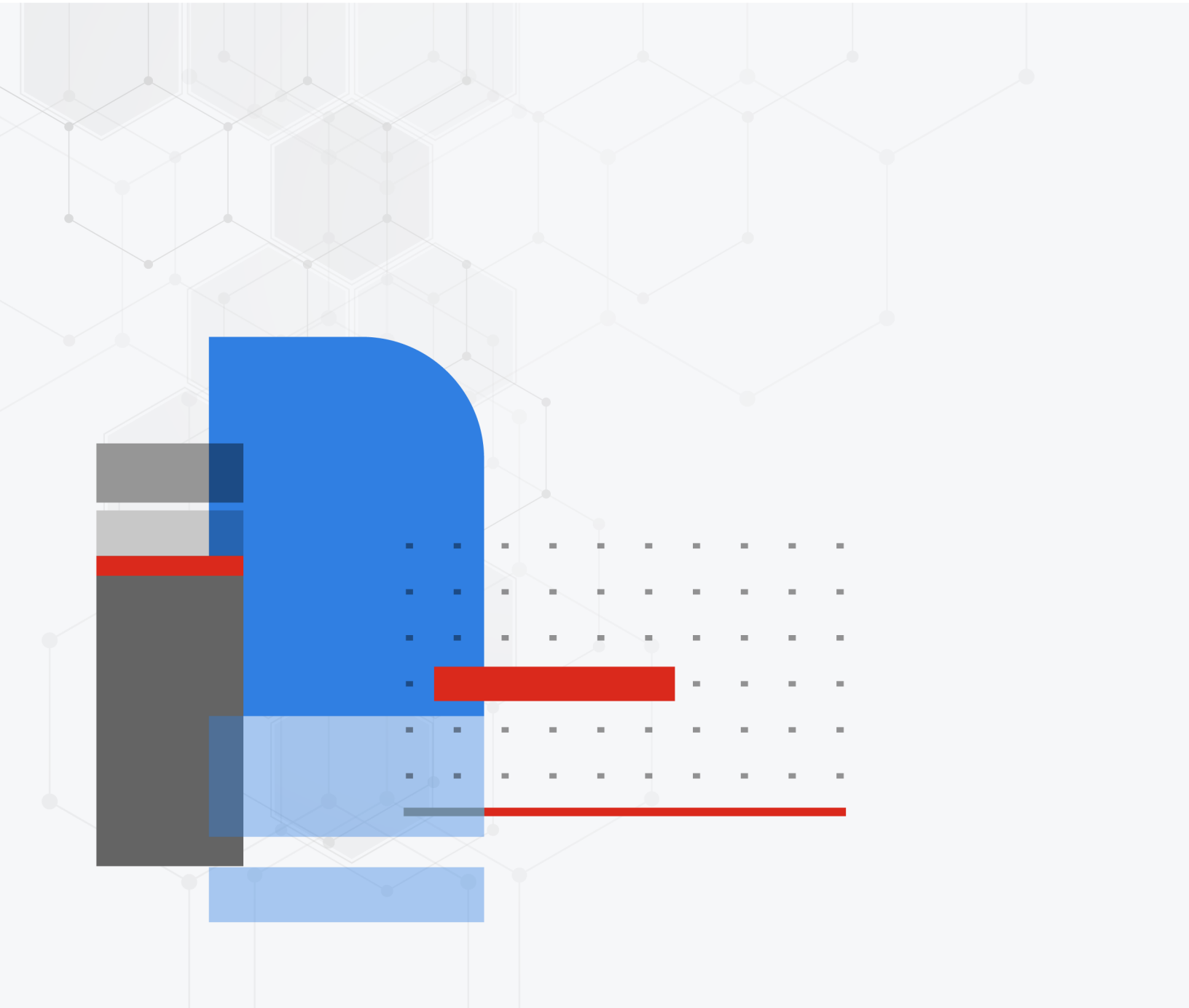




CLI Reference

FortiProxy 7.4.7



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



December 13, 2024

FortiProxy 7.4.7 CLI Reference

45-747-1024864-20241213

TABLE OF CONTENTS

Change log	25
FortiProxy CLI Interface	26
alertemail	27
config alertemail setting	27
config alertemail setting	28
antivirus	34
config antivirus exempt-list	34
config antivirus exempt-list	34
config antivirus profile	35
config antivirus profile	38
config antivirus quarantine	65
config antivirus quarantine	65
config antivirus settings	70
config antivirus settings	70
application	72
config application custom	72
config application custom	72
config application group	73
config application group	73
config application list	74
config application list	76
config application name	83
config application name	83
config application rule-settings	85
config application rule-settings	85
authentication	86
config authentication rule	86
config authentication rule	86
config authentication scheme	89
config authentication scheme	89
config authentication setting	91
config authentication setting	92
automation	95
config automation setting	95
config automation setting	95
casb	96
config casb profile	96
config casb profile	97
config casb saas-application	99
config casb saas-application	99
config casb user-activity	100
config casb user-activity	101

certificate	106
config certificate ca	106
config certificate ca	106
config certificate crt	107
config certificate crt	108
config certificate local	109
config certificate local	110
config certificate remote	113
config certificate remote	114
dlp	115
config dlp data-type	115
config dlp data-type	115
config dlp dictionary	116
config dlp dictionary	117
config dlp exact-data-match	118
config dlp exact-data-match	119
config dlp filepattern	119
config dlp filepattern	120
config dlp fp-doc-source	123
config dlp fp-doc-source	123
config dlp profile	126
config dlp profile	126
config dlp sensitivity	130
config dlp sensitivity	131
config dlp sensor	131
config dlp sensor	131
config dlp settings	132
config dlp settings	133
dnsfilter	134
config dnsfilter domain-filter	134
config dnsfilter domain-filter	134
config dnsfilter profile	135
config dnsfilter profile	136
emailfilter	141
config emailfilter block-allow-list	141
config emailfilter block-allow-list	142
config emailfilter bword	143
config emailfilter bword	144
config emailfilter dnsbl	145
config emailfilter dnsbl	146
config emailfilter fortishield	147
config emailfilter fortishield	147
config emailfilter iptrust	147
config emailfilter iptrust	148
config emailfilter mheader	149
config emailfilter mheader	149

config emailfilter options	150
config emailfilter options	151
config emailfilter profile	151
config emailfilter profile	152
endpoint-control	159
config endpoint-control fctems	159
config endpoint-control fctems	160
file-filter	164
config file-filter profile	164
config file-filter profile	164
firewall	167
config firewall access-proxy-ssh-client-cert	168
config firewall access-proxy-ssh-client-cert	169
config firewall access-proxy-virtual-host	171
config firewall access-proxy-virtual-host	171
config firewall access-proxy	172
config firewall access-proxy	175
config firewall access-proxy6	197
config firewall access-proxy6	197
config firewall address	198
config firewall address	199
config firewall address6-template	203
config firewall address6-template	203
config firewall address6	205
config firewall address6	206
config firewall addrgrp	208
config firewall addrgrp	209
config firewall addrgrp6	210
config firewall addrgrp6	211
config firewall auth-portal	212
config firewall auth-portal	212
config firewall central-snat-map	212
config firewall central-snat-map	213
config firewall city	214
config firewall city	214
config firewall country	214
config firewall country	215
config firewall decrypted-traffic-mirror	215
config firewall decrypted-traffic-mirror	215
config firewall global	216
config firewall global	216
config firewall identity-based-route	217
config firewall identity-based-route	217
config firewall internet-service-addition	218
config firewall internet-service-addition	218
config firewall internet-service-append	219

config firewall internet-service-append	220
config firewall internet-service-botnet	220
config firewall internet-service-botnet	220
config firewall internet-service-custom-group	221
config firewall internet-service-custom-group	221
config firewall internet-service-custom	221
config firewall internet-service-custom	222
config firewall internet-service-definition	223
config firewall internet-service-definition	224
config firewall internet-service-extension	225
config firewall internet-service-extension	226
config firewall internet-service-group	229
config firewall internet-service-group	229
config firewall internet-service-ipbl-reason	229
config firewall internet-service-ipbl-reason	230
config firewall internet-service-ipbl-vendor	230
config firewall internet-service-ipbl-vendor	230
config firewall internet-service-list	230
config firewall internet-service-list	231
config firewall internet-service-name	231
config firewall internet-service-name	231
config firewall internet-service-owner	232
config firewall internet-service-owner	232
config firewall internet-service-reputation	233
config firewall internet-service-reputation	233
config firewall internet-service-sld	233
config firewall internet-service-sld	233
config firewall internet-service-subapp	234
config firewall internet-service-subapp	234
config firewall internet-service	234
config firewall internet-service	235
config firewall ippool	236
config firewall ippool	237
config firewall ippool6	237
config firewall ippool6	237
config firewall network-service-dynamic	238
config firewall network-service-dynamic	238
config firewall policy	239
config firewall policy	241
config firewall profile-group	251
config firewall profile-group	252
config firewall profile-protocol-options	253
config firewall profile-protocol-options	256
config firewall proxy-address	278
config firewall proxy-address	278
config firewall proxy-address6	282

