <password-field_str>	Enter the password for the username.	No default.
cookie-jar-file <cookie-jar-file_str>	Designate a cookie jar file. The cookie jar file must be in mozilla format.	No default.
session-check-url <session-check-url_str>	Enter the URL where the packets are sent to.	No default.
session-check-str <session-check-url_str>	Enter the string in the response message. If the string can be checked, the authentication succeeds; otherwise, the authentication will be re-launched.	No default.
data-format <data-format_str>	Add extra parameters here for authentication as required by some websites, for example, <code>%u=%U&%p=%P&security_level=0&form-submit.</code> The default value <code>%u=%U&%p=%P</code> includes the values for Username Field and Password Field.	No default.

Related topics

- [wvs policy on page 738](#)
- [wvs schedule on page 743](#)
- [wvs template on page 745](#)

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 details, see [Permissions on page 46](#).

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>"	Enter the name of new or existing WVS schedule. The maximum length is 63 characters. To display the list of existing schedule, enter: 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>" on page 744. - recurring—Run the scan periodically, on a schedule. Also configure time "<time_str>" on page 744 and wday {Sunday Monday Tuesday Wednesday Thursday Friday Saturday} on page 744.	onetime
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 The yyyy range is 2001–2050. This only applies if type {recurring onetime} on page 744 is onetime.	No default.
time "<time_str>"	Enter 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 {recurring onetime} on page 744 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 {recurring onetime} on page 744 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

- [wvs profile on page 740](#)
- [wvs policy on page 738](#)

wvs template

Use this command to pre-define the scan profile.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `wvsgroup` area. For details, see [Permissions on page 46](#).

Syntax

```
config wvs template
  edit "<wvs_template_name>"
    set audit {BLIND_SQLI | BUFFER_OVERFLOW | CORS_ORIGIN...}
    set bruteforce {BASIC_AUTH | FORM_AUTH}
    set crawl {ARCHIVE_DOT_ORG | BING_SPIDER | CONTENT_NEGOTIATION...}
    set grep {ANALYZE_COOKIES | BLANK_BODY | CACHE_CONTROL...}
    set infrastructure {AFD | ALLOWED_METHODS | DETECT_REVERSE_PROXY...}
  end
```

Variable	Description	Default
"<wvs_template_name>"	Enter a name for the scan template.	No default.

Variable	Description	Default
audit {BLIND_SQLI BUFFER_OVERFLOW CORS_ORIGIN...}	Configure the plugins for a scan template.	No default.
bruteforce {BASIC_AUTH FORM_AUTH}		
crawl {ARCHIVE_DOT_ ORG BING_SPIDER CONTENT_ NEGOTIATION...}		
grep {ANALYZE_COOKIES BLANK_BODY CACHE_ CONTROL...}		
infrastructure {AFD ALLOWED_METHODS DETECT_REVERSE_ PROXY...}		

Example

This example shows how to configure a wvs template.

```
config wvs template1
  edit template1
    set audit BLIND_SQLI
    set bruteforce BASIC_AUTH
    set crawl CONTENT_NEGOTIATION
    set infrastructure AFD
    set grep CACHE_CONTROL
  end
```

Related topics

- [wvs policy on page 738](#)
- [wvs schedule on page 743](#)
- [wvs profile on page 740](#)

diagnose

The `diagnose` commands display diagnostic information that help you troubleshoot problems. These commands do not have an equivalent in the web UI.

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:

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}]
```

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"
```

If necessary start debugging specific to the module, such as:

```
debug flow trace start
```

Enable debug logs overall. To do this, enter:

```
debug enable
```

View the debug logs. For convenience, debugging logs are immediately outputted to your local console display or terminal emulator, but debug log files can also be uploaded to a server.

To do this, use the command:

```
debug upload
```

For more complex issues or bugs, this may be required in order to send debug information to Fortinet Customer Service & Support (<https://support.fortinet.com>).



Debug logs will be generated only if the application is running. To verify this, use [system top on page 813](#). Otherwise, use [debug crashlog on page 754](#) instead.

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

- [debug application](#)
- [log](#)

debug application

Use this command to view and set the verbosity level of debug logs for each module.

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. For details, see [Permissions on page 46](#).

Syntax

```
diagnose debug application <module_name> <verbosity-level_int>
```

Variable	Description	Default
<module_name>	The name of the module that you want to set the debug log verbosity level for. Enter <code>diagnose debug application ?</code> to display all the available module names if you don't know the exact name of the module.	no default
<verbosity-level_int>	Specify the verbosity level to output to the CLI display after the command executes. The valid range is 0–7, where 0 disables debug logs for the module and 7 generates the most verbose logging. If you omit the number, the CLI displays the current verbosity level. For example: <pre>autosync debug level is 0</pre>	0

Related topics

- [debug on page 747](#)
- [debug console timestamp on page 752](#)
- [debug info on page 763](#)
- [debug reset on page 769](#)
- [debug upload on page 772](#)

debug asan

Use this command to collect memory violation events.

To use this command, your administrator account's access control profile requires `r` permission to the `mntgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose debug asan <program> {enable | disable}
```

Variable	Description	Default
<program>	Enter the name of program for which you want to collect the memory violation events.	no default

Variable	Description	Default
{enable disable}	You can run <code>diagnose debug asan show</code> to check all the programs that support ASAN and their corresponding enable/disable state. enable When enabled, the system will perform the following actions (using proxyd as an example): 1. Backup "/bin/proxyd" to "/bin/proxyd.bak" 2. Create symbolic link between "/bin/proxyd" and "/var/log/debug/symbol/asan/bin/proxyd" 3. Kill proxyd This causes the proxyd daemon to respawn with the ASAN version. You leave the system in its state and let the ASAN version of proxyd daemon run and collect memory violation events. For more info on troubleshooting the memory violation issues, see Diagnose memory violation issues. Please note the changes above is not persistent across reboot. If the system is reloaded, the normal version of daemon will be running. disable Once the data is collected, you use <code>disable</code> to revert back to the normal daemon. The system will perform the following actions (using proxyd as an example): 1. Rename "/bin/proxyd.bak" to "/bin/proxyd" 2. Kill proxyd This causes the daemon to respawn with the original executable. Please note that respawning will cause traffic interruption.	disable

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 [debug on page 747](#).

To use this command, your administrator account's access control profile requires only `r` permission in any profile area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose debug cli <cli_int>
```

Variable	Description	Default
cli <cli_int>	Specify the verbosity level to output to the CLI display after the command executes. The valid range is 0–7, 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: <pre>cli debug level is 0</pre>	3

Related topics

- [debug on page 747](#)
- [debug console timestamp on page 752](#)
- [debug info on page 763](#)
- [debug reset on page 769](#)
- [debug upload on page 772](#)

debug cmdb

Use this command to enable the debug log for the configuration management database (CMDDB).

Before you will be able to see any debug logs, you must first enable debug log output using the command [debug on page 747](#).

To use this command, your administrator account's access control profile requires only `r` permission in any profile area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose debug cmdb <cmdb_int>
```

Variable	Description	Default
cmdb <cmdb_int>	Specify the verbosity level to output to the CLI display after the command executes. The valid range is 0–7, where 0 disables SNMP debugging and 7 generates the most verbose logging. If you omit the number, the CLI displays the current verbosity level: <pre>cmdb debug level is 0</pre>	0

Related topics

- [debug on page 747](#)
- [debug console timestamp on page 752](#)
- [debug info on page 763](#)
- [debug reset on page 769](#)
- [debug upload on page 772](#)

debug comlog

Use this command for the comlog related operations.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose debug comlog {info|read|clear|disable|enable}
```

Variable	Description	Default
{info read clear disable enable}	Enable: Enable to record COMlog. Disable: Disable the recording of the COMlog. info: View the COMlog status including status (enable or disable), log space, and log size. read: Record the console log to /var/log/gui_upload/console.log. You can download the console.log from System > Maintainece > Backup&Restore > GUI File Download . dump: print the console log to command line interface(CLI). clear: Dump the console log.	Enable

It also can be enabled or disabled by this command:

```
config system global
  set console-log {disable|enable}
end
```

debug console timestamp

Use this command to enable or disable the timestamp in debug logs.

Before you will be able to see any debug logs, you must first enable debug log output using the command [debug on page 747](#).

To use this command, your administrator account's access control profile requires only `r` permission in any profile area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose debug console timestamp {enable | disable}
```

Variable	Description	Default
timestamp {enable disable}	Enable to add timestamps to debug output. If you omit the selection, the CLI displays the current timestamp status: <code>console timestamp is disabled.</code>	disable

Related topics

- [debug reset on page 769](#)
- [debug info on page 763](#)

debug coredumplog

Use this command to record the stack information in the core file of the proxyd program.

Before you will be able to see any debug logs, you must first enable debug log output using the command [enable-debug-log {enable | disable} on page 374](#).

To use this command, your administrator account's access control profile requires only `r` permission in any profile area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose debug coredumplog show  
diagnose debug coredumplog clear
```

Related Topic

- [debug on page 747](#)

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.

Before you will be able to see any debug logs, you must first enable debug log output using the command [enable-debug-log {enable | disable} on page 374](#).

To use this command, your administrator account's access control profile requires only `r` permission in any profile area. For details, see [Permissions on page 46](#).

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 daemonlog

Use this command to process call information on specific interface records.

Before you will be able to see any debug logs, you must first enable debug log output using the command [enable-debug-log {enable | disable} on page 374](#).

To use this command, your administrator account's access control profile requires only `r` permission in any profile area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose debug daemonlog show
diagnose debug daemonlog clear
```

Related Topic

- [debug on page 747](#)

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. The update time and update interval information will also be listed in the output.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose debug dnsproxy list
```

Example

If the domain specified for the server pool member is `www.example.org` and has resolved to `123.126.104.68`, output similar to the following is displayed:

```
diagnose debug dnsproxy list
Domain Name: www.example.org
IPv4 Last Update:2019-08-12 01:23:58
IPv4 Update Interval (TTL):109 seconds
Domain IPv4 Addresses:123.126.104.68
IPv6 Last Update:2019-08-12 01:23:30
IPv6 Update Interval(TTL):119 seconds
Domain IPv6 Addresses:2408:80f0:4100:4007::4 2408:80f0:4100:4007::5
```

Related topics

- [system dns on page 279](#)

debug emerglog

Use this command to view or erase disk read-only error logs.

Before you will be able to see any debug logs, you must first enable debug log output using the command [debug on page 747](#).

To use this command, your administrator account's access control profile requires only `r` permission in any profile area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose debug emerglog {show | clear}
```

Variable	Description	Default
{show clear}	Enter <code>show</code> to view disk read-only error logs. Enter <code>clear</code> 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.

Before you will be able to see any debug logs, you must first enable debug log output using the command [debug on page 747](#).

To use this command, your administrator account's access control profile requires only `r` permission in any profile area. For details, see [Permissions on page 46](#).

Syntax

To show the details of traffic flows (including HTTP, FTP, etc.), run the following commands. You can use `client-ip`, `server-ip`, and `policy` as the filter conditions (these filter conditions are in "AND" relation).

```
diagnose debug enable
diagnose debug flow trace start
diagnose debug flow filter flow-detail debug flow filter
diagnose debug flow filter client-ip debug flow filter
diagnose debug flow filter server-ip debug flow filter
diagnose debug flow filter policy <policy_name>
diagnose debug flow trace stop
```

To show the details of the traffic flows passing through certain modules, run the following commands. You can use `client-ip`, `server-ip`, and `policy` as the filter conditions (these filter conditions are in "AND" relation).

```
diagnose debug enable
diagnose debug flow trace start
diagnose debug flow filter module-detail {x-forwarded-for | ip-list | ip-reputation |
    quarant-ip | known-engine | geo-block | ... | url-rewriting} <verbosity-level_int>
diagnose debug flow filter client-ip debug flow filter
diagnose debug flow filter server-ip debug flow filter
diagnose debug flow filter policy <policy_name>
diagnose debug flow trace stop
```

To show the details of the HTTP traffic flows, run the following commands. You can use `client-ip`, `server-ip`, and `policy` as the filter conditions (these filter conditions are in "AND" relation).

```
diagnose debug enable
diagnose debug flow trace start
diagnose debug flow filter http-detail debug flow filter
diagnose debug flow filter client-ip debug flow filter
diagnose debug flow filter server-ip debug flow filter
diagnose debug flow filter policy <policy_name>
diagnose debug flow trace stop
```

Variable	Description	Default
{x-forwarded-for ip-list ip-reputation quarant-ip known-engine geo-block ... url-rewriting} <verbosity-level_int>	Select the name of module that needs to be traced (separated by space). Enter <code>diagnose debug flow filter module-detail ?</code> to display all the available module names if you don't know the exact name of the module.	No default.
<verbosity-level_int>	Specify the verbosity level to output to the CLI display after the command executes. The valid range is 0–7, where 0 disables debug logs and 7 generates the most verbose logging. If you omit the number, the CLI displays the current verbosity level. The default verbosity-level value for <code>flow-detail</code> is 1. For <code>http-detail</code> and <code>module-detail</code> , the default value is 0, which means "disabled".	0 or 1
<source_ipv4 source_ipv6>	Enter 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.
<destination_ipv4 destination_ipv6>	Enter 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)	No default.

Variable	Description	Default
	This will generate only packet flow debug log messages involving that server IP address.	
<policy_name>	Enter the name of the server policy to filter out the connections that match the Network Configuration in the policy.	No default.

Related topics

- [debug flow trace on page 759](#)

debug flow filter module-bypass-info

If a certain security module doesn't block the request as expected, it might be due to the request being allowed by a precedent module, causing it to skip all the following modules. To check which modules might have such an effect, allowing a request to pass before reaching the current one, you can use this command.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose debug flow filter module-bypass-info <module name>
```

Below is an example of the command and its printout:

```
FortiWeb # dia deb flow filter module-bypass-info IP-Reputation
<Enter>

Note:
The reference information below details which modules may be bypassed by IP-Reputation and which modules may bypass IP-Reputation.
[Bypasses Modules]:
--> IP-Reputation

[Bypassed By]:
--> Global-Allow-List
--> IP-List
--> IP-Reputation
```

Related topics

- [debug info](#)
- [debug console timestamp](#)
- [debug application](#)
- [debug cli](#)

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. For details, see [Permissions on page 46](#).

Syntax

```
diagnose debug flow reset
```

Related topics

- [debug flow filter on page 756](#)
- ["debug flow filter module-detail" on page 1](#)

debug flow trace

Use this command to trace the flow of packets through the FortiWeb appliance's processing modules and network stack.

Before you will be able to see any debug logs, you must first enable debug log output using the command [debug on page 747](#).

To use this command, your administrator account's access control profile requires only `r` permission in any profile area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose debug flow trace {start | stop}
```

Variable	Description	Default
trace {start stop}	Select whether to enable (<code>start</code>) or disable (<code>stop</code>) the recording of packet flow trace debug log messages.	No default.

Example

This example configures a filter based on the packet destination IP `192.0.2.48`, 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 192.0.2.48
```

```
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_ALLOW_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_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_ALLOW_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_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
192.0.2.48:47368"
session_id=1 packet_id=0 policy_name=policy1 msg="Receive packet from client
192.0.2.48:59682"
session_id=252 packet_id=0 policy_name=policy1 msg="Receive packet from client
192.0.2.48:47376"
session_id=503 packet_id=0 policy_name=policy1 msg="Receive packet from client
192.0.2.48:59687"
session_id=754 packet_id=0 policy_name=policy1 msg="Receive packet from client
192.0.2.48:47382"
session_id=2 packet_id=0 policy_name=policy1 msg="Receive packet from client
192.0.2.48:47385"
session_id=253 packet_id=0 policy_name=policy1 msg="Receive packet from client
192.0.2.48:47387"
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 192.0.2.225:49428)
- 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. For details, see [noparse {enable | disable} on page 164](#).

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*:

<https://docs.fortinet.com/document/fortiweb>

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 allowlisted, and therefore the module is being skipped.
- `Execution:4`—URL access policy has caused the module to be skipped.

Related topics

- [server-policy policy on page 150](#)
- [server-policy server-pool on page 182](#)
- [server-policy custom-application application-policy on page 1](#)
- [waf url-access url-access-rule on page 669](#)
- [policy on page 797](#)
- [debug flow filter on page 756](#)
- ["debug flow filter module-detail" on page 1](#)
- [debug on page 747](#)

debug ha

Use this command debug HA related issues.

Syntax

```
diagnose debug ha
```

- `all {enable | disable}`
Enable to track all debugs.
- `arp {enable | disable}`
Enable to track HA ARP.
- `basic {enable | disable}`
Enable to debug basic issues. The output including configuration, upgrade, file, and messages.
- `cloud {enable | disable}`
Enable to debug for public cloud platform HA AP switching.
- `configuration {enable | disable}`
Enable to track HA configuration synchronization.
- `errors {enable | disable}`
Enable to track HA errors during synchronization.
- `file {enable | disable}`
Enable to track any file in HA synchronization.
- `heartbeat {enable | disable}`
Enable to track HA heartbeat packets.
- `list`
List all debug settings.

- `message {enable | disable}`
Enable to track HA sync messages, such as GEODB/Licenses.
- `state {enable | disable}`
Enable to track HA state changes and monitor ports state changes.
- `udp-tunnel {enable | disable}`
Enable to track HA unicast.
- `upgrade {enable | disable}`
Enable to track firmware upgrade.
- `write-to-debugfile {enable | disable}`
Enable to write HA console debug output to file.

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. For details, see [Permissions on page 46](#).

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

- [debug reset](#)
- [debug](#)
- [debug application](#)
- [debug console timestamp](#)
- [debug cli](#)

debug init

Use this command to record packet flow trace log messages.

Before you will be able to see any debug logs, you must first enable debug log output using the command [debug](#) on page 747.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area. For details, see [Permissions](#) on page 46.

Syntax

```
diagnose debug init {enable | disable}
```

Variable	Description	Default
init {enable disable}	Select whether to enable (<code>start</code>) or disable (<code>stop</code>) the recording of packet flow trace debug log messages. If you omit the selection, the CLI displays the current timestamp status: <code>init output: disabled</code>	No default.

debug jemalloc-heap

If the jemalloc profile is activated and the memory usage exceeds the configured threshold, the heap file will be generated in directory `/var/log/gui_upload`.

You can use this command to show or clear the heap files. At most 10 heap files are kept on device.

Syntax

```
diagnose debug jemalloc-heap {show | clear}
```

Related commands

To activate or deactivate jemalloc profile:

```
diagnose system kill 43 <pid_of_proxyd>
```

To parse the heap file via jeprof tool:

```
diagnose system jeprof
```

diagnose debug jemalloc proxyd

The `diagnose debug jemalloc proxyd` command provides debugging tools for analyzing memory allocation and detecting potential leaks in proxyd. It offers options for generating memory dump files, inspecting object pools, and identifying long-lived objects that may indicate memory retention issues.

Specifically, the `diagnose debug jemalloc proxyd pdump-leaks` command dumps objects that have existed for a specified duration, helping to identify potential memory leaks by listing persistent objects in proxyd's object pools. Each object pool allocates fixed-size memory chunks for tasks such as packet handling, session tracking, and connection management. By monitoring object lifespan, FortiWeb detects abnormal memory retention that may indicate a leak.

To maintain efficiency and prevent excessive output, the command limits the number of dumped entries to 100 per object pool per working thread.

Syntax

```
diagnose debug jemalloc proxyd dump
diagnose debug jemalloc proxyd pdump
diagnose debug jemalloc proxyd pdump-leaks <minutes>
```

dump	Generates a memory dump file for proxyd using the jemalloc allocator.
pdump	Dumps object pool details, including active allocations.
pdump-leaks <minutes>	Identifies and logs object pool entries that have persisted beyond the expected lifespan, aiding in memory leak detection. If <minutes> is not provided, the default is 30 minutes.

Examples

```
/var/log/gui_upload# cat proxyd-objpool-3488-1732325050.txt
                                objpool name:                total  incsize  objsize  nodesize  lock
nallocated      nfreed
      worker_run-1-packet_t:      4136000      500      4096      4136      no
1000      963
Total age > 2 min: 37
```

```

        worker_run-1-session_t:          188000      500      336      376      no
500          499
session age 3 min, policy server_policy1
Total age > 2 min: 1
        worker_run-1-pt_stream_t:        280000      500      520      560      no
500          498
stream age 3 min, dir 1, policy server_policy1
stream age 3 min, dir 0, policy server_policy1
Total age > 2 min: 2
        worker_run-0-packet_t:           2068000     500      4096     4136      no
500          500
Total age > 2 min: 0
        worker_run-0-session_t:          188000      500      336      376      no
500          500
Total age > 2 min: 0
        worker_run-1-connection_t:       536000     1000      496      536      no
1000         998
connection age 3 min, (192.168.2.1:14162->192.168.2.2:80)
connection age 3 min, (10.159.28.221:56012->10.159.28.226:443)
Total age > 2 min: 2
        worker_run-0-pt_stream_t:        280000      500      520      560      no
500          500
Total age > 2 min: 0
        worker_run-1-pt_service_t:       948000      500     1856     1896      no
500          498
service age 3, type 0, policy server_policy1
service age 3, type 0, policy server_policy1
Total age > 2 min: 2
        worker_run-1-pt_substream:       320000      500      600      640      no
500          498
substream 321e0528 age 3 min, status 0, peer 321e07a8, policy server_policy1
substream 321e07a8 age 3 min, status 0, peer 321e0528, policy server_policy1
Total age > 2 min: 2
        worker_run-0-connection_t:       536000     1000      496      536      no
1000         1000
Total age > 2 min: 0
        worker_run-0-pt_service_t:       948000      500     1856     1896      no
500          500
Total age > 2 min: 0
        worker_run-0-pt_substream:       320000      500      600      640      no
500          500
Total age > 2 min: 0

```

debug netstatlog

Use this command to record the print information of the `netstat -anlt` when the proxyd program is overloaded.

Before you will be able to see any debug logs, you must first enable debug log output using the command [enable-debug-log {enable | disable} on page 374](#).

To use this command, your administrator account's access control profile requires only `r` permission in any profile area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose debug netstatlog show
diagnose debug netstatlog clear
```

Related Topic

- [debug on page 747](#)