config firewall proxy-address6	283
config firewall proxy-addrgrp	286
config firewall proxy-addrgrp	287
config firewall proxy-addrgrp6	288
config firewall proxy-addrgrp6	288
config firewall region	289
config firewall region	289
config firewall schedule group	289
config firewall schedule group	290
config firewall schedule onetime	290
config firewall schedule onetime	291
config firewall schedule recurring	291
config firewall schedule recurring	292
config firewall service category	292
config firewall service category	293
config firewall service custom	293
config firewall service custom	294
config firewall service group	296
config firewall service group	297
config firewall shaper per-ip-shaper	297
config firewall shaper per-ip-shaper	298
config firewall shaper traffic-shaper	299
config firewall shaper traffic-shaper	300
config firewall shaping-policy	301
config firewall shaping-policy	302
config firewall shaping-profile	305
config firewall shaping-profile	305
config firewall sniffer	306
config firewall sniffer	307
config firewall ssh host-key	308
config firewall ssh host-key	308
config firewall ssh local-ca	309
config firewall ssh local-ca	310
config firewall ssh local-key	310
config firewall ssh local-key	311
config firewall ssh setting	311
config firewall ssh setting	311
config firewall ssl-server	312
config firewall ssl-server	313
config firewall ssl-ssh-profile	315
config firewall ssl-ssh-profile	318
config firewall ssl default-certificate	346
config firewall ssl default-certificate	346
config firewall ssl keyring-list	346
config firewall ssl keyring-list	346
config firewall ssl setting	347

config firewall ssl setting	347
config firewall traffic-class	348
config firewall traffic-class	349
config firewall ttl-policy	349
config firewall ttl-policy	349
config firewall vendor-mac-summary	350
config firewall vendor-mac	350
config firewall vendor-mac	351
config firewall vip	351
config firewall vip	353
config firewall vipgrp	383
config firewall vipgrp	383
config firewall wildcard-fqdn custom	383
config firewall wildcard-fqdn custom	384
config firewall wildcard-fqdn group	384
config firewall wildcard-fqdn group	384
ftp-proxy	386
config ftp-proxy explicit	386
config ftp-proxy explicit	386
hardware	389
config hardware cpu	389
config hardware memory	389
config hardware nic	389
config hardware nic	389
config hardware status	390
icap	391
config icap local-server	391
config icap local-server	392
config icap profile	394
config icap profile	395
config icap remote-server-group	402
config icap remote-server-group	403
config icap remote-server	403
config icap remote-server	404
image-analyzer	406
config image-analyzer profile	406
config image-analyzer profile	407
ips	411
config ips custom	411
config ips custom	411
config ips decoder	413
config ips decoder	413
config ips global	413
config ips global	414
config ips rule-settings	417

config ips rule-settings	417
config ips rule	417
config ips rule	418
config ips sensor	419
config ips sensor	420
config ips session	425
config ips settings	425
config ips settings	425
config ips view-map	426
config ips view-map	426
ipsec	428
config ipsec tunnel	428
isolator	429
config isolator profile	429
config isolator profile	429
config isolator setting	430
config isolator setting	431
log	432
config log custom-field	433
config log custom-field	433
config log disk filter	434
config log disk filter	434
config log disk setting	437
config log disk setting	438
config log eventfilter	442
config log eventfilter	443
config log fortianalyzer-cloud filter	446
config log fortianalyzer-cloud filter	447
config log fortianalyzer-cloud override-filter	450
config log fortianalyzer-cloud override-filter	450
config log fortianalyzer-cloud override-setting	453
config log fortianalyzer-cloud override-setting	453
config log fortianalyzer-cloud setting	454
config log fortianalyzer-cloud setting	454
config log fortianalyzer2 filter	457
config log fortianalyzer2 filter	458
config log fortianalyzer2 override-filter	461
config log fortianalyzer2 override-filter	461
config log fortianalyzer2 override-setting	464
config log fortianalyzer2 override-setting	465
config log fortianalyzer2 setting	468
config log fortianalyzer2 setting	469
config log fortianalyzer3 filter	473
config log fortianalyzer3 filter	473
config log fortianalyzer3 override-filter	476
config log fortianalyzer3 override-filter	477

config log fortianalyzer3 override-setting	480
config log fortianalyzer3 override-setting	480
config log fortianalyzer3 setting	484
config log fortianalyzer3 setting	485
config log fortianalyzer filter	488
config log fortianalyzer filter	489
config log fortianalyzer override-filter	492
config log fortianalyzer override-filter	492
config log fortianalyzer override-setting	495
config log fortianalyzer override-setting	496
config log fortianalyzer setting	499
config log fortianalyzer setting	500
config log fortiguard filter	504
config log fortiguard filter	504
config log fortiguard override-filter	507
config log fortiguard override-filter	508
config log fortiguard override-setting	510
config log fortiguard override-setting	511
config log fortiguard setting	512
config log fortiguard setting	513
config log gui-display	515
config log gui-display	515
config log memory filter	515
config log memory filter	516
config log memory global-setting	519
config log memory global-setting	519
config log memory setting	519
config log memory setting	520
config log null-device filter	520
config log null-device filter	520
config log null-device setting	523
config log null-device setting	523
config log setting	524
config log setting	524
config log syslogd2 filter	528
config log syslogd2 filter	529
config log syslogd2 override-filter	531
config log syslogd2 override-filter	532
config log syslogd2 override-setting	535
config log syslogd2 override-setting	535
config log syslogd2 setting	539
config log syslogd2 setting	540
config log syslogd3 filter	544
config log syslogd3 filter	545
config log syslogd3 override-filter	548
config log syslogd3 override-filter	548

config log syslogd3 override-setting	551
config log syslogd3 override-setting	552
config log syslogd3 setting	556
config log syslogd3 setting	557
config log syslogd4 filter	561
config log syslogd4 filter	561
config log syslogd4 override-filter	564
config log syslogd4 override-filter	565
config log syslogd4 override-setting	568
config log syslogd4 override-setting	568
config log syslogd4 setting	572
config log syslogd4 setting	573
config log syslogd filter	577
config log syslogd filter	578
config log syslogd override-filter	581
config log syslogd override-filter	581
config log syslogd override-setting	584
config log syslogd override-setting	585
config log syslogd setting	589
config log syslogd setting	590
config log tacacs+accounting2 filter	594
config log tacacs+accounting2 filter	594
config log tacacs+accounting2 setting	595
config log tacacs+accounting2 setting	595
config log tacacs+accounting3 filter	596
config log tacacs+accounting3 filter	596
config log tacacs+accounting3 setting	597
config log tacacs+accounting3 setting	597
config log tacacs+accounting filter	598
config log tacacs+accounting filter	598
config log tacacs+accounting setting	599
config log tacacs+accounting setting	599
config log threat-weight	599
config log threat-weight	601
config log webtrends filter	610
config log webtrends filter	611
config log webtrends setting	613
config log webtrends setting	614
mgmt-data	615
config mgmt-data status	615
report	616
config report layout	616
config report layout	617
config report setting	624
config report setting	624
config report sql status	625

router	626
config router policy	626
config router policy	626
config router static	628
config router static	628
config router static6	630
config router static6	630
rule	633
config rule fmwp	633
config rule fmwp	633
ssh-filter	636
config ssh-filter profile	636
config ssh-filter profile	636
system	639
config system accprofile	642
config system accprofile	643
config system acme	652
config system acme	653
config system admin	653
config system admin	655
config system affinity-interrupt	660
config system affinity-interrupt	661
config system affinity-packet-redistribution	661
config system affinity-packet-redistribution	661
config system alarm	662
config system alarm	663
config system alias	665
config system alias	665
config system api-user	665
config system api-user	666
config system arp-table	667
config system arp-table	668
config system arp	668
config system auto-install	668
config system auto-install	668
config system auto-script	669
config system auto-script	669
config system auto-update status	670
config system auto-update versions	671
config system automation-action	671
config system automation-action	672
config system automation-destination	676
config system automation-destination	676
config system automation-stitch	677
config system automation-stitch	677
config system automation-trigger	678