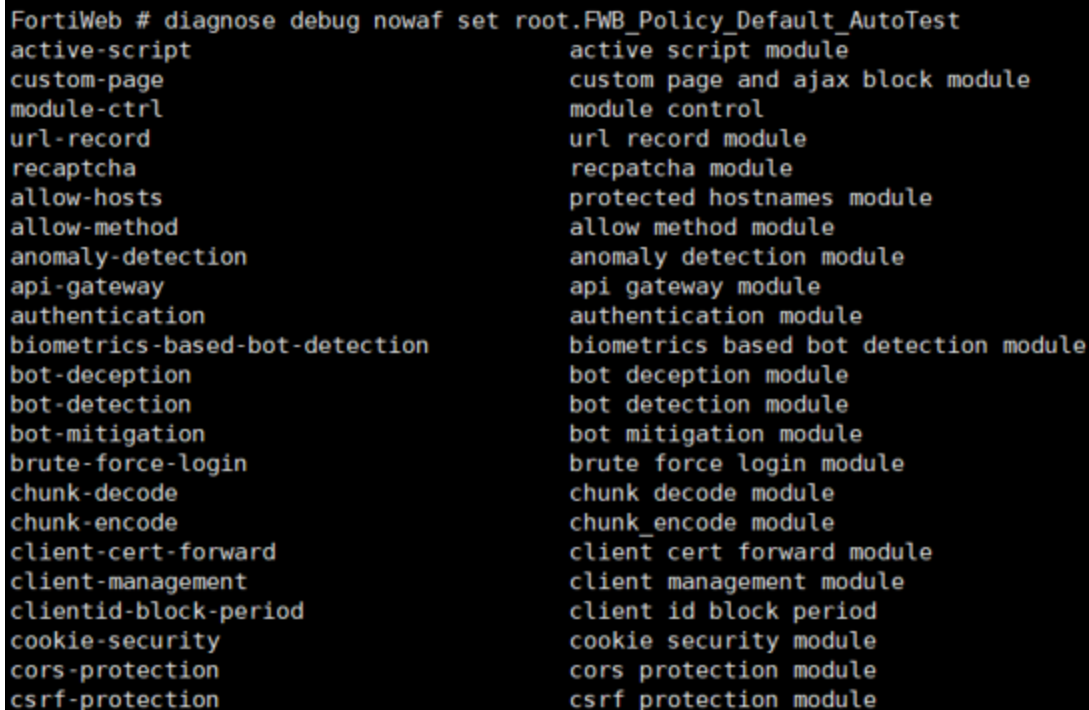
debug nowaf

Use this command to disable all or some of security modules in a policy to narrow down the root cause.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose debug nowaf enable
diagnose debug nowaf set <adom name>.< policy name> <module name1> <module name2> ... <module nameN>
```



```
FortiWeb # diagnose debug nowaf set root.FWB_Policy_Default_AutoTest
active-script          active script module
custom-page           custom page and ajax block module
module-ctrl           module control
url-record            url record module
recaptcha             recaptcha module
allow-hosts           protected hostnames module
allow-method          allow method module
anomaly-detection     anomaly detection module
api-gateway           api gateway module
authentication        authentication module
biometrics-based-bot-detection biometrics based bot detection module
bot-deception         bot deception module
bot-detection         bot detection module
bot-mitigation        bot mitigation module
brute-force-login     brute force login module
chunk-decode          chunk decode module
chunk-encode          chunk_encode module
client-cert-forward   client cert forward module
client-management     client management module
clientid-block-period client id block period
cookie-security       cookie security module
cors-protection       cors protection module
csrf-protection       csrf protection module
```

Related topics

- [debug info](#)
- [debug console timestamp](#)
- [debug application](#)
- [debug cli](#)

debug pkcs11providerlog

Use this command to view debug logs for PKCS#11 provider operations, including key access and cryptographic function calls.

Syntax

```
diagnose debug pkcs11providerlog show
diagnose debug pkcs11providerlog clear
```

Variable	Description	Default
show	Displays debug logs for PKCS#11 provider operations, including key access and cryptographic function calls.	No default.
clear	Clears the debug logs for PKCS#11 provider operations, including key access and cryptographic function calls.	No default.

Related topics:

- [system nethsm on page 353](#)
- [debug primuslog on page 769](#)

debug proxy log

Use this command to print the logs generated by proxyd.

Syntax

```
diagnose debug proxy log {1 | 2 | 3}
```

1: Print error messages.

2: Print error messages and warnings.

3: Print error messages, warnings, and other logs.

Related Topic

- [debug on page 747](#)

debug primuslog

Use this command to view debug logs related to the Primus HSM integration.

Syntax

```
diagnose debug primuslog show
diagnose debug primuslog clear
```

Variable	Description	Default
show	Displays debug logs related to the Primus HSM integration.	No default.
clear	Clears the debug logs related to the Primus HSM integration.	No default.

Related topics:

- [system nethsm on page 353](#)
- [debug pkcs11providerlog on page 768](#)

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. For details, see [Permissions on page 46](#).

Syntax

```
diagnose debug reset
```

Related topics

- [debug info](#)
- [debug console timestamp](#)
- [debug application](#)
- [debug cli](#)

debug shell-access history show

Use this command to show the history of commands executed in Shell.

To use this command, your administrator account's access control profile must have `rw` or `w` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose debug shell-access history show
```

Please note that to view the history you must have enabled shell-access in `config system global`.

Run the following commands to enable shell access and specify trusted hosts.

```
config system global
    set shell-access enable
    set shell-history-size <int>
    set shell-trusthostv4 <IPv4_address_range>
    set shell-trusthostv6 <IPv6_address_range>
end
```

For more information, see [config system global](#).

debug trace report

Use this command to start or stop collecting debug logs.

Only administrators or users with the `prof_admin` access file have permission to this command.

Syntax

```
diagnose trace report {start | stop} on page 771
```

Variable	Description	Default
trace report {start stop}	Select whether to enable (<code>start</code>) or disable (<code>stop</code>) collecting debug logs.	No default

Related topics

- [debug on page 747](#)

debug trace tcpdump

Use this demand to trace packets with tcpdump.

Syntax

```
diagnose trace tcpdump "<filter_str>" {any | "<interface_str>"} "<max-packet-count_int>"  
{reset}
```

Variable	Description	Default
"<filter_str>"	Specify which protocols and port numbers that you do or do not want to capture, such as 'tcp and port 80 and host IP1 and (IP2 or IP3) ', or leave this field blank for no filters. Note that please use the same filter expression as <code>tcpdump</code> for this filter, you can refer to the Linux main page of TCPDUMP (http://www.tcpdump.org/manpages/tcpdump.1.html).	No default
{any "<interface_str>"}	Select the network interface on which you want to capture packets, such as <code>port1</code> , or <code>any</code> for all interfaces.	<code>any</code>
"<max-packet-count_int>"	Specify the maximum packets you want to capture for the policy. Capture will stop automatically if the total captured packets hit the count.	4000
{reset}	Reset all the settings to default.	No default

Related topics

- [debug on page 747](#)

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 Customer Service & Support:

<https://support.fortinet.com>

To use this command, your administrator account's access control profile requires only `r` permission in any profile area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose debug upload <ftp_ipv4> <user_str> <password_str> <upload-dir_str>
```

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 192.0.2.5 user1 1passw0Rd C:/uploads
```

Related topics

- [debug on page 747](#)
- [db rebuild on page 829](#)

ha synchronize health-check

For FortiWeb appliances in Active-Passive and Active-Active-Standard modes, use this command to immediately synchronize the back-end servers' health check status from the primary to the secondary FortiWeb nodes. This ensures that when an HA fail-over occurs, the new primary FortiWeb appliance can immediately know the health status of the back-end servers, ensuring seamless traffic continuity during fail-over.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
execute ha synchronize health-check
```

Please note that by default the health check status is synchronized when there are changes in the back-end server health check status. Use this command only when you want to synchronize health check status immediately.

hardware bypass info

Use this command to display bypass firmware version information.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Please note this command is only supported on FortiWeb 2000F, 3000F and 4000F.

Syntax

```
diagnose hardware bypass info
```

hardware check

Use this command to check the appliance hardware for errors. In the case of FortiWeb, 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 | psu | sslcard | cpu | logdisk | memory | nic}
```

Variable	Description	Default
{all psu sslcard cpu logdisk memory nic}	Enter the type of hardware to check, or enter <code>all</code> to check all hardware. For FortiWeb-VM versions, the <code>sslcard</code> option is not available. Note:	No default.

Variable	Description	Default
	• <code>sslcard</code> is only supported on FortiWeb 600D, 1000D, 3000D, 3000DFSX, 4000D, 1000E, 2000E, 3000E, 3010E, 4000E, 2000F, 3000F, and 4000F. • <code>psu</code> is only supported on FortiWeb2000E, 3000E, 3010E, 4000E, 2000F, 3000F and 4000F.	

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 cpld info

Use this command to display the cpld firmware version information.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Please note this command is only supported on FortiWeb 2000F, 3000F and 4000F.

Syntax

```
diagnose hardware cpld info
```

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 details, see [Permissions on page 46](#).

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

- [system top on page 813](#)
- [hardware mem on page 778](#)
- [system performance on page 863](#)

hardware fail-open

Fail-to-wire/bypass behavior is available for specific models only. For details, see [system fail-open on page 286](#).

hardware hddisk

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 details, see [Permissions on page 46](#).

Syntax

```
diagnose hardware hddisk [list]
```

Example

```
diagnose hardware hddisk 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

- [hardware logdisk info on page 777](#)
- [hardware raid list on page 782](#)
- [system flash on page 799](#)
- [system mount on page 813](#)
- [system performance on page 863](#)

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 details, see [Permissions on page 46](#).

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

- [system performance on page 863](#)

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 details, see [Permissions on page 46](#).

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

- [hardware harddisk on page 775](#)
- [log on page 784](#)
- [system mount on page 813](#)
- [system performance on page 863](#)

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 details, see [Permissions on page 46](#).

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

- [policy on page 797](#)
- [system flash on page 799](#)
- [system top on page 813](#)
- [system performance on page 863](#)

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 details, see [Permissions on page 46](#).

Syntax

```
diagnose hardware nic list [<interface_name>]
```

Variable	Description	Default
list [<interface_name>]	Optionally, enter the name of a physical network interface, such as <code>port1</code>, 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 (<code>lo</code>): <pre>lo port1 port2 port3 port4</pre> 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 on page 345 to configure <code>port1</code> with <code>set status down</code>, if the cable is physically plugged in, <code>diagnose hardware nic list port1</code> will indicate correctly that the link is up (<code>Link detected: yes</code>).	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 queue len 1000
RX bytes 72772373 (69.4 Mb)
TX bytes 32288070 (30.7 Mb)
```

Related topics

- [system interface on page 344](#)
- [hardware interrupts on page 776](#)
- [network ip on page 786](#)
- [network sniffer on page 790](#)
- [network tcp list on page 795](#)
- [network udp list on page 796](#)
- [system ha mac on page 806](#)
- [traceroute on page 857](#)
- [system performance on page 863](#)

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 details, see [Permissions on page 46](#).

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

- [system raid on page 364](#)
- [hardware harddisk on page 775](#)
- [system mount on page 813](#)
- [create-raid level on page 826](#)
- [create-raid rebuild on page 827](#)
- [system performance on page 863](#)

hardware raid-card info

Use this command to display raid-card firmware version information.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Please note this command is only supported on FortiWeb 2000F, 3000F and 4000F.

Syntax

```
diagnose hardware raid-card info
```

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 details, see [Permissions on page 46](#).

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>	Enter the number of most recent logs to display.	No default.
set <queue_int>	Enter the maximum length of the log before it is flushed and written to disk. The valid range is 0–32,768.	No default.

Example

This example displays a list of logs processed.

```
diagnose index all show
```

Related topics

- [log attack-log on page 61](#)
- [log event-log on page 71](#)
- [log traffic-log on page 95](#)
- [debug on page 747](#)
- [hardware logdisk info on page 777](#)

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 details, see [Permissions on page 46](#).

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: <code>all</code>—All logs <code>alog</code>—Attack logs <code>dlog</code>—Debug logs <code>elog</code>—Event logs <code>tlog</code>—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

- [log attack-log on page 61](#)
- [log event-log on page 71](#)
- [log traffic-log on page 95](#)
- [debug on page 747](#)
- [hardware logdisk info on page 777](#)

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 details, see "Permissions" on page 1.

Syntax

```
diagnose network arp add <interface_name> {<interface_ipv4> | interface_ipv6} <mac-address_hex>
diagnose network arp delete <interface_name> {<interface_ipv4> | interface_ipv6}
diagnose network arp list
diagnose network arp flush
```

Variable	Description	Default
<interface_name>	Enter the name of the interface to add or delete from the ARP table.	No default.
{<interface_ipv4> interface_ipv6}	Enter the IP address of the interface.	No default.
<mac-address_hex>	Enter the MAC address of the interface.	No default.

Example

This example displays a list of ARP table entries.

```
FortiWeb # diagnose network arp list
port_ha: 169.254.0.2 fc:aa:14:75:c0:e0 reachable
port1: 10.0.0.1 00:09:0f:77:11:1d stale
port2: 10.65.13.3 00:0c:29:02:f1:bb reachable
lo: 10::13:101 0: 0: 0: 0: 0: 0 noarp
port2: ff02::16 33:33: 0: 0: 0:16 noarp
vlan66: ff02::16 33:33: 0: 0: 0:16 noarp
port7: ff02::2 33:33: 0: 0: 0: 2 noarp
port_ha: ff02::2 33:33: 0: 0: 0: 2 noarp
port_tn: ff02::16 33:33: 0: 0: 0:16 noarp
port7: ff02::16 33:33: 0: 0: 0:16 noarp
port_ha: ff02::16 33:33: 0: 0: 0:16 noarp
gretap0: ff02::16 33:33: 0: 0: 0:16 noarp
```

Related topics

- [network route on page 787](#)
- [network ip on page 786](#)
- [router static on page 101](#)
- [system interface on page 344](#)

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. 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 details, see [Permissions on page 46](#).

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>	Enter the name of the interface to add or delete from the network interface table.	No default.
{<interface_ipv4> interface_ipv6}	Enter the IP address of the network interface.	No default.
{<interface_ipv4mask> <interface_v6mask>}	Enter the subnet mask.	No default.

Example

This example displays a list of enabled network interfaces, including the loopback (`lo`).

```
FortiWeb # diagnose network ip list  
lo: 127.0.0.1/24  
port1: 10.200.123.2/16  
lo: ::1/128  
port1: fe80::20c:29ff:fec3:34a6/64
```

```
port5: fe80::20c:29ff:fec3:34ce/64
port9: fe80::20c:29ff:fec3:34f6/64
port2: fe80::20c:29ff:fec3:34b0/64
port6: fe80::20c:29ff:fec3:34d8/64
port10: fe80::20c:29ff:fec3:3400/64
port3: fe80::20c:29ff:fec3:34ba/64
port7: fe80::20c:29ff:fec3:34e2/64
port4: fe80::20c:29ff:fec3:34c4/64
port8: fe80::20c:29ff:fec3:34ec/64
port_tn: fe80::1854:64ff:fe68:fd55/64
```

Example

This example deletes the IP of a virtual server on port2.

```
diagnose network ip delete port1 192.0.2.221
```

Related topics

- [network route on page 787](#)
- [network arp on page 785](#)
- [system interface on page 344](#)

network route

Use this command to add or delete a route in the routing table, or to list the routing table.

This command displays **all** individual entries, including automatically configured routes for the loopback interface and VLANs, and also displays each route's priority. Unlike [network rtcache on page 789](#), 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 details, see [Permissions on page 46](#).

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>
diagnose network route list
```

Variable	Description	Default
{<source_ipv4mask> <source_ipv6mask>}	Enter the IP address and network mask of the source, separated by a space.	No default.
<interface_name>	Enter the name of the interface to add or delete from the routing table.	No default.
{<destination_ipv4mask> <destination_ipv6mask>}	Enter the IP address and network mask of the source, separated by a space.	No 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 valid range is 1–256.	0

Example

This example displays the routing table.

```
FortiWeb # diagnose network route list
0.0.0.0/0(none)->10.200.0.0/16(port1) via 0.0.0.0, pri 0 prot 2 scope 253
::/0(none)->fe80::/64(port1) via ::, pri 256 prot 2 scope 0
::/0(none)->fe80::/64(port2) via ::, pri 256 prot 2 scope 0
::/0(none)->fe80::/64(port3) via ::, pri 256 prot 2 scope 0
::/0(none)->fe80::/64(port4) via ::, pri 256 prot 2 scope 0
::/0(none)->fe80::/64(port5) via ::, pri 256 prot 2 scope 0
::/0(none)->fe80::/64(port6) via ::, pri 256 prot 2 scope 0
::/0(none)->fe80::/64(port7) via ::, pri 256 prot 2 scope 0
::/0(none)->fe80::/64(port8) via ::, pri 256 prot 2 scope 0
::/0(none)->fe80::/64(port9) via ::, pri 256 prot 2 scope 0
::/0(none)->fe80::/64(port10) via ::, pri 256 prot 2 scope 0
::/0(none)->fe80::/64(port_tn) via ::, pri 256 prot 2 scope 0
```

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

- [router all on page 1](#)
- [ping on page 838](#)
- [ping6 on page 839](#)
- [traceroute on page 857](#)
- [network rtcache on page 789](#)
- [router static on page 101](#)

network rtcache

Use this command to display the routing cache.

Unlike [network route on page 787](#), 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 [network route on page 787](#), 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 details, see [Permissions on page 46](#).

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

- [router all on page 1](#)
- [ping on page 838](#)
- [ping6 on page 839](#)
- [traceroute on page 857](#)
- [network route on page 787](#)
- [router static on page 101](#)

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 `prof_admin` area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose network sniffer [{any | "<interface_name>"} [{none | "<filter_str>"} [{1 | 2 | 3} [<packets_int>]]]
```

Variable	Description	Default
{any "<interface_name>"}	Enter the name of a network interface whose packets you want to capture, such as <code>port1</code> , or type <code>any</code> to capture packets on all network interfaces.	No default.

Variable	Description	Default
	If you omit this and the following parameters for the command, the command captures all packets on all network interfaces.	
{none "<filter_str>"}	Enter either <code>none</code> 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 <code>"tcp port 25"</code>. Filters use <code>tcpdump</code> (http://www.tcpdump.org) syntax: <pre>"[[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>]"</pre> 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: <pre>"udp and port 1812 and src host 1.example.com and dst \(2.example.com or 2.example.com \)"</pre>	none
{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 (<code>ihl</code>) - type of service/differentiated services code point (<code>tos</code>) - explicit congestion notification - total packet or fragment length - packet ID - IP header checksum - time to live (<code>TTL</code>) - fragment offset - options bits 2—All of the output from 1, plus the packet payload in both hexadecimal and ASCII.	1

Variable	Description	Default
	3—All of the output from 2, plus the link layer (Ethernet) header. For troubleshooting purposes, Fortinet Technical Support may request the most verbose level (3).	
<packets_int>	Enter 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 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 (<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>)
- A plain text editor such as Notepad
- A Perl interpreter
- Network protocol analyzer software such as Wireshark (<http://www.wireshark.org/>)

To view packet capture output using PuTTY and Wireshark

On your management computer, start PuTTY.

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 33](#).

Type the packet capture command, such as:

```
diag network sniffer packet port1 'tcp port 443' 3 100
```

but do **not** press Enter yet.

In the upper left corner of the window, click the PuTTY icon to open its drop-down menu, then select **Change Settings**.

In the **Category** tree on the left, go to **Session > Logging**.

Select Printable output.

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.

Click **Apply**.

Press Enter to send the CLI command to the FortiMail appliance, beginning packet capture.

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.

Close the PuTTY window.

Open the packet capture file using a plain text editor such as Notepad.

Delete the first and last lines, which look like this:

```
===== PuTTY log 8/14/2025.07.25 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.

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 recognizable by Wireshark (`.pcap`) using the `fgt2eth.pl` Perl script. To download `fgt2eth.pl`, see the Fortinet Knowledge Base article "Using the FortiOS built-in packet sniffer:"

<http://kb.fortinet.com/kb/documentLink.do?externalId=11186>

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:

```
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



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`.

Open the converted file in your network protocol analyzer application. For further instructions, see the documentation for that application.

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. `0A` 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 details, see [Permissions on page 46](#).

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

- [network arp on page 785](#)
- [network ip on page 786](#)

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 details, see [Permissions on page 46](#).

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
    ffff88003acb80 0

```

Related topics

- [network arp on page 785](#)
- [network ip on page 786](#)

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 details, see [Permissions on page 46](#).

Syntax

```
diagnose policy pserver [list "<policy_name>"]
diagnose policy session [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}
diagnose policy total-session [list "<session_number>"]
diagnose policy total-traffic http [list "<session_number>"]
diagnose policy "<policy_name>"
```

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.

Variable	Description	Default
total-session [list "<session_number>"]	Displays the total number of the current connections.	No default.
total-traffic http [list "<session_number>"]	Displays the total throughput in HTTP level. This statistics from CLI only includes HTTP payload, does not include L2 & L3 headers	No default.
"<policy_name>"	Enter 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:

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(FortiWeb_server_pool):
total = 1
server[0]
id: 1
ip: 10.20.1.22
port: 80
alive: 2
session: 0
status: 1
```

Related topics

- [server-policy policy on page 150](#)
- [network ip on page 786](#)
- [debug flow filter on page 756](#)
- [system performance on page 863](#)

system endpoint-control

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

To check client information such as IP address, MAC address, FortiClient SN, run:

```
diagnose system endpoint-control clients
```

To check EMS tags, run:

```
diagnose system endpoint-control tags
```

To check the EMS server connection status, run:

```
diagnose system endpoint-control test
```

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 details, see [Permissions on page 46](#).

Syntax

```
diagnose system flash default <partition_int>
diagnose system flash list
```

Variable	Description	Default
<partition_int>	Enter 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

- [restore image on page 849](#)
- [system status on page 864](#)

system ha backup-config

Use this command to export the configuration file of the HA nodes. It only backs up the configurations synchronized between HA nodes. The most common scenario for using this command is to compare the configuration files between the HA nodes and check which part of the configuration is not synchronized as expected.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose system ha backup-config <node-id>
```

Example

```
diagnose system ha backup-config 1
```

system ha confd_status

Use this command to display the HA information.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose system ha confd_status
```

Example

The following is an example of the output.

```
HA information
```

```
Model=FortiWeb-1000E 6.37,build1102(GA),200911, Mode=active-active-high-volume Group=2
```

```
HA group member information: is_manage_primary=1.
```

```
LocalSN: FV-1KE44179XXXXX confd
```

```
member cnt: 2
```

```
msg_queue:0 file_queue:0 md5_rep_ignore:0 do_md5sum:14030
```

```
FV-1KE4417900091: primary
```

```
pending:0 update:0 time:0 sync:0
```

```
SYS: 1C5663E93F5FEE916C06CF9F383999CB
```

```
CLI: FA6AD08C032E3DB66954E6B33D848CB3
```

```
FV-1KE4417900092: secondary
```

```
pending:2773937 update:2773937 time:2773937 sync:0
```

```
SYS: 1C5663E93F5FEE916C06CF9F383999CB
```

```
CLI: FA6AD08C032E3DB66954E6B33D848CB3
```

system ha dev-info

Use this command to display the network interface information of the HA nodes, including port name, index number, Mac addresses.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose system ha dev-info
```

Example

The following is an example of the output.