config system automation-trigger	679
config system autoupdate schedule	683
config system autoupdate schedule	683
config system autoupdate tunneling	684
config system autoupdate tunneling	684
config system central-management	685
config system central-management	686
config system central-mgmt	689
config system checksum status	690
config system cmdb	690
config system console	690
config system console	690
config system csf	691
config system csf	692
config system custom-language	697
config system custom-language	697
config system ddns	697
config system ddns	698
config system device-upgrade	700
config system device-upgrade	701
config system dhcp6 server	703
config system dhcp6 server	704
config system dhcp server	706
config system dhcp server	708
config system dns-database	721
config system dns-database	721
config system dns-server	724
config system dns-server	724
config system dns	725
config system dns	726
config system dscp-based-priority	728
config system dscp-based-priority	728
config system email-server	729
config system email-server	729
config system external-resource	731
config system external-resource	732
config system fabric-vpn	734
config system fabric-vpn	735
config system federated-upgrade	738
config system federated-upgrade	738
config system fips-cc	741
config system fips-cc	742
config system fortianalyzer-connectivity	742
config system fortiguard-log-service	742
config system fortiguard-service	742
config system fortiguard	743

config system fortiguard	744
config system fortindr	753
config system fortindr	753
config system fortisandbox	754
config system fortisandbox	754
config system fsso-polling	755
config system fsso-polling	756
config system ftm-push	756
config system ftm-push	757
config system geoip-country	757
config system geoip-country	757
config system geoip-override	758
config system geoip-override	758
config system global	759
config system global	763
config system gre-tunnel	804
config system gre-tunnel	805
config system ha-lic	806
config system ha-lic	807
config system ha-monitor	807
config system ha-monitor	807
config system ha-nonsync-csum	808
config system ha	808
config system ha	810
config system info admin ssh	818
config system info admin status	818
config system interface	818
config system interface	823
config system ip-conflict status	851
config system ipam	851
config system ipam	852
config system ips-urlfilter-dns	853
config system ips-urlfilter-dns	854
config system ips-urlfilter-dns6	854
config system ips-urlfilter-dns6	854
config system ips	855
config system ips	855
config system ipv6-neighbor-cache	855
config system ipv6-neighbor-cache	856
config system link-monitor	856
config system link-monitor	857
config system management-tunnel	861
config system management-tunnel	862
config system mgmt-csum	863
config system nethsm	863
config system nethsm	864

config system network-visibility	866
config system network-visibility	867
config system ntp	868
config system ntp	868
config system object-tagging	871
config system object-tagging	871
config system password-policy-guest-admin	872
config system password-policy-guest-admin	873
config system password-policy	874
config system password-policy	875
config system performance status	876
config system performance top	877
config system performance top	877
config system probe-response	877
config system probe-response	877
config system proxy-arp	878
config system proxy-arp	879
config system ptp	879
config system ptp	879
config system replacemsg-group	881
config system replacemsg-group	883
config system replacemsg-image	893
config system replacemsg-image	894
config system replacemsg admin	894
config system replacemsg admin	894
config system replacemsg alertmail	895
config system replacemsg alertmail	895
config system replacemsg auth	896
config system replacemsg auth	896
config system replacemsg automation	897
config system replacemsg automation	897
config system replacemsg custom-message	898
config system replacemsg custom-message	898
config system replacemsg fortiguard-wf	899
config system replacemsg fortiguard-wf	899
config system replacemsg ftp	899
config system replacemsg ftp	900
config system replacemsg http	900
config system replacemsg http	901
config system replacemsg icap	901
config system replacemsg icap	901
config system replacemsg mail	902
config system replacemsg mail	902
config system replacemsg nac-quar	903
config system replacemsg nac-quar	903
config system replacemsg spam	904

config system replacemsg spam	904
config system replacemsg sslvpn	905
config system replacemsg sslvpn	905
config system replacemsg traffic-quota	906
config system replacemsg traffic-quota	906
config system replacemsg utm	907
config system replacemsg utm	907
config system replacemsg webproxy	907
config system replacemsg webproxy	908
config system resource-limits	908
config system resource-limits	909
config system saml	910
config system saml	911
config system sdn-connector	914
config system sdn-connector	916
config system session-ttl	923
config system session-ttl	923
config system session	924
config system session6	924
config system settings	924
config system settings	926
config system sms-server	938
config system sms-server	939
config system snmp community	939
config system snmp community	940
config system snmp mib-view	945
config system snmp mib-view	946
config system snmp sysinfo	946
config system snmp sysinfo	946
config system snmp user	947
config system snmp user	948
config system source-ip status	953
config system span-port	953
config system span-port	953
config system speed-test-schedule	954
config system speed-test-schedule	954
config system speed-test-server	956
config system speed-test-server	956
config system speed-test-setting	957
config system speed-test-setting	958
config system sso-admin	958
config system sso-admin	958
config system sso-forticloud-admin	958
config system sso-forticloud-admin	959
config system sso-fortigate-cloud-admin	959
config system sso-fortigate-cloud-admin	959

config system startup-error-log	959
config system status	960
config system storage	960
config system storage	960
config system vdom-dns	961
config system vdom-dns	962
config system vdom-exception	963
config system vdom-exception	964
config system vdom-link	966
config system vdom-link	966
config system vdom-property	966
config system vdom-property	967
config system vdom-radius-server	968
config system vdom-radius-server	968
config system vdom	968
config system vdom	969
config system vne-tunnel	969
config system vne-tunnel	969
config system vxlan	970
config system vxlan	971
config system wccp	972
config system wccp	972
config system zone	975
config system zone	976
test	977
config test acd	978
config test acd	979
config test acsd	979
config test acsd	979
config test autod	979
config test autod	979
config test awsd	980
config test awsd	980
config test azd	980
config test azd	980
config test bfd	980
config test bfd	981
config test csfd	981
config test csfd	981
config test ddnsd	981
config test ddnsd	981
config test dhcp6c	981
config test dhcp6c	982
config test dhcp6r	982
config test dhcp6r	982
config test dhcprelay	982

config test dhcprelay	982
config test dlpfingerprint	983
config test dlpfingerprint	983
config test dlpfpcache	983
config test dlpfpcache	983
config test dnsproxy	983
config test dnsproxy	984
config test dsd	984
config test dsd	984
config test eap_supp	984
config test eap_supp	984
config test fas	984
config test fas	985
config test fcnacd	985
config test fcnacd	985
config test fds_notify	985
config test fds_notify	985
config test fgtlogd	986
config test fgtlogd	986
config test fnbamd	986
config test fnbamd	986
config test forticldd	986
config test forticldd	987
config test forticron	987
config test forticron	987
config test fsd	987
config test fsd	987
config test fsvrd	987
config test fsvrd	988
config test gcpd	988
config test gcpd	988
config test harelay	988
config test harelay	988
config test hasync	989
config test hasync	989
config test hataalk	989
config test hataalk	989
config test ibmd	989
config test ibmd	990
config test imap	990
config test imap	990
config test init	990
config test init	990
config test iotd	990
config test iotd	991
config test ipamd	991

config test ipamd	991
config test ipamsd	991
config test ipamsd	991
config test ipdbd	992
config test ipdbd	992
config test ipseengine	992
config test ipseengine	992
config test ipsmonitor	992
config test ipsmonitor	993
config test ipsufd	993
config test ipsufd	993
config test kubed	993
config test kubed	993
config test l2tpcd	993
config test l2tpcd	994
config test lnkmttd	994
config test lnkmttd	994
config test locallogd	994
config test locallogd	994
config test miglogd	995
config test miglogd	995
config test mrd	995
config test mrd	995
config test netxd	995
config test netxd	996
config test nntp	996
config test nntp	996
config test ocid	996
config test ocid	996
config test openstackd	996
config test openstackd	997
config test ovrd	997
config test ovrd	997
config test pop3	997
config test pop3	997
config test pptpcd	998
config test pptpcd	998
config test quarantined	998
config test quarantined	998
config test radius-das	998
config test radius-das	999
config test radiusd	999
config test radiusd	999
config test radvd	999
config test radvd	999
config test reportd	999

config test reportd	1000
config test rt_router	1000
config test rt_router	1000
config test sdncd	1000
config test sdncd	1000
config test sdnd	1001
config test sdnd	1001
config test sepmc	1001
config test sepmc	1001
config test sessionsync	1001
config test sessionsync	1002
config test sfupgraded	1002
config test sfupgraded	1002
config test smtp	1002
config test smtp	1002
config test snmpd	1002
config test snmpd	1003
config test syslogd	1003
config test syslogd	1003
config test updated	1003
config test updated	1003
config test uploadd	1004
config test uploadd	1004
config test urlfilter	1004
config test urlfilter	1004
config test vned	1004
config test vned	1005
config test wad	1005
config test wad	1005
config test wccpd	1005
config test wccpd	1005
config test wf_monitor	1005
config test wf_monitor	1006
config test wiredapd	1006
config test wiredapd	1006
user	1007
config user adgrp	1007
config user adgrp	1008
config user certificate	1008
config user certificate	1008
config user domain-controller	1009
config user domain-controller	1010
config user exchange	1013
config user exchange	1013
config user external-identity-provider	1015
config user external-identity-provider	1016

config user fortitoken	1017
config user fortitoken	1017
config user fsso-polling	1018
config user fsso-polling	1019
config user fsso	1020
config user fsso	1021
config user group	1024
config user group	1025
config user krb-keytab	1029
config user krb-keytab	1029
config user ldap	1030
config user ldap	1031
config user local	1037
config user local	1038
config user password-policy	1041
config user password-policy	1041
config user peer	1042
config user peer	1042
config user peergrp	1044
config user peergrp	1044
config user pop3	1044
config user pop3	1044
config user radius	1045
config user radius	1047
config user saml	1058
config user saml	1059
config user security-exempt-list	1062
config user security-exempt-list	1062
config user setting	1063
config user setting	1064
config user tacacs+	1067
config user tacacs+	1068
videofilter	1070
config videofilter profile	1070
config videofilter profile	1070
config videofilter youtube-channel-filter	1072
config videofilter youtube-channel-filter	1073
config videofilter youtube-key	1074
config videofilter youtube-key	1074
vpn	1075
config vpn certificate ca	1075
config vpn certificate ca	1075
config vpn certificate crt	1077
config vpn certificate crt	1077
config vpn certificate local	1078
config vpn certificate local	1079

config vpn certificate ocsdp-server	1082
config vpn certificate ocsdp-server	1083
config vpn certificate remote	1083
config vpn certificate remote	1084
config vpn certificate setting	1084
config vpn certificate setting	1085
config vpn ipsec phase1-interface	1089
config vpn ipsec phase1-interface	1091
config vpn ipsec phase2-interface	1104
config vpn ipsec phase2-interface	1105
waf	1113
config waf main-class	1113
config waf main-class	1113
config waf profile	1113
config waf profile	1117
config waf signature	1138
config waf signature	1138
config waf sub-class	1139
config waf sub-class	1139
wanopt	1140
config wanopt auth-group	1140
config wanopt auth-group	1140
config wanopt cache-service	1141
config wanopt cache-service	1142
config wanopt content-delivery-network-rule	1143
config wanopt content-delivery-network-rule	1144
config wanopt peer	1148
config wanopt peer	1149
config wanopt profile	1149
config wanopt profile	1150
config wanopt remote-storage	1157
config wanopt remote-storage	1157
config wanopt settings	1157
config wanopt settings	1158
web-proxy	1159
config web-proxy debug-url	1159
config web-proxy debug-url	1159
config web-proxy dynamic-bypass	1160
config web-proxy dynamic-bypass	1160
config web-proxy explicit-proxy	1161
config web-proxy explicit-proxy	1162
config web-proxy forward-server-group	1167
config web-proxy forward-server-group	1167
config web-proxy forward-server	1168
config web-proxy forward-server	1169
config web-proxy global	1170

config web-proxy global	1171
config web-proxy implicit-proxy-rule	1175
config web-proxy implicit-proxy-rule	1176
config web-proxy implicit-proxy-setting	1177
config web-proxy implicit-proxy-setting	1177
config web-proxy isolator-server	1177
config web-proxy isolator-server	1178
config web-proxy pac-policy	1179
config web-proxy pac-policy	1179
config web-proxy profile	1180
config web-proxy profile	1180
config web-proxy redirect-profile	1184
config web-proxy redirect-profile	1185
config web-proxy url-list	1185
config web-proxy url-list	1186
config web-proxy url-match	1187
config web-proxy url-match	1187
config web-proxy wisp	1188
config web-proxy wisp	1188
webcache	1190
config webcache prefetch	1190
config webcache prefetch	1190
config webcache reverse-cache-server	1191
config webcache reverse-cache-server	1192
config webcache settings	1192
config webcache settings	1193
config webcache user-agent	1196
config webcache user-agent	1196
webfilter	1197
config webfilter categories	1197
config webfilter content-header	1197
config webfilter content-header	1198
config webfilter content	1199
config webfilter content	1199
config webfilter domain-list	1200
config webfilter domain-list	1201
config webfilter fortiguard	1201
config webfilter fortiguard	1202
config webfilter ftgd-local-cat	1204
config webfilter ftgd-local-cat	1204
config webfilter ftgd-local-rating	1204
config webfilter ftgd-local-rating	1205
config webfilter ftgd-local-risk	1205
config webfilter ftgd-local-risk	1205
config webfilter ftgd-risk-level	1206
config webfilter ftgd-risk-level	1206

config webfilter ftgd-statistics	1206
config webfilter ips-urlfilter-cache-setting	1207
config webfilter ips-urlfilter-cache-setting	1207
config webfilter ips-urlfilter-setting	1207
config webfilter ips-urlfilter-setting	1207
config webfilter ips-urlfilter-setting6	1208
config webfilter ips-urlfilter-setting6	1208
config webfilter override-usr	1209
config webfilter override	1209
config webfilter override	1209
config webfilter profile	1210
config webfilter profile	1213
config webfilter search-engine	1227
config webfilter search-engine	1228
config webfilter status	1229
config webfilter status	1229
config webfilter url-list	1229
config webfilter url-list	1230
config webfilter urlfilter	1230
config webfilter urlfilter	1231

Change log

Date	Change Description
2024-12-13	Initial release.

FortiProxy CLI Interface

This document describes FortiProxy 7.4.7 CLI commands that are used to configure and manage FortiProxy from the command line interface (CLI). For information on using the CLI, see the [FortiProxy 7.4.7 Administration Guide](#).

alertemail

This section includes syntax for the following commands:

- [config alertemail setting on page 27](#)

config alertemail setting

Configure alert email settings.

```
config alertemail setting
    Description: Configure alert email settings.
    set username {string}
    set mailto1 {string}
    set mailto2 {string}
    set mailto3 {string}
    set filter-mode [category|threshold]
    set email-interval {integer}
    set IPS-logs [enable|disable]
    set firewall-authentication-failure-logs [enable|disable]
    set HA-logs [enable|disable]
    set IPsec-errors-logs [enable|disable]
    set FDS-update-logs [enable|disable]
    set PPP-errors-logs [enable|disable]
    set antivirus-logs [enable|disable]
    set webfilter-logs [enable|disable]
    set configuration-changes-logs [enable|disable]
    set violation-traffic-logs [enable|disable]
    set admin-login-logs [enable|disable]
    set FDS-license-expiring-warning [enable|disable]
    set log-disk-usage-warning [enable|disable]
    set fortiguard-log-quota-warning [enable|disable]
    set amc-interface-bypass-mode [enable|disable]
    set FIPS-CC-errors [enable|disable]
    set FSSO-disconnect-logs [enable|disable]
    set ssh-logs [enable|disable]
    set fpx-license-logs [enable|disable]
    set FDS-license-expiring-days {integer}
    set local-disk-usage {integer}
    set emergency-interval {integer}
    set alert-interval {integer}
    set critical-interval {integer}
    set error-interval {integer}
    set warning-interval {integer}
    set notification-interval {integer}
    set information-interval {integer}
    set debug-interval {integer}
    set severity [emergency|alert|...]
end
```

config alertemail setting

Parameter	Description	Type	Size	Default						
username	Name that appears in the From: field of alert emails (max. 63 characters).	string	Maximum length: 63							
mailto1	Email address to send alert email to (usually a system administrator) (max. 63 characters).	string	Maximum length: 63							
mailto2	Optional second email address to send alert email to (max. 63 characters).	string	Maximum length: 63							
mailto3	Optional third email address to send alert email to (max. 63 characters).	string	Maximum length: 63							
filter-mode	How to filter log messages that are sent to alert emails.	option	-	category						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>category</td><td>Filter based on category.</td></tr><tr><td>threshold</td><td>Filter based on severity.</td></tr></table>				Option	Description	category	Filter based on category.	threshold	Filter based on severity.
Option	Description									
category	Filter based on category.									
threshold	Filter based on severity.									
email-interval	Interval between sending alert emails.	integer	Minimum value: 1 Maximum value: 99999	5						
IPS-logs	Enable/disable IPS logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IPS logs in alert email.</td></tr><tr><td>disable</td><td>Disable IPS logs in alert email.</td></tr></table>				Option	Description	enable	Enable IPS logs in alert email.	disable	Disable IPS logs in alert email.
Option	Description									
enable	Enable IPS logs in alert email.									
disable	Disable IPS logs in alert email.									
firewall-authentication-failure-logs	Enable/disable firewall authentication failure logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable firewall authentication failure logs in alert email.</td></tr><tr><td>disable</td><td>Disable firewall authentication failure logs in alert email.</td></tr></table>				Option	Description	enable	Enable firewall authentication failure logs in alert email.	disable	Disable firewall authentication failure logs in alert email.
Option	Description									
enable	Enable firewall authentication failure logs in alert email.									
disable	Disable firewall authentication failure logs in alert email.									
HA-logs	Enable/disable HA logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable HA logs in alert email.</td></tr><tr><td>disable</td><td>Disable HA logs in alert email.</td></tr></table>				Option	Description	enable	Enable HA logs in alert email.	disable	Disable HA logs in alert email.
Option	Description									
enable	Enable HA logs in alert email.									
disable	Disable HA logs in alert email.									