```
SN: FV-1KE44XXXXXX91
```

Name	Phyindex	Mac
port7	3	00:0b:ab:f5:3e:94
port8	4	00:0b:ab:f5:3e:95
port9	5	00:0b:ab:f5:3e:96
port10	6	00:0b:ab:f5:3e:97
port1	7	74:fe:48:20:4f:5f
port2	8	74:fe:48:20:4f:60
port3	9	74:fe:48:20:4f:61
port4	10	74:fe:48:20:4f:62
port5	11	74:fe:48:20:4f:61
port6	12	74:fe:48:20:4f:62
mgmt1	13	74:fe:48:20:4f:65
mgmt2	14	74:fe:48:20:4f:66
port11	18	00:0b:ab:f5:4f:72
port12	19	00:0b:ab:f5:4f:73

```
SN: FV-1KE44XXXXXX92
```

Name	Phyindex	Mac
port7	3	00:0b:ab:f5:3e:2c
port8	4	00:0b:ab:f5:3e:2d
port9	5	00:0b:ab:f5:3e:2e
port10	6	00:0b:ab:f5:3e:2f
port1	7	74:fe:48:20:38:8c
port2	8	74:fe:48:20:38:8d
port3	9	74:fe:48:20:38:8e
port4	10	74:fe:48:20:38:8f
port5	11	74:fe:48:20:38:8e
port6	12	74:fe:48:20:38:8f
mgmt1	13	74:fe:48:20:38:92

mgmt2	14	74:fe:48:20:38:93
port11	18	00:0b:ab:f5:50:ca
port12	19	00:0b:ab:f5:50:cb

system ha export-eventlog

Use this command to export event logs of the secondary node in the HA cluster. This command should be run on the primary node.

To download the logs, first run the following command to enable file upload:

```
config system settings
    set enable-file-upload enable
end
```

Then, go to **System > Maintenance > Backup&Restore** to download the logs.

Syntax

```
diagnose system ha export-eventlog <node-index> <start-time> <end-time>
```

Example

```
diagnose system ha export-eventlog 2 29/12/2019:00:00:00 31/12/2019:00:00:00
```

system ha file-log

Use this command to manage the HA event logs.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose system ha file-log {clear | disable | enable | show | status}
```

enable

Enable the system to generate HA event log and store it in `var/log/gui_upload/ha_event_log`.

disable	Disable generating HA event logs.
clear	Clear the HA log files in var/log/gui_upload/ha_event_log.
show	Display HA event logs in console.
status	Show the status of the HA event log, whether it is enabled or not.

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:
  2021-01-03
  Last Update Time: 2017-02-17 Method: Scheduled
  Signature Build Number-0.00177
FortiWeb Antivirus Service:
  2021-01-03
  Last Update Time: 2017-02-17 Method: Scheduled
  Regular Virus Database Version-42.00885
  Extended Virus Database Version-42.00814
FortiWeb IP Reputation Service:
  2021-01-03
  Last Update Time: 2017-02-17 Method: Scheduled
  Signature Build Number-3.00315
System files MD5SUM: 5660BD9FA1F6C86E8A31B2A139045F17
CLI files MD5SUM: 71BF206315679018536D9E19B37CBEAE
```

Related topics

- [ha disconnect on page 833](#)
- [ha manage on page 835](#)
- [system ha status on page 808](#)
- [system status on page 864](#)

system ha interface-macinfo

Use this command to display the virtual MAC addresses of the HA node.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose system ha interface-macinfo
```

Example

Below is a sample output.

```
mgmt1 origin mac 74:fe:48:20:4f:65
mgmt2 origin mac 74:fe:48:20:4f:66
port1 origin mac 74:fe:48:20:4f:5f
port2 origin mac 74:fe:48:20:4f:60
port3 origin mac 74:fe:48:20:4f:61
port4 origin mac 74:fe:48:20:4f:62
port5 origin mac 74:fe:48:20:4f:61
port6 origin mac 74:fe:48:20:4f:62
port7 origin mac 0:b:ab:f5:3e:94
port8 origin mac 0:b:ab:f5:3e:95
port9 origin mac 0:b:ab:f5:3e:96
port10 origin mac 0:b:ab:f5:3e:97
port11 origin mac 0:b:ab:f5:4f:72
port12 origin mac 0:b:ab:f5:4f:73
```

Related topics

- [system ha mac on page 806](#)
- [ha manage on page 835](#)
- [system ha status on page 808](#)
- [system status on page 864](#)

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 details, see [Permissions on page 46](#).

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

- [ha disconnect on page 833](#)
- [ha manage on page 835](#)
- [system ha status on page 808](#)
- [system status on page 864](#)
- [system ha on page 319](#)

system ha md5fixed

This command will interfere the functioning of HA features. Do not use this command unless you are instructed by FortiWeb's support engineers or developers.

system ha md5sum-gen

This command will interfere the functioning of HA features. Do not use this command unless you are instructed by FortiWeb's support engineers or developers.

system ha nodes

Use this command to display the HA node information.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose system ha nodes
```

Example

Below is a sample output.

SN	Local	Used	State	Count
FV-1KE44XXXXXX91	1	1	0	3
FV-1KE44XXXXXX92	0	1	0	2

system ha sessions_stat

Use this command to display the HA session status.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose system ha sessions_stat
```

Example

Below is a sample output.

```
count:          0
searched:       0
```

```
new: 0
new_expect: 0
new_fail: 0
new_cancel: 0
new_unknown: 0
confirmed: 0
confirmed_fail: 0
select: 0
select_fail: 0
tuple_fail: 0
nat_request: 0
nat_done: 0
expectation: 0
sync_tx: 0
sync_tx_full: 0
sync_tx_schedule: 0
sync_tx_error: 0
```

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 details, see [Permissions on page 46](#).

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
```



```
HA group member information: is_manage_primary=1.  
FV-1KD3A13800012, primary, 4, 0, 196417  
FV-1KD3A13800091, secondary, 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

- [ha disconnect on page 833](#)
- [ha manage on page 835](#)
- [system ha status on page 808](#)
- [system status on page 864](#)

system ha sync-config

Use this command to display or change the enable/disable status of the HA synchronization

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

Use the following command to show whether the HA synchronization is enabled or not.

```
diagnose system ha sync-config get-status
```

Use the following command to enable or disable HA synchronization.

```
diagnose system ha sync-config set-status {enable | disable}
```

system ha sync-stat

Use this command to display the status of the high availability (HA) synchronization process.

Syntax

```
diagnose system ha sync-stat
```

Status	Description
INIT	Initiation. Last synchronization completed and system is ready and waiting for next synchronization.
SENDING	Synchronization is in process; data is sending.
SUCCESS	Success in data sending; synchronization is complete.
SEND_TIMEOUT	Data sending timeout; synchronization is incomplete.

Example

This example lists the HA synchronization status.

```
diagnose system ha sync-stat
```

Below is a sample output.

```
Image INIT
Config INIT
System INIT
CLI INIT
Signature SUCCESS
GeoDB SUCCESS
AV SUCCESS
IpReputation SUCCESS
HarvestCredentials SUCCESS
```

Related topics

- [ha disconnect on page 833](#)
- [ha manage on page 835](#)
- [system ha status on page 808](#)
- [system status on page 864](#)

system ha traffic-distribution

Use this command to display the traffic distribution information of 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 details, see [Permissions on page 46](#).

Syntax

```
diagnose system ha traffic-distribution
```

Example

Below is a sample output.

Traffic group information:

Name :Auto_Cluster_Group_1

Work Sn:FV-1KE4417900091

Vip List:name index ip4 ip6
FortiWeb_Vserver_Vip1 10.51.1.240/16 10:51::1:240/64

Node List:id sn

1 FV-1KE4417900091
2 FV-1KE4417900092

Name :Auto_Cluster_Group_2

Work Sn:FV-1KE4417900091

Vip List:name index ip4 ip6
FortiWeb_Vserver_Vip22 10.51.1.241/16 10:51::1:241/64

Node List:id sn

1 FV-1KE4417900091
2 FV-1KE4417900092

system jeprof

If the jemalloc profile is activated and the memory usage exceeds the configured threshold, the heap file will be generated in directory /var/log/gui_upload.

You can use this command to parse the heap file via jeprof tool. At most 10 heap files are kept on device.

Syntax

```
diagnose system jeprof
```

Related commands

To activate or deactivate jemalloc profile:

```
diagnose system kill 43 <pid_of_proxyd>
```

To check the generated heap file:

```
diagnose debug jemalloc-heap show
```

To clear generated heap file:

```
diagnose debug jemalloc-heap clear
```

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 details, see [Permissions on page 46](#).

Syntax

```
diagnose system kill <signal_int> <pid_int>
```

Variable	Description	Default
<signal_int>	Enter the ID of the signal to send to the process. This is 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; <code>SIGHUP</code>). 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; <code>SIGINT</code>). 3—Force termination immediately and do a core dump (quit; <code>SIGQUIT</code>). 9—Force termination immediately (kill; <code>SIGKILL</code>). 15—Request termination by inter-process communication (terminate; <code>SIGTERM</code>). 43—Request to activate or deactivate the jemalloc profile. If you run it the first time, jemalloc profile is activated. Running the same command again will deactivate the jemalloc profile. The following <pid_int> should be defined with the pid of the proxyd. Considering jemalloc profile has a big impact on the system performance, it's recommended to deactivate it after jemalloc profile debug.	No default.
<pid_int>	Enter the process ID where the signal is sent to. To list all current process IDs, use system top on page 813.	No default.

Related topics

- [system top on page 813](#)
- [hardware cpu on page 774](#)
- [hardware mem on page 778](#)
- [system performance on page 863](#)

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 details, see [Permissions on page 46](#).

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

- [hardware logdisk info on page 777](#)
- [hardware raid list on page 782](#)

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 details, see [Permissions on page 46](#).

Syntax

```
diagnose system top [<delay_int> [<delay_int>]]
```

Variable	Description	Default
<delay_int>	Enter 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
hatalnk 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

- [system kill on page 812](#)
- [hardware cpu on page 774](#)
- [hardware mem on page 778](#)
- [system performance on page 863](#)

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.

system waf-signature pcre-high-cpu-cost

In some cases, certain PCRE (Perl Compatible Regular Expression) patterns may result in inefficient matching processes that consume significant CPU resources. This can lead to performance issues such as "CPU stuck" scenarios, where FortiWeb may appear unresponsive, and the client's website may temporarily become inaccessible.

To address this, timing thresholds are used to identify high-CPU-cost PCRE matches for further analysis:

- Threshold for inbound traffic (Client-to-FortiWeb): **2** seconds
- Threshold for outbound traffic (FortiWeb-to-Client): **5** seconds

If a PCRE match exceeds the designated threshold, FortiWeb automatically records detailed information about the match. This information can be later dumped or stored in nonvolatile storage for further review and optimization.

Relevant CLI commands for monitoring and managing high CPU usage by PCRE

Starting from 7.6.1, the following commands are added for troubleshooting the high CPU usage caused by PCRE.

- Enable/disable pcre high CPU cost monitoring:

```
diagnose system waf-signature pcre-high-cpu-cost { enable | disable } //default: enable
```

- View high CPU cost configuration and summary:

```
diagnose system waf-signature pcre-high-cpu-cost show { config | briefing }
```

- Dump recorded high CPU cost pcre data:

```
diagnose system waf-signature pcre-high-cpu-cost dump
```

- Clear high CPU cost pcre records:

```
diagnose system waf-signature pcre-high-cpu-cost cleanup
```

- Set timing thresholds for high CPU cost pcre matching:

```
diagnose system waf-signature pcre-high-cpu-cost config threshold { request | response }  
    <threshold> // (1~600) in deci-seconds
```

- Set extra delay for debugging purposes (available in debug versions only):

```
diagnose system waf-signature pcre-high-cpu-cost set extra-delay <extra-delay> // (0~6000)  
    in deci-seconds
```

These commands allow you to monitor and manage high CPU usage caused by inefficient PCRE pattern matching, helping to improve FortiWeb's performance by identifying and addressing patterns that may require optimization.