Parameter	Description	Type	Size	Default						
IPsec-errors-logs	Enable/disable IPsec error logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPsec error logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable IPsec error logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPsec error logs in alert email.	<i>disable</i>	Disable IPsec error logs in alert email.			
Option	Description									
<i>enable</i>	Enable IPsec error logs in alert email.									
<i>disable</i>	Disable IPsec error logs in alert email.									
FDS-update-logs	Enable/disable FortiGuard update logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiGuard update logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable FortiGuard update logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiGuard update logs in alert email.	<i>disable</i>	Disable FortiGuard update logs in alert email.			
Option	Description									
<i>enable</i>	Enable FortiGuard update logs in alert email.									
<i>disable</i>	Disable FortiGuard update logs in alert email.									
PPP-errors-logs	Enable/disable PPP error logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable PPP error logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable PPP error logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable PPP error logs in alert email.	<i>disable</i>	Disable PPP error logs in alert email.			
Option	Description									
<i>enable</i>	Enable PPP error logs in alert email.									
<i>disable</i>	Disable PPP error logs in alert email.									
antivirus-logs	Enable/disable antivirus logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable antivirus logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable antivirus logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable antivirus logs in alert email.	<i>disable</i>	Disable antivirus logs in alert email.			
Option	Description									
<i>enable</i>	Enable antivirus logs in alert email.									
<i>disable</i>	Disable antivirus logs in alert email.									
webfilter-logs	Enable/disable web filter logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable web filter logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable web filter logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable web filter logs in alert email.	<i>disable</i>	Disable web filter logs in alert email.			
Option	Description									
<i>enable</i>	Enable web filter logs in alert email.									
<i>disable</i>	Disable web filter logs in alert email.									
configuration-changes-logs	Enable/disable configuration change logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable configuration change logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable configuration change logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable configuration change logs in alert email.	<i>disable</i>	Disable configuration change logs in alert email.			
Option	Description									
<i>enable</i>	Enable configuration change logs in alert email.									
<i>disable</i>	Disable configuration change logs in alert email.									
violation-traffic-logs	Enable/disable violation traffic logs in alert email.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable violation traffic logs in alert email.		
	<i>disable</i>	Disable violation traffic logs in alert email.		
admin-login-logs	Enable/disable administrator login/logout logs in alert email.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable administrator login/logout logs in alert email.		
	<i>disable</i>	Disable administrator login/logout logs in alert email.		
FDS-license-expiring-warning	Enable/disable FortiGuard license expiration warnings in alert email.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FortiGuard license expiration warnings in alert email.		
	<i>disable</i>	Disable FortiGuard license expiration warnings in alert email.		
log-disk-usage-warning	Enable/disable disk usage warnings in alert email.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable disk usage warnings in alert email.		
	<i>disable</i>	Disable disk usage warnings in alert email.		
fortiguard-log-quota-warning	Enable/disable FortiCloud log quota warnings in alert email.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FortiCloud log quota warnings in alert email.		
	<i>disable</i>	Disable FortiCloud log quota warnings in alert email.		
amc-interface-bypass-mode	Enable/disable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert email.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert email.		
	<i>disable</i>	Disable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert email.		

Parameter	Description	Type	Size	Default
FIPS-CC-errors	Enable/disable FIPS and Common Criteria error logs in alert email.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FIPS and Common Criteria error logs in alert email.		
	<i>disable</i>	Disable FIPS and Common Criteria error logs in alert email.		
FSSO-disconnect-logs	Enable/disable logging of FSSO collector agent disconnect.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging of FSSO collector agent disconnect.		
	<i>disable</i>	Disable logging of FSSO collector agent disconnect.		
ssh-logs	Enable/disable SSH logs in alert email.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable SSH logs in alert email.		
	<i>disable</i>	Disable SSH logs in alert email.		
fpx-license-logs	Enable/disable FortiProxy license related logs in alert email.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FortiProxy license related warnings in alert email.		
	<i>disable</i>	Disable FortiProxy license related warnings in alert email.		
FDS-license-expiring-days	Number of days to send alert email prior to FortiGuard license expiration.	integer	Minimum value: 1 Maximum value: 100	15
local-disk-usage	Disk usage percentage at which to send alert email.	integer	Minimum value: 1 Maximum value: 99	75
emergency-interval	Emergency alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	1

Parameter	Description	Type	Size	Default
alert-interval	Alert alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	2
critical-interval	Critical alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	3
error-interval	Error alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	5
warning-interval	Warning alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	10
notification-interval	Notification alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	20
information-interval	Information alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	30
debug-interval	Debug alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	60
severity	Lowest severity level to log.	option	-	alert
	Option	Description		
	emergency	Emergency level.		
	alert	Alert level.		

Parameter	Description		Type	Size	Default
	Option	Description			
	<i>critical</i>	Critical level.			
	<i>error</i>	Error level.			
	<i>warning</i>	Warning level.			
	<i>notification</i>	Notification level.			
	<i>information</i>	Information level.			
	<i>debug</i>	Debug level.			

antivirus

This section includes syntax for the following commands:

- [config antivirus exempt-list on page 34](#)
- [config antivirus profile on page 35](#)
- [config antivirus quarantine on page 65](#)
- [config antivirus settings on page 70](#)

config antivirus exempt-list

Configure a list of hashes to be exempt from AV scanning.

```
config antivirus exempt-list
  Description: Configure a list of hashes to be exempt from AV scanning.
  edit <name>
    set comment {var-string}
    set hash-type [md5|sha1|...]
    set hash {string}
    set status [disable|enable]
  next
end
```

config antivirus exempt-list

Parameter	Description	Type	Size	Default
name	Table entry name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
hash-type	Hash type.	option	-	sha1
	Option		Description	
	<i>md5</i>		MD5 hash value (32 characters in length).	
	<i>sha1</i>		SHA1 hash value (40 characters in length).	
	<i>sha256</i>		SHA256 hash value (64 characters in length).	
hash	Hash value to be matched.	string	Maximum length: 64	

Parameter	Description	Type	Size	Default
status	Enable/disable table entry.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable AV exempt-list table entry.		
	<i>enable</i>	Enable AV exempt-list table entry.		