Related topics

- [debug on page 747](#)
- [debug console timestamp on page 752](#)
- [debug info on page 763](#)
- [debug reset on page 769](#)
- [debug upload on page 772](#)

test application

Use this command to check if an IP address is in irdb (IP reputation database) and geodb database.

To use this command, your administrator account's access control profile requires only `r` permission in any profile area. For details, see [Permissions on page 46](#).

Syntax

```
diagnose test application irdb <IP_address>  
diagnose test application geodb <IP_address>
```

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.

backup cert-config

Use this command to back up certificates of a FortiWeb appliance to a TFTP server.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
execute backup cer-config <filename_str> <tftp_ipv4> [<password_str>]
```

Variable	Description	Default
<filename_str>	Enter the name of the file to be used for the backup file, such as <code>FortiWeb_backup.zip</code> .	No default.
<tftp_ipv4>	Enter the IP address of the TFTP server.	No default.
[<password_str>]	Enter a password to be used when decompressing the backup file. 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 won't be able to use that encrypted backup file.	No default.

Example

This example backs up certificates of the FortiWeb appliance on a TFTP server at IP address `192.0.2.23`. The file is encrypted with the password `P@ssword1`.

```
execute backup cert-config tftp FortiWeb_backup.zip 192.0.2.23 P@ssword1
```

Related topics

- [backup cli-config on page 821](#)
- [backup full-config on page 822](#)

- [system backup on page 245](#)

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:

- 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. For details, see [backup full-config on page 822](#) or [system backup on page 245](#).

This command also 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 [backup full-config on page 822](#).

Alternatively, you can back up the configuration to an FTP or SFTP server. For details, see [system backup on page 245](#).

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
execute backup cli-config tftp <filename_str> <tftp_ipv4> [<password_str>]
```

Variable	Description	Default
<filename_str>	Enter the name of the file to be used for the backup file, such as <code>FortiWeb_backup.conf</code> .	No default.
<tftp_ipv4>	Enter the IP address of the TFTP server.	No default.
[<password_str>]	Enter a password to be used when encrypting the backup file to a <code>.zip</code> extension file. If you don't provide a password, the backup file will be stored as a clear file with a <code>.zip</code> extension. 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 won't 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.zip` on a TFTP server at IP address `192.0.2.23`. The file will not be password-encrypted.

```
execute backup cli-config tftp fweb.zip 192.0.2.23
```

Related topics

- [backup full-config on page 822](#)
- [restore config on page 848](#)
- [system backup on page 245](#)

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.



We strongly recommend 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. For details, see [system backup on page 245](#).

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 details, see [Permissions on page 46](#).

Syntax

```
execute backup full-config tftp <filename_str> <tftp_ipv4> [<password_str>]
```

Variable	Description	Default
<filename_str>	Enter the name of the file to be used for the backup file, such as <code>FortiWeb_backup.conf</code> .	No default.
<tftp_ipv4>	Enter the IP address of the TFTP server.	No default.
[<password_str>]	Enter a password to be used when encrypting the backup file to a <code>.zip</code> extension file.	No default.

Variable	Description	Default
	If you don't provide a password, the backup file will be stored as a clear file with a <code>.zip</code> extension. 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.	

Example

This example uploads the FortiWeb appliance's entire configuration, including uploaded error page and HTTPS certificate files, to a file named `fweb.zip` on a TFTP server at IP address `192.0.2.23`. The file is encrypted with the password `P@ssword1`.

```
execute backup full-config tftp fweb.zip 192.0.2.23 P@ssword1
```

Related topics

- [backup cli-config on page 821](#)
- [system backup on page 245](#)

backup full-config-with-ML-data

Use this command to manually back up the entire configuration file with machine learning data, **including** those settings that remain at their default values, to a TFTP server.



We strongly recommend 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. For details, see [system backup on page 245](#).

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 details, see [Permissions on page 46](#).

Syntax

```
execute backup full-config-with-ML-data tftp <filename_str> <tftp_ipv4> [<password_str>]
```

Variable	Description	Default
<filename_str>	Enter the name of the file to be used for the backup file, such as <code>FortiWeb_backup.conf</code> .	No default.
<tftp_ipv4>	Enter the IP address of the TFTP server.	No default.
[<password_str>]	Enter a password to be used when encrypting the backup file to a <code>.zip</code> extension file. If you don't provide a password, the backup file will be stored as a clear file with a <code>.zip</code> extension. 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 with machine learning data, including uploaded error page and HTTPS certificate files, to a file named `fweb.zip` on a TFTP server at IP address `192.0.2.23`. The file is encrypted with the password `P@ssword1`.

```
execute backup full-config-with-ML-data tftp fweb.zip 192.0.2.23 P@ssword1
```

Related topics

- [backup full-config on page 822](#)
- [backup cli-config on page 821](#)
- [system backup on page 245](#)

backup web-protection-profile

Use this command to back up web protection profiles of a FortiWeb appliance to a TFTP server.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
execute backup web-protection-profile <filename_str> <tftp_ipv4>[<password_str>]
```

Variable	Description	Default
<filename_str>	Enter the name of the backup file, such as <code>config.zip</code> .	No

Variable	Description	Default
		default.
<tftp_ipv4>	Enter the IP address of the TFTP server.	No default.
[<password_str>]	Enter a password to be used when encrypting the backup .zip extension file. This is optional. If you don't provide a password, the backup file will be stored as a clear file with a .zip extension. 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 won't be able to use that encrypted backup file.	No default.

Example

This example backs up web protection profiles of the FortiWeb appliance on a TFTP server at IP address 192.0.2.23. The file is encrypted with the password P@ssword1.

```
execute backup web-protection-profile tftp config.zip 192.0.2.23 P@ssword1
```

Related topics

- [system backup on page 245](#)

batch

Use this command to execute commands in a group. If a command in the group fails or an operation cannot be completed, every command in the group can be rolled back, whether they were successful or not.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
execute batch start
execute batch status
execute batch lastlog
execute batch recover
execute batch end
```

Variable	Description	Default
start	Enter to initiate batch mode. Every subsequent command will be grouped until you enter the <code>execute batch end</code> command.	No default.
status	Enter to determine whether batch mode is running. If batch mode is running, you will see this message: <code>Batch mode is running...</code> If batch mode is not running, you will see this command: <code>Batch mode is stopped...</code>	No default.
lastlog	Enter to view the executed commands in the current batch mode.	No default.
recover	Enter to rollback every command that has been executed in the current batch mode.	No default.
end	Enter to turn off batch mode.	No default.

create-raid level

Use the this command to initialize the RAID.

Currently, only RAID level 1 is supported, and only on FortiWeb 1000B/C/D/E, 2000E, 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 details, see [Permissions on page 46](#).

Syntax

```
execute create-raid level {raid1}
```

Variable	Description	Default
level {raid1}	Enter the RAID level. Currently, only RAID level 1 is supported.	raid1

Related topics

- [system raid on page 364](#)
- [hardware raid list on page 782](#)
- [create-raid rebuild on page 827](#)

create-raid rebuild

Use the this command to rebuild the RAID.

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-1000E
- FortiWeb-1000F
- FortiWeb-2000E
- FortiWeb-3000C
- FortiWeb-3000D
- FortiWeb-3000E
- FortiWeb-4000C
- FortiWeb-4000D
- FortiWeb-4000E

Note: All supported platforms use hardware RAID, except for the FortiWeb-1000E and 1000F models, which implement software RAID.

On FortiWeb-1000E and 1000F (software RAID), executing this command displays a “data will be clearing” prompt before proceeding. On all other supported hardware RAID platforms, no such prompt is shown.

RAID cannot be activated on older appliances that were upgraded to FortiWeb 4.0 MR1.



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 details, see [Permissions on page 46](#).

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 on page 364](#)
- [hardware raid list on page 782](#)

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 details, see [Permissions on page 46](#).

Syntax

```
execute date <date_str>
```

Variable	Description	Default
date <date_str>	Enter the current date for the FortiWeb appliance's time zone, using the format <code>yyyy-mm-dd</code>, where: • <code>yyyy</code> is the year. Valid years are 2001 to 2037. • <code>mm</code> is the month. Valid months are 01 to 12. • <code>dd</code> 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 <code>06</code> instead of <code>2006</code> for the year or <code>1</code> instead of <code>01</code> for the month or day, are not valid.	No default.

Example

This example sets the date to September 23, 2017:

```
execute date 2017-09-23
```

Related topics

- [time on page 856](#)

db rebuild

Use this command to clean and rebuild the FortiWeb appliance's database for disklog. Please note in HA mode, running `execute db rebuild` on master appliance will take effect on all slaves simultaneously.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For details, see [Permissions on page 46](#).



For some cases, it would take a long time to complete database rebuild depending on how many logs the system has. While the database is rebuilding, new generated logs are postponed to be written to the database so the newly generated logs are not available immediately on GUI. The logs are all saved in log files. No logs would be lost.

Syntax

```
execute db rebuild
```

Related topics

- [formatlogdisk on page 832](#)
- [debug upload on page 772](#)

dnscache-cleanup

Use this command to clean up all the DNS proxy cache information.

Syntax

```
execute dnscache-cleanup
This operation will clean up all the dnsproxy cache information!
Do you want to continue? (y/n)
```

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. For details, see [system fips-cc](#) on page 291.

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. The valid range is 1–35.	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 details about creating a backup, see [backup cli-config](#) on page 821.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For details, see [Permissions](#) on page 46.

Syntax

```
execute factoryreset
```

Related topics

- [backup cli-config](#) on page 821
- [backup full-config](#) on page 822
- [restore config](#) on page 848

fctems

Use this command to verify or unverify the EMS server, or show the verification status.

Syntax

To verify the certificate of an EMS server, run:

```
execute fctems verify <ems_name>
```

To disconnect from an EMS server, run:

```
execute fctems unverify <ems_name>
```

To check whether an EMS server is verified, run:

```
execute fctems is-verified <ems_name>
```

Related topics

- [system endpoint-control on page 281](#)
- [fctems on page 831](#)
- [server-policy ztna-profile on page 217](#)
- [server-policy ztna-rule on page 219](#)

fdnserver delete

Use this command to delete all FDS servers. FortiWeb will update the FDS servers during the next update.

Syntax

```
execute fdnserver delete
```

Related topics

[fdnserver show on page 832](#)

fdnserver show

Use this command to show the list of all current FDS servers.

Syntax

```
execute fdnserver show
```

Example

```
execute fdnserver show
SerialNumber=FPT-FDS-
  DELL0002|Address=173.243.138.80:443|FDNListener=173.243.138.80:8889|TimeZone=9
SerialNumber=FPT-FDS-
  DELL0004|Address=173.243.138.66:443|FDNListener=173.243.138.66:8889|TimeZone=-8
```

Related topics

[fdnserver delete on page 831](#)

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.
 - The system will reboot after this command is executed.
-

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

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

- [db rebuild on page 829](#)

forticloud-sandbox

These commands allow administrators to manage FortiCloud Sandbox connectivity. The **update** command refreshes the contract information to ensure the device has the latest service entitlement, while the **show** command retrieves the current FortiCloud Sandbox IP address for verification and troubleshooting.