config antivirus profile

Configure AntiVirus profiles.

```
config antivirus profile
  Description: Configure AntiVirus profiles.
  edit <name>
    set comment {var-string}
    set replacemsg-group {string}
    set fortisandbox-mode [inline|analytics-suspicious|...]
    set fortisandbox-max-upload {integer}
    set analytics-ignore-filetype {integer}
    set analytics-accept-filetype {integer}
    set analytics-db [disable|enable]
    set mobile-malware-db [disable|enable]
    config http
      Description: Configure HTTP AntiVirus options.
      set av-scan [disable|block|...]
      set outbreak-prevention [disable|block|...]
      set external-blocklist [disable|block|...]
      set fortindr [disable|block|...]
      set fortisandbox [disable|block|...]
      set quarantine [disable|enable]
      set archive-block {option1}, {option2}, ...
      set archive-log {option1}, {option2}, ...
      set emulator [enable|disable]
      set content-disarm [disable|enable]
    end
    config ftp
      Description: Configure FTP AntiVirus options.
      set av-scan [disable|block|...]
      set outbreak-prevention [disable|block|...]
      set external-blocklist [disable|block|...]
      set fortindr [disable|block|...]
      set fortisandbox [disable|block|...]
      set quarantine [disable|enable]
      set archive-block {option1}, {option2}, ...
      set archive-log {option1}, {option2}, ...
      set emulator [enable|disable]
    end
    config imap
      Description: Configure IMAP AntiVirus options.
      set av-scan [disable|block|...]
```

```
    set outbreak-prevention [disable|block|...]
    set external-blocklist [disable|block|...]
    set fortindr [disable|block|...]
    set fortisandbox [disable|block|...]
    set quarantine [disable|enable]
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
    set executables [default|virus]
    set content-disarm [disable|enable]
end
config pop3
    Description: Configure POP3 AntiVirus options.
    set av-scan [disable|block|...]
    set outbreak-prevention [disable|block|...]
    set external-blocklist [disable|block|...]
    set fortindr [disable|block|...]
    set fortisandbox [disable|block|...]
    set quarantine [disable|enable]
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
    set executables [default|virus]
    set content-disarm [disable|enable]
end
config smtp
    Description: Configure SMTP AntiVirus options.
    set av-scan [disable|block|...]
    set outbreak-prevention [disable|block|...]
    set external-blocklist [disable|block|...]
    set fortindr [disable|block|...]
    set fortisandbox [disable|block|...]
    set quarantine [disable|enable]
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
    set executables [default|virus]
    set content-disarm [disable|enable]
end
config mapi
    Description: Configure MAPI AntiVirus options.
    set av-scan [disable|block|...]
    set outbreak-prevention [disable|block|...]
    set external-blocklist [disable|block|...]
    set fortindr [disable|block|...]
    set fortisandbox [disable|block|...]
    set quarantine [disable|enable]
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
    set executables [default|virus]
end
config nntp
    Description: Configure NNTP AntiVirus options.
    set av-scan [disable|block|...]
    set outbreak-prevention [disable|block|...]
```

```
    set external-blocklist [disable|block|...]
    set fortindr [disable|block|...]
    set fortisandbox [disable|block|...]
    set quarantine [disable|enable]
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
end
config cifs
    Description: Configure CIFS AntiVirus options.
    set av-scan [disable|block|...]
    set outbreak-prevention [disable|block|...]
    set external-blocklist [disable|block|...]
    set fortindr [disable|block|...]
    set fortisandbox [disable|block|...]
    set quarantine [disable|enable]
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
end
config ssh
    Description: Configure SFTP and SCP AntiVirus options.
    set av-scan [disable|block|...]
    set outbreak-prevention [disable|block|...]
    set external-blocklist [disable|block|...]
    set fortindr [disable|block|...]
    set fortisandbox [disable|block|...]
    set quarantine [disable|enable]
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
end
config nac-quar
    Description: Configure AntiVirus quarantine settings.
    set infected [none|quar-src-ip]
    set expiry {user}
    set log [enable|disable]
end
config content-disarm
    Description: AV Content Disarm and Reconstruction settings.
    set original-file-destination [fortisandbox|quarantine|...]
    set error-action [block|log-only|...]
    set office-macro [disable|enable]
    set office-hylink [disable|enable]
    set office-linked [disable|enable]
    set office-embed [disable|enable]
    set office-dde [disable|enable]
    set office-action [disable|enable]
    set pdf-javacode [disable|enable]
    set pdf-embedfile [disable|enable]
    set pdf-hyperlink [disable|enable]
    set pdf-act-gotor [disable|enable]
    set pdf-act-launch [disable|enable]
    set pdf-act-sound [disable|enable]
    set pdf-act-movie [disable|enable]
    set pdf-act-java [disable|enable]
```

```

        set pdf-act-form [disable|enable]
        set cover-page [disable|enable]
        set detect-only [disable|enable]
    end
    set outbreak-prevention-archive-scan [disable|enable]
    set external-blocklist-enable-all [disable|enable]
    set external-blocklist <name1>, <name2>, ...
    set ems-threat-feed [disable|enable]
    set fortindr-error-action [log-only|block|...]
    set fortindr-timeout-action [log-only|block|...]
    set fortisandbox-error-action [log-only|block|...]
    set fortisandbox-timeout-action [log-only|block|...]
    set av-virus-log [enable|disable]
    set av-block-log [enable|disable]
    set scan-mode [default|legacy]
next
end

```

config antivirus profile

Parameter	Description	Type	Size	Default								
name	Profile name.	string	Maximum length: 35									
comment	Comment.	var-string	Maximum length: 255									
replacemsg-group	Replacement message group customized for this profile.	string	Maximum length: 35									
fortisandbox-mode	FortiSandbox scan modes.	option	-	analytics-everything								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>inline</i></td><td>FortiSandbox inline scan.</td></tr><tr><td><i>analytics-suspicious</i></td><td>FortiSandbox post-transfer scan: submit supported files if heuristics or other methods determine they are suspicious.</td></tr><tr><td><i>analytics-everything</i></td><td>FortiSandbox post-transfer scan: submit supported files and known infected files.</td></tr></table>				Option	Description	<i>inline</i>	FortiSandbox inline scan.	<i>analytics-suspicious</i>	FortiSandbox post-transfer scan: submit supported files if heuristics or other methods determine they are suspicious.	<i>analytics-everything</i>	FortiSandbox post-transfer scan: submit supported files and known infected files.
	Option	Description										
	<i>inline</i>	FortiSandbox inline scan.										
	<i>analytics-suspicious</i>	FortiSandbox post-transfer scan: submit supported files if heuristics or other methods determine they are suspicious.										
<i>analytics-everything</i>	FortiSandbox post-transfer scan: submit supported files and known infected files.											
fortisandbox-max-upload	Maximum size of files that can be uploaded to FortiSandbox.	integer	Minimum value: 1 Maximum value: 26214	10								

Parameter	Description	Type	Size	Default						
analytics-ignore-filetype	Do not submit files matching this DLP file-pattern to FortiSandbox (post-transfer scan only).	integer	Minimum value: 0 Maximum value: 4294967295	0						
analytics-accept-filetype	Only submit files matching this DLP file-pattern to FortiSandbox (post-transfer scan only).	integer	Minimum value: 0 Maximum value: 4294967295	0						
analytics-db	Enable/disable using the FortiSandbox signature database to supplement the AV signature databases.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Use only the standard AV signature databases.</td></tr><tr><td>enable</td><td>Also use the FortiSandbox signature database.</td></tr></table>	Option	Description	disable	Use only the standard AV signature databases.	enable	Also use the FortiSandbox signature database.			
Option	Description									
disable	Use only the standard AV signature databases.									
enable	Also use the FortiSandbox signature database.									
mobile-malware-db	Enable/disable using the mobile malware signature database.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not use the mobile malware signature database.</td></tr><tr><td>enable</td><td>Also use the mobile malware signature database.</td></tr></table>	Option	Description	disable	Do not use the mobile malware signature database.	enable	Also use the mobile malware signature database.			
Option	Description									
disable	Do not use the mobile malware signature database.									
enable	Also use the mobile malware signature database.									
outbreak-prevention-archive-scan	Enable/disable outbreak-prevention archive scanning.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Analyze files as sent, not the content of archives.</td></tr><tr><td>enable</td><td>Analyze files including the content of archives.</td></tr></table>	Option	Description	disable	Analyze files as sent, not the content of archives.	enable	Analyze files including the content of archives.			
Option	Description									
disable	Analyze files as sent, not the content of archives.									
enable	Analyze files including the content of archives.									
external-blocklist-enable-all	Enable/disable all external blocklists.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Use configured external blocklists.</td></tr><tr><td>enable</td><td>Enable all external blocklists.</td></tr></table>	Option	Description	disable	Use configured external blocklists.	enable	Enable all external blocklists.			
Option	Description									
disable	Use configured external blocklists.									
enable	Enable all external blocklists.									