Syntax

```
execute forticloud-sandbox update
execute forticloud-sandbox show
```

Variable	Description	Default
update	Updates the FortiCloud Sandbox contract information.	No default.
show	Displays the IP address of the FortiCloud Sandbox service.	No default.

Example

```
FortiWeb # execute forticloud-sandbox update
Region: Europe
connectivity status: Connected

FortiWeb # execute forticloud-sandbox show
Region: Europe
Server ip addr: 83.231.212.151
Server port: 514
Alternate server ip addr: 83.231.212.157
Alternate server port: 514
```

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 details, see [Permissions on page 46](#).

Syntax

```
execute ha disconnect <serial-number_str> <interface_name> <interface_ipv4mask/ipv6mask>
```

Variable	Description	Default
disconnect <serial-number_str>	Enter 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, enter: <code>execute ha disconnect ?</code>	No default.
<interface_name>	Enter the name of the network interface, such as <code>port1</code> , that will be configured as the ejected appliance's management interface.	No default.
<interface_ipv4mask/ipv6mask>	Enter 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 interface, reachable at 192.0.2.123.

```
execute ha disconnect FV-1KC3R11111111 port1 192.0.2.123/24 192::2:123/64
```

After the command completes, to reconfigure the ejected appliance, you could then use either a web browser or SSH client to connect to 192.0.2.123 in order to reconfigure it for standalone operation.

Related topics

- [ha disconnect on page 833](#)
- [ha manage on page 835](#)
- [ha md5sum on page 836](#)
- [system ha status on page 808](#)
- [system ha mac on page 806](#)
- [system status on page 864](#)

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) from the main (primary) 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 details, see [Permissions on page 46](#).

Syntax

```
execute ha manage <cluster-index>
```

Variable	Description	Default
<cluster-index>	Enter 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: <pre>execute ha manage ?</pre>	No default.

Example

In this example, you are logged in to the main appliance.

```
execute ha manage ?
<id>    please input peer box index.
<2>     Subsidiary unit FV-1KD3A12345678
<3>     Subsidiary 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, enter `exit`.

Related topics

- [ha disconnect on page 833](#)
- [ha md5sum on page 836](#)
- [ha synchronize on page 836](#)
- [system ha status on page 808](#)
- [system ha mac on page 806](#)

ha md5sum

Use this command to retrieve the CLI system configuration MD5 from the appliances in an HA cluster.

This information allows you to confirm whether the HA configuration is synchronized.

Syntax

```
execute ha md5sum
```

Example

Below is a sample output.

```
FortiWeb # execute ha md5sum
FV-1KD3A15800048<Primary>
  SYS: A4BA318B0762E202B4CAE44173F08CB5
  CLI: 408268C68309651DC4C9D8C094B1EF0F
FV-1KD3A14800059<Secondary>
  SYS: A4BA318B0762E202B4CAE44173F08CB5
  CLI: 408268C68309651DC4C9D8C094B1EF0F
```

Related topics

- [ha disconnect on page 833](#)
- [ha manage on page 835](#)

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, including 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
- Manually force synchronization of files that are not automatically synchronized
- 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 details, see [Permissions on page 46](#).

Syntax

```
execute ha synchronize {all | avupd | cli | geodb | sys}
```

Variable	Description	Default
synchronize {all avupd cli geodb sys}	Select which part of the configuration and/or FortiGuard service-related packages to synchronize. <code>all</code>—Entire configuration, including CLI configuration, system files, and signature databases. <code>avupd</code>—Only the FortiGuard Antivirus service package, including the virus signatures, scan engine, and proxy. <code>cli</code>—Only the core CLI configuration file (FortiWeb_system.conf). You can use the <code>show</code> command to view the contents of the configuration file. <code>geodb</code>—Only the geography-to-IP address mappings. Similar to firmware, these can be downloaded from the Fortinet Customer Service & Support website: https://support.fortinet.com <code>sys</code>—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 <code>execute ha synchronize stop</code> to pause it manually.	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 primary...
```

Related topics

- [ha disconnect on page 833](#)
- [ha manage on page 835](#)
- [ha md5sum on page 836](#)

icap-cache-clear

ICAP server receives files from FortiWeb to verify whether the files pose a threat and returns the results to FortiWeb. The results are stored in FortiWeb cache for a certain period so that during then FortiWeb does not re-submit the file to ICAP server.

Use this command to clear ICAP cache. You can specify the hash value of the file to clear the cached results for specific files, or clear all cache.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
execute icap-cache-clear sha256 <sha256 strings of file1> <sha256 strings of file2> ...
execute icap-cache-clear all
```

Variable	Description	Default
<sha256 strings of file1> <sha256 strings of file2> ...	Enter the sha256 strings of the files to be cleared. Up to 32 hash value strings are allowed.	No default.
all	Clear all cache.	No default.

Example

```
FortiWeb # execute icap-cache-clear sha256 XXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXX
FortiWeb # execute icap-cache-clear all
```

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 details, see [Permissions on page 46](#).

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 192.0.2.10.

```
execute ping 192.0.2.10
```

The CLI displays the following:

```
PING 192.0.2.10 (192.0.2.10): 56 data bytes
 64 bytes from 192.0.2.10: icmp_seq=0 ttl=128 time=0.5 ms
 64 bytes from 192.0.2.10: icmp_seq=1 ttl=128 time=0.2 ms
 64 bytes from 192.0.2.10: icmp_seq=2 ttl=128 time=0.2 ms
```

```
64 bytes from 192.0.2.10: icmp_seq=3 ttl=128 time=0.2 ms
64 bytes from 192.0.2.10: icmp_seq=4 ttl=128 time=0.2 ms
--- 192.0.2.10 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 192.0.2.10. 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 192.0.2.78.

```
execute ping 192.0.2.78
```

The CLI displays the following:

```
PING 192.0.2.78 (192.0.2.78): 56 data bytes
```

After several seconds, no output appears. The administrator halts the ping by pressing Ctrl+C. The CLI displays the following:

```
--- 192.0.2.78 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 192.0.2.78. To determine the point of failure along the route, further diagnostic tests are required, such as [traceroute on page 857](#).

Related topics

- [system interface on page 344](#)
- [server-policy vserver on page 215](#)
- [ping-options on page 841](#)
- [ping6 on page 839](#)
- [telnettest on page 854](#)
- [traceroute on page 857](#)
- [network ip on page 786](#)
- [hardware nic on page 779](#)
- [network sniffer on page 790](#)

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 in [ping-options on page 841](#).

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 details, see [Permissions on page 46](#).

Syntax

```
execute ping6 {<host_fqdn> | <host_ipv6>}
```

Variable	Description	Default
ping6 {<host_fqdn> <host_ipv6>}	Enter either the IP address or fully qualified domain name (FQDN) of the host.	No default.

Example

This example pings a host with the IP address `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 857](#).

Related topics

- [system interface on page 344](#)
- [server-policy vserver on page 215](#)
- [ping6-options on page 842](#)
- [telnettest on page 854](#)
- [traceroute on page 857](#)
- [network ip on page 786](#)
- [hardware nic on page 779](#)
- [network route on page 787](#)
- [network sniffer on page 790](#)

ping-options

Use these commands to configure the behavior of the [ping on page 838](#) command.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

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> on page 841 .	56
df-bit {yes no}	Enter either <code>yes</code> to set the DF bit in the IP header to prevent the ICMP packet from being fragmented, or enter <code>no</code> to allow the ICMP packet to be fragmented.	no
pattern <bufferpattern_hex>	Enter a hexadecimal pattern, such as <code>00ffaabb</code> , 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> on page 841 .	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 <code>auto</code> 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: <code>default</code>—Do not indicate. That is, set the TOS byte to 0. <code>lowcost</code>—Minimize cost. <code>lowdelay</code>—Minimize delay.	default

Variable	Description	Default
	- reliability—Maximize reliability. - throughput—Maximize throughput.	
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 192.0.2.1, then views the ping options to verify their configuration.

```
execute ping-option repeat-count 3
execute ping-option source 192.0.2.1
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: 192.0.2.1
Pattern:
Pattern Size in Bytes: 0
Validate Reply: no
```

Related topics

- [ping on page 838](#)
- [traceroute on page 857](#)

ping6-options

Use these commands to configure the behavior of the [ping6 on page 839](#) command.

To use this command, your administrator account's access control profile must have at least `r` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

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_ipv6>}
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> on page 841 .	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> on page 841 .	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 <code>auto</code> 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: <code>default</code>—Do not indicate. That is, set the TOS byte to 0. <code>lowcost</code>—Minimize cost. <code>lowdelay</code>—Minimize delay. <code>reliability</code>—Maximize reliability. <code>throughput</code>—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

- [ping6 on page 839](#)
- [traceroute on page 857](#)

private-encryption-key

When private encryption is enabled (see [system encryption-method on page 280](#)), FortiWeb generates a private key to secure sensitive configurations. If private encryption is disabled and later re-enabled, a new private key is generated, which can cause backup configurations encrypted with the previous key to become unusable.

To troubleshoot such scenarios, use the `execute private-encryption-key sample` command to generate a base64-encoded clear text string and its HMAC signature encrypted with the current private key. Before any private key changes, users should generate and record this sample for future verification.

If a backup configuration fails to restore, the `execute private-encryption-key verify` command can be used to check whether the stored sample still matches the current private key. A failed verification indicates that a new private key was generated, confirming that the original key is no longer in use. If the verification passes, the private key remains unchanged.

Syntax

```
execute private-encryption-key sample
execute private-encryption-key verify <sample>
```

Variable	Description	Default
sample	Generate a base64-encoded clear text string and its HMAC signature encrypted using the private key.	No default.
verify <sample>	Verify the HMAC signature of the provided base64-encoded clear text using the private key. Use the sample generated by <code>execute private-encryption-key sample</code> .	No default.

Example

```
# execute private-encryption-key sample
B64TEXT: ec1d9EtAaX7ZH16CBihdb4/8QdqgjWZwkrEqqJYswbk=
B64HMAC: hDYGL62rIeg4NuspIAt2Pd8thrE=

# execute private-encryption-key verify ec1d9EtAaX7ZH16CBihdb4/8QdqgjWZwkrEqqJYswbk=
hDYGL62rIeg4NuspIAt2Pd8thrEa
Verification failed.
```

Related topics

[system encryption-method on page 280](#)

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 details, see [Permissions on page 46](#).

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

- [shutdown on page 853](#)
- [system performance on page 863](#)

redis rebuild

Use this command to clean and rebuild the database for ML and Client Management. Please note in HA mode, running `execute db rebuild` on master appliance will take effect on all slaves simultaneously. It will reboot the system.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
execute redis rebuild
```

Related topics

- [formatlogdisk on page 832](#)
- [debug upload on page 772](#)

remove vmlicense

Use this command to remove a FortiWeb-VM license.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For details, see [Permissions on page 46](#).

For more information on FortiWeb-VM licenses, see the *FortiWeb-VM Install Guide*:

<https://docs.fortinet.com/fortiweb/hardware>

Syntax

```
execute remove vmlicense
```

Example

This example shows the remove command in action.

```
execute remove vmlicense
```

The CLI displays the following:

```
This operation will remove existing license!  
Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following:

```
removing license .....
```

Related Topics

- [restore vmlicense on page 851](#)

restore cert-config

Use this command to restore certificates of a FortiWeb appliance from a TFTP, SFTP, or FTP server.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `mntgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
execute restore cer-config <sftp/ftp/tftp> <filename_str><ipv4>[<password_str>]
```

Variable	Description	Default
<filename_str>	Enter the name of the file to be used for the backup file, such as <code>FortiWeb_backup.zip</code> .	No default.
<ipv4>	Enter the IP address of the TFTP, SFTP, or FTP server.	No default.
[<password_str>]	Enter a password to be used when decompressing the backup file. 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 won't be able to use that encrypted backup file.	No default.