Parameter	Description	Type	Size	Default								
external-blocklist <name>	One or more external malware block lists. External blocklist.	string	Maximum length: 79									
ems-threat-feed	Enable/disable use of EMS threat feed when performing AntiVirus scan. Analyzes files including the content of archives.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable use of EMS threat feed when performing AntiVirus scan.</td></tr><tr><td>enable</td><td>Enable use of EMS threat feed when performing AntiVirus scan.</td></tr></table>	Option	Description	disable	Disable use of EMS threat feed when performing AntiVirus scan.	enable	Enable use of EMS threat feed when performing AntiVirus scan.					
Option	Description											
disable	Disable use of EMS threat feed when performing AntiVirus scan.											
enable	Enable use of EMS threat feed when performing AntiVirus scan.											
fortindr-error-action	Action to take if FortiNDR encounters an error.	option	-	log-only								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>log-only</td><td>Log FortiNDR error, but allow the file.</td></tr><tr><td>block</td><td>Block the file on FortiNDR error.</td></tr><tr><td>ignore</td><td>Do nothing on FortiNDR error.</td></tr></table>	Option	Description	log-only	Log FortiNDR error, but allow the file.	block	Block the file on FortiNDR error.	ignore	Do nothing on FortiNDR error.			
Option	Description											
log-only	Log FortiNDR error, but allow the file.											
block	Block the file on FortiNDR error.											
ignore	Do nothing on FortiNDR error.											
fortindr-timeout-action	Action to take if FortiNDR encounters a scan timeout.	option	-	log-only								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>log-only</td><td>Log FortiNDR scan timeout, but allow the file.</td></tr><tr><td>block</td><td>Block the file on FortiNDR scan timeout.</td></tr><tr><td>ignore</td><td>Do nothing on FortiNDR scan timeout.</td></tr></table>	Option	Description	log-only	Log FortiNDR scan timeout, but allow the file.	block	Block the file on FortiNDR scan timeout.	ignore	Do nothing on FortiNDR scan timeout.			
Option	Description											
log-only	Log FortiNDR scan timeout, but allow the file.											
block	Block the file on FortiNDR scan timeout.											
ignore	Do nothing on FortiNDR scan timeout.											
fortisandbox-error-action	Action to take if FortiSandbox inline scan encounters an error.	option	-	log-only								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>log-only</td><td>Log FortiSandbox inline scan error, but allow the file.</td></tr><tr><td>block</td><td>Block the file on FortiSandbox inline scan error.</td></tr><tr><td>ignore</td><td>Do nothing on FortiSandbox inline scan error.</td></tr></table>	Option	Description	log-only	Log FortiSandbox inline scan error, but allow the file.	block	Block the file on FortiSandbox inline scan error.	ignore	Do nothing on FortiSandbox inline scan error.			
Option	Description											
log-only	Log FortiSandbox inline scan error, but allow the file.											
block	Block the file on FortiSandbox inline scan error.											
ignore	Do nothing on FortiSandbox inline scan error.											
fortisandbox-timeout-action	Action to take if FortiSandbox inline scan encounters a scan timeout.	option	-	log-only								

Parameter	Description	Type	Size	Default
	Option Description			
	<i>log-only</i>	Log FortiSandbox inline scan timeout, but allow the file.		
	<i>block</i>	Block the file on FortiSandbox inline scan timeout.		
	<i>ignore</i>	Do nothing on FortiSandbox inline scan timeout.		
av-virus-log	Enable/disable AntiVirus logging.	option	-	enable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
av-block-log	Enable/disable logging for AntiVirus file blocking.	option	-	enable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
scan-mode	Configure scan mode.	option	-	default
	Option Description			
	<i>default</i>	On the fly decompression and scanning of certain archive files.		
	<i>legacy</i>	Scan archive files only after the entire file is received.		

config http

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option Description			
	<i>disable</i>	Disable.		
	<i>block</i>	Block the virus infected files.		
	<i>monitor</i>	Log the virus infected files.		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	Option Description			
	<i>disable</i>	Disable.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Block the matched files.</td></tr><tr><td><i>monitor</i></td><td>Log the matched files.</td></tr></table>	Option	Description	<i>block</i>	Block the matched files.	<i>monitor</i>	Log the matched files.					
	Option	Description										
	<i>block</i>	Block the matched files.										
<i>monitor</i>	Log the matched files.											
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the matched files.</td></tr><tr><td><i>monitor</i></td><td>Log the matched files.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the matched files.	<i>monitor</i>	Log the matched files.			
	Option	Description										
	<i>disable</i>	Disable.										
	<i>block</i>	Block the matched files.										
<i>monitor</i>	Log the matched files.											
fortindr	Enable scanning of files by FortiNDR.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the FortiNDR detected infections.</td></tr><tr><td><i>monitor</i></td><td>Log the FortiNDR detected infections.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the FortiNDR detected infections.	<i>monitor</i>	Log the FortiNDR detected infections.			
	Option	Description										
	<i>disable</i>	Disable.										
	<i>block</i>	Block the FortiNDR detected infections.										
<i>monitor</i>	Log the FortiNDR detected infections.											
fortisandbox	Enable scanning of files by FortiSandbox.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the FortiSandbox detected infections.</td></tr><tr><td><i>monitor</i></td><td>Log the FortiSandbox detected infections.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the FortiSandbox detected infections.	<i>monitor</i>	Log the FortiSandbox detected infections.			
	Option	Description										
	<i>disable</i>	Disable.										
	<i>block</i>	Block the FortiSandbox detected infections.										
<i>monitor</i>	Log the FortiSandbox detected infections.											
quarantine	Enable/disable quarantine for infected files.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable quarantine for infected files.</td></tr><tr><td><i>enable</i></td><td>Enable quarantine for infected files.</td></tr></table>	Option	Description	<i>disable</i>	Disable quarantine for infected files.	<i>enable</i>	Enable quarantine for infected files.					
	Option	Description										
	<i>disable</i>	Disable quarantine for infected files.										
<i>enable</i>	Enable quarantine for infected files.											
archive-block	Select the archive types to block.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Block encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Block corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Block partially corrupted archives.</td></tr></table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.			
	Option	Description										
	<i>encrypted</i>	Block encrypted archives.										
	<i>corrupted</i>	Block corrupted archives.										
<i>partiallycorrupted</i>	Block partially corrupted archives.											

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>multipart</i></td><td>Block multipart archives.</td></tr><tr><td><i>nested</i></td><td>Block nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Block mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Block scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Block archives that FortiProxy cannot open.</td></tr></table>	Option	Description	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Block mail bomb archives.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiProxy cannot open.									
	Option	Description																				
	<i>multipart</i>	Block multipart archives.																				
	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.																				
	<i>mailbomb</i>	Block mail bomb archives.																				
	<i>timeout</i>	Block scan timeout.																				
<i>unhandled</i>	Block archives that FortiProxy cannot open.																					
archive-log	Select the archive types to log.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Log encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Log corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Log partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Log multipart archives.</td></tr><tr><td><i>nested</i></td><td>Log nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Log mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Log scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Log archives that FortiProxy cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Log mail bomb archives.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiProxy cannot open.			
	Option	Description																				
	<i>encrypted</i>	Log encrypted archives.																				
	<i>corrupted</i>	Log corrupted archives.																				
	<i>partiallycorrupted</i>	Log partially corrupted archives.																				
	<i>multipart</i>	Log multipart archives.																				
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.																				
	<i>mailbomb</i>	Log mail bomb archives.																				
	<i>timeout</i>	Log scan timeout.																				
<i>unhandled</i>	Log archives that FortiProxy cannot open.																					
emulator	Enable/disable the virus emulator.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the virus emulator.</td></tr><tr><td><i>disable</i></td><td>Disable the virus emulator.</td></tr></table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.															
	Option	Description																				
	<i>enable</i>	Enable the virus emulator.																				
<i>disable</i>	Disable the virus emulator.																					
content-disarm	Enable/disable Content Disarm and Reconstruction when performing AntiVirus scan.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Content Disarm and Reconstruction when performing AntiVirus scan.</td></tr><tr><td><i>enable</i></td><td>Enable Content Disarm and Reconstruction when performing AntiVirus scan.</td></tr></table>	Option	Description	<i>disable</i>	Disable Content Disarm and Reconstruction when performing AntiVirus scan.	<i>enable</i>	Enable Content Disarm and Reconstruction when performing AntiVirus scan.															
	Option	Description																				
<i>disable</i>	Disable Content Disarm and Reconstruction when performing AntiVirus scan.																					
<i>enable</i>	Enable Content Disarm and Reconstruction when performing AntiVirus scan.																					

config ftp

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable

Parameter	Description	Type	Size	Default
	Option Description			
	<i>disable</i>	Disable.		
	<i>block</i>	Block the virus infected files.		
	<i>monitor</i>	Log the virus infected files.		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	Option Description			
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable
	Option Description			
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
fortindr	Enable scanning of files by FortiNDR.	option	-	disable
	Option Description			
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiNDR detected infections.		
	<i>monitor</i>	Log the FortiNDR detected infections.		
fortisandbox	Enable scanning of files by FortiSandbox.	option	-	disable
	Option Description			
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiSandbox detected infections.		
	<i>monitor</i>	Log the FortiSandbox detected infections.		
quarantine	Enable/disable quarantine for infected files.	option	-	disable

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable quarantine for infected files.</td></tr><tr><td><i>enable</i></td><td>Enable quarantine for infected files.</td></tr></table>	Option	Description	<i>disable</i>	Disable quarantine for infected files.	<i>enable</i>	Enable quarantine for infected files.															
	Option	Description																				
	<i>disable</i>	Disable quarantine for infected files.																				
<i>enable</i>	Enable quarantine for infected files.																					
archive-block	Select the archive types to block.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Block encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Block corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Block partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Block multipart archives.</td></tr><tr><td><i>nested</i></td><td>Block nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Block mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Block scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Block archives that FortiProxy cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Block mail bomb archives.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiProxy cannot open.			
	Option	Description																				
	<i>encrypted</i>	Block encrypted archives.																				
	<i>corrupted</i>	Block corrupted archives.																				
	<i>partiallycorrupted</i>	Block partially corrupted archives.																				
	<i>multipart</i>	Block multipart archives.																				
	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.																				
	<i>mailbomb</i>	Block mail bomb archives.																				
	<i>timeout</i>	Block scan timeout.																				
<i>unhandled</i>	Block archives that FortiProxy cannot open.																					
archive-log	Select the archive types to log.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Log encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Log corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Log partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Log multipart archives.</td></tr><tr><td><i>nested</i></td><td>Log nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Log mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Log scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Log archives that FortiProxy cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Log mail bomb archives.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiProxy cannot open.			
	Option	Description																				
	<i>encrypted</i>	Log encrypted archives.																				
	<i>corrupted</i>	Log corrupted archives.																				
	<i>partiallycorrupted</i>	Log partially corrupted archives.																				
	<i>multipart</i>	Log multipart archives.																				
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.																				
	<i>mailbomb</i>	Log mail bomb archives.																				
	<i>timeout</i>	Log scan timeout.																				
<i>unhandled</i>	Log archives that FortiProxy cannot open.																					
emulator	Enable/disable the virus emulator.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the virus emulator.</td></tr><tr><td><i>disable</i></td><td>Disable the virus emulator.</td></tr></table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.															
	Option	Description																				
	<i>enable</i>	Enable the virus emulator.																				
<i>disable</i>	Disable the virus emulator.																					

config imap

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the virus infected files.		
	<i>monitor</i>	Log the virus infected files.		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
fortindr	Enable scanning of files by FortiNDR.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiNDR detected infections.		
	<i>monitor</i>	Log the FortiNDR detected infections.		
fortisandbox	Enable scanning of files by FortiSandbox.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiSandbox detected infections.		
	<i>monitor</i>	Log the FortiSandbox detected infections.		
quarantine	Enable/disable quarantine for infected files.	option	-	disable

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable quarantine for infected files.</td></tr><tr><td><i>enable</i></td><td>Enable quarantine for infected files.</td></tr></table>	Option	Description	<i>disable</i>	Disable quarantine for infected files.	<i>enable</i>	Enable quarantine for infected files.															
	Option	Description																				
	<i>disable</i>	Disable quarantine for infected files.																				
<i>enable</i>	Enable quarantine for infected files.																					
archive-block	Select the archive types to block.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Block encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Block corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Block partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Block multipart archives.</td></tr><tr><td><i>nested</i></td><td>Block nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Block mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Block scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Block archives that FortiProxy cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Block mail bomb archives.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiProxy cannot open.			
	Option	Description																				
	<i>encrypted</i>	Block encrypted archives.																				
	<i>corrupted</i>	Block corrupted archives.																				
	<i>partiallycorrupted</i>	Block partially corrupted archives.																				
	<i>multipart</i>	Block multipart archives.																				
	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.																				
	<i>mailbomb</i>	Block mail bomb archives.																				
	<i>timeout</i>	Block scan timeout.																				
<i>unhandled</i>	Block archives that FortiProxy cannot open.																					
archive-log	Select the archive types to log.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Log encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Log corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Log partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Log multipart archives.</td></tr><tr><td><i>nested</i></td><td>Log nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Log mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Log scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Log archives that FortiProxy cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Log mail bomb archives.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiProxy cannot open.			
	Option	Description																				
	<i>encrypted</i>	Log encrypted archives.																				
	<i>corrupted</i>	Log corrupted archives.																				
	<i>partiallycorrupted</i>	Log partially corrupted archives.																				
	<i>multipart</i>	Log multipart archives.																				
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.																				
	<i>mailbomb</i>	Log mail bomb archives.																				
	<i>timeout</i>	Log scan timeout.																				
<i>unhandled</i>	Log archives that FortiProxy cannot open.																					
emulator	Enable/disable the virus emulator.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the virus emulator.</td></tr><tr><td><i>disable</i></td><td>Disable the virus emulator.</td></tr></table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.															
	Option	Description																				
	<i>enable</i>	Enable the virus emulator.																				
<i>disable</i>	Disable the virus emulator.																					
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default																		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.		
	<i>virus</i>	Treat Windows executables as viruses.		
content-disarm	Enable/disable Content Disarm and Reconstruction when performing AntiVirus scan.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable Content Disarm and Reconstruction when performing AntiVirus scan.		
	<i>enable</i>	Enable Content Disarm and Reconstruction when performing AntiVirus scan.		

config pop3

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the virus infected files.		
	<i>monitor</i>	Log the virus infected files.		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
fortindr	Enable scanning of files by FortiNDR.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiNDR detected infections.		
	<i>monitor</i>	Log the FortiNDR detected infections.		
fortisandbox	Enable scanning of files by FortiSandbox.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiSandbox detected infections.		
	<i>monitor</i>	Log the FortiSandbox detected infections.		
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable quarantine for infected files.		
	<i>enable</i>	Enable quarantine for infected files.		
archive-block	Select the archive types to block.	option	-	
	Option	Description		
	<i>encrypted</i>	Block encrypted archives.		
	<i>corrupted</i>	Block corrupted archives.		
	<i>partiallycorrupted</i>	Block partially corrupted archives.		
	<i>multipart</i>	Block multipart archives.		
	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Block mail bomb archives.		
	<i>timeout</i>	Block scan timeout.		
	<i>unhandled</i>	Block archives that FortiProxy cannot open.		
archive-log	Select the archive types to log.	option	-	
	Option	Description		
	<i>encrypted</i>	Log encrypted archives.		
	<i>corrupted</i>	Log corrupted archives.		
	<i>partiallycorrupted</i>	Log partially corrupted archives.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>multipart</i>	Log multipart archives.		
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Log mail bomb archives.		
	<i>timeout</i>	Log scan timeout.		
	<i>unhandled</i>	Log archives that FortiProxy cannot open.		
emulator	Enable/disable the virus emulator.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable the virus emulator.		
	<i>disable</i>	Disable the virus emulator.		
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default
	Option	Description		
	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.		
	<i>virus</i>	Treat Windows executables as viruses.		
content-disarm	Enable/disable Content Disarm and Reconstruction when performing AntiVirus scan.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable Content Disarm and Reconstruction when performing AntiVirus scan.		
	<i>enable</i>	Enable Content Disarm and Reconstruction when performing AntiVirus scan.		

config smtp

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the virus infected files.		
	<i>monitor</i>	Log the virus infected files.		

Parameter	Description	Type	Size	Default								
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the matched files.</td></tr><tr><td><i>monitor</i></td><td>Log the matched files.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the matched files.	<i>monitor</i>	Log the matched files.			
Option	Description											
<i>disable</i>	Disable.											
<i>block</i>	Block the matched files.											
<i>monitor</i>	Log the matched files.											
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the matched files.</td></tr><tr><td><i>monitor</i></td><td>Log the matched files.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the matched files.	<i>monitor</i>	Log the matched files.			
Option	Description											
<i>disable</i>	Disable.											
<i>block</i>	Block the matched files.											
<i>monitor</i>	Log the matched files.											
fortindr	Enable scanning of files by FortiNDR.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the FortiNDR detected infections.</td></tr><tr><td><i>monitor</i></td><td>Log the FortiNDR detected infections.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the FortiNDR detected infections.	<i>monitor</i>	Log the FortiNDR detected infections.			
Option	Description											
<i>disable</i>	Disable.											
<i>block</i>	Block the FortiNDR detected infections.											
<i>monitor</i>	Log the FortiNDR detected infections.											
fortisandbox	Enable scanning of files by FortiSandbox.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the FortiSandbox detected infections.</td></tr><tr><td><i>monitor</i></td><td>Log the FortiSandbox detected infections.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the FortiSandbox detected infections.	<i>monitor</i>	Log the FortiSandbox detected infections.			
Option	Description											
<i>disable</i>	Disable.											
<i>block</i>	Block the FortiSandbox detected infections.											
<i>monitor</i>	Log the FortiSandbox detected infections.											
quarantine	Enable/disable quarantine for infected files.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable quarantine for infected files.</td></tr><tr><td><i>enable</i></td><td>Enable quarantine for infected files.</td></tr></table>	Option	Description	<i>disable</i>	Disable quarantine for infected files.	<i>enable</i>	Enable quarantine for infected files.					
Option