Example

This example restores certificates of the FortiWeb appliance on a TFTP server at IP address `192.0.2.23`. The file is encrypted with the password `P@ssword1`.

```
execute restore cert-config tftp FortiWeb_backup.zip 192.0.2.23 P@ssword1
```

Related topics

- [restore config on page 848](#)

restore config

Use this command to restore the configuration from a configuration backup file on a TFTP, SFTP, or FTP 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 [backup cli-config on page 821](#) and [backup full-config on page 822](#).

To use this command, your administrator account’s access control profile must have either `w` or `rw` permission to the `mntgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
execute restore config <sftp/ftp/tftp> <filename_str> <ipv4> [<password_str>]
```

Variable	Description	Default
<filename_str>	Enter the name of the backup or firmware image file.	No default.
<ipv4>	Enter the IP address of the TFTP, SFTP, or FTP servers.	No default.
[<password_str>]	Enter 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 a clear file with a <code>.zip</code> extension.	No default.

Example

This example downloads a configuration file named `backup.zip` from the TFTP server, `192.0.2.23`, to the FortiWeb appliance. The backup file was encrypted with the password `P@ssword1`.

```
execute restore config tftp backup.zip 192.0.2.23 P@ssword1
```

The FortiWeb appliance then applies the configuration backup and reboots.

Related topics

- [backup full-config on page 822](#)
- [restore config on page 848](#)
- [restore image on page 849](#)
- [restore secondary-image on page 850](#)

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 [backup full-config on page 822](#) and [backup cli-config on page 821](#).

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 details, see [Permissions on page 46](#).

Syntax

```
execute restore image ftp <filename_str> <ftp_ipv4>
execute restore image tftp <filename_str> <tftp_ipv4>
```

Variable	Description	Default
<filename_str>	Enter the name of the firmware image file.	No default.
<ftp_ipv4>	Enter the IP address of the TFTP server.	No default.
<tftp_ipv4>	Enter the IP address of the FTP server.	No default.

Example

This example installs a firmware file named `firmware.out` from the TFTP server, `192.0.2.23`, to the FortiWeb appliance.

```
execute restore image tftp firmware.out 192.0.2.23
```

The FortiWeb appliance downloads the firmware file, installs it, and reboots.

Related topics

- [backup cli-config on page 821](#)
- [backup full-config on page 822](#)
- [restore config on page 848](#)
- [restore secondary-image on page 850](#)
- [system flash on page 799](#)
- [system status on page 864](#)

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 822](#) and [backup cli-config on page 821](#).

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 details, see [Permissions on page 46](#).

Syntax

```
execute restore secondary-image ftp <filename_str> <ftp_ipv4>
execute restore secondary-image tftp <filename_str> <tftp_ipv4>
```

Variable	Description	Default
<filename_str>	Enter the name of the firmware image file.	No default.
<ftp_ipv4>	Enter the IP address of the FTP server.	No default.
<tftp_ipv4>	Enter the IP address of the TFTP server.	No default.

Example

This example installs a firmware file named `firmware.out` from the TFTP server, `192.0.2.23`, to the FortiWeb appliance.

```
execute restore secondary-image tftp firmware.out 192.0.2.23
```

The FortiWeb appliance downloads the firmware file, installs it, and reboots.

Related topics

- [backup cli-config on page 821](#)
- [backup full-config on page 822](#)
- [restore config on page 848](#)
- [restore image on page 849](#)
- [system flash on page 799](#)
- [system status on page 864](#)

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 details, see [Permissions on page 46](#).

For more information on FortiWeb-VM licenses, see the *FortiWeb-VM Install Guide*:

<https://docs.fortinet.com/fortiweb/hardware>

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>"	Enter the name of the license file.	No default.
"<ftp_ipv4>"	Enter the IP address of the FTP server.	No default.
"<user_str>"	Enter the user name that FortiWeb uses to authenticate with the server.	No default.
"<password_str>"	Enter the password for the account specified by <user_str>.	No default.
"<tftp_ipv4>"	Enter the IP address of the TFTP server.	No default.

Example

This example uploads the license file `FVVM040000010871.lic` from the TFTP server `192.0.2.23` to the FortiWeb appliance.

```
execute restore vmlicense tftp FVVM040000010871.lic 192.0.2.23
```

The FortiWeb appliance uploads the file, and then prompts you to log out and log in again.

sandbox-cache-clear

Use this command to clear Sandbox cache. You can specify the hash value of the file to clear the cached results for specific files, or clear all cache.

To use this command, your administrator account's access control profile must have either `w` or `rw` permission to the `sysgrp` area. For details, see [Permissions on page 46](#).

Syntax

```
execute sandbox-cache-clear sha256 <sha256 strings of file1> <sha256 strings of file2>
...
execute sandbox-cache-clear all
```

Variable	Description	Default
<sha256 strings of file1> <sha256 strings of file2> ...	Enter the sha256 strings of the files to be cleared. Up to 32 hash value strings are allowed.	No default.
all	Clear all cache.	No default.

Example

```
FortiWeb # execute sandbox-cache-clear sha256 XXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXX
FortiWeb # execute sandbox-cache-clear all
```

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 details, see [Permissions on page 46](#).

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 details, see [Permissions on page 46](#).

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

- [reboot on page 845](#)

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 details, see [Permissions on page 46](#).

Syntax

```
execute telnet "<host_ipv4>"
```

Variable	Description	Default
telnet "<host_ipv4>"	Enter the IP address of the host.	No default.

Example

This example Telnets to a host with the IP address 192.0.2.10.

```
execute telnet 192.0.2.10
login: admin
Password: *****
```

Related topics

- [telnettest on page 854](#)
- [ping on page 838](#)
- [ping6 on page 839](#)

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 details, see [Permissions on page 46](#).

Syntax

```
execute telnettest {"<host_ipv4>" | "<host_ipv6>" | "<host_fqdn>"}
```

Variable	Description	Default
telnettest {"<host_ipv4>" "<host_ipv6>" "<host_fqdn>"}	Enter 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 `192.0.2.10` on port `80`, the IANA standard port for HTTP.

```
FortiWeb# exec telnettest 192.0.2.10:80
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 192.0.2.10 port 80:
```

```
Connecting to remote host succeeded.
```

Related topics

- [telnet on page 854](#)
- [ping on page 838](#)
- [ping6 on page 839](#)

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 details, see [Permissions on page 46](#).

Syntax

```
execute time [<time_str>]
```

Variable	Description	Default
time [<time_str>]	Enter the current date for the FortiWeb appliance's time zone, using the format <code>hh:mm:ss</code>, where: <code>hh</code> is the hour. Valid hours are 00–23 <code>mm</code> is the minute. Valid minutes are 00–59. <code>ss</code> is the second. Valid seconds are 00–59. If you do not specify a time, the command returns the current system time. Shortened values, such as <code>1</code> instead of <code>01</code> for the hour, are valid. For example, you could enter either <code>01:01:01</code> or <code>1:1:1</code>.	No default.

Example

This example sets the system time to 15:31:03:

```
execute time 15:31:03
```

Related topics

- [date on page 828](#)

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 details, see [Permissions on page 46](#).

Syntax

```
execute traceroute {"<host_fqdn>" | "<host_ipv4>"}
```

Variable	Description	Default
traceroute {"<host_fqdn>" "<host_ipv4>"}	Enter 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
1 192.0.2.200 (192.0.2.200) 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 [system dns on page 279](#).

Related topics

- [ping on page 838](#)
- [ping-options on page 841](#)
- [network ip on page 786](#)
- [hardware nic on page 779](#)
- [network sniffer on page 790](#)

ttp_src_ip_whitelist

Use this command to manage the source IP whitelist used to bypass Transparent Proxy (TTP) processing for TCP monitoring traffic. When a source IP is on the whitelist, FortiWeb forwards TCP connections from that IP directly to the backend server without applying delayed binding or full proxy behavior.

This is useful in scenarios where external monitoring systems rely on TCP-level probes to determine backend availability.

Syntax

```
execute ttp_src_ip_whitelist {add | del} <ip_address>
execute ttp_src_ip_whitelist flush
execute ttp_src_ip_whitelist list
```

Parameter	Description
add <ip_address>	Adds the specified IP address to the whitelist.
del <ip_address>	Removes the specified IP address from the whitelist.
flush	Clears all entries from the whitelist.
list	Displays the current list of whitelisted IP addresses.

Example

```
execute ttp_src_ip_whitelist add 192.0.2.10
execute ttp_src_ip_whitelist list
execute ttp_src_ip_whitelist del 192.0.2.10
execute ttp_src_ip_whitelist flush
```

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 details, see [Permissions on page 46](#).

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 : 192.0.2.19
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.

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 192.0.2.10
FortiWeb (dns)# get
primary : 192.0.2.19
secondary : 192.0.2.10
domain : example.com
FortiWeb (dns)# get system dns
primary : 192.0.2.19
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 [system performance on page 863](#), 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.



Although not explicitly shown in this section, for all [config on page 60](#) commands, there are related `get` and [show on page 867](#) 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 60](#).

When ADOMs are enabled, 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.

system fortisandbox-statistics

Use this command to display a count of uploaded files that FortiSandbox has evaluated in the past seven days, by evaluation result.

FortiWeb organizes 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

- [system fortisandbox on page 305](#)
- [waf file-upload-restriction-policy on page 497](#)
- [log reports on page 77](#)

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

- [system status on page 864](#)
- [hardware cpu on page 774](#)
- [hardware mem on page 778](#)
- [hardware raid list on page 782](#)
- [system kill on page 812](#)
- [system top on page 813](#)
- [policy on page 797](#)
- [reboot on page 845](#)

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

- [system performance on page 863](#)
- [system ha status on page 808](#)

waf predefined-global-allow-list

Use this command to get the global object allow list. This feature reduces false positives and improves performance.

Syntax

```
get waf predefined-global-allow-list
```

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

- [waf signature on page 612](#)

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 on page 60](#) commands, there are related [get on page 861](#) 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 60](#).

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.

Append `grep -f <keyword>` to the `show` or `show full-configuration` command to display configurations related to the search keywords. This command will not only show the lines containing the keywords but also the entire upper-level command structure associated with them. For example, if you want to view the context of the SNMP command, run the following:

```
show full-configuration | grep -f snmp
```

The system will display the configurations which contain the keyword "snmp":

```
show full-configuration | grep -f snmp
config global
  config system interface
    edit "mgmt1"
      set type physical
      set ip 
      set ip6 ::/0
      set allowaccess ping ssh snmp http https FWB-manager <---
      set status up
      set mode static
      set ip6-mode static
      unset description
      unset ip6-allowaccess
      unset adom
      set wccp disable
      set mtu 1500
      unset dynamic_gateway
      unset dynamic_dns1
      unset dynamic_dns2
    next
  end
  config system snmp sysinfo <---
    set status disable
    unset engine-id
    unset description
    unset contact-info
    unset location
  end
  config system snmp community <---
  end
  config system snmp user <---
  end
end
```



If you have entered settings but cannot remember how they differ from the existing configuration, the two different forms of `show`, with and without the object name, can be a useful way to remind yourself.

If you were to now enter `end`, saving your setting to disk, `show` output for both syntactical forms would again match. However, if you were to enter `abort` at this point and discard your recently entered secondary DNS setting instead of saving it to disk, the FortiWeb appliance's configuration would therefore match the second output, not the first.

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

- `show global` displays settings that only `admin` or other accounts with the **prof_admin** access profile can change.
- `show 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.



www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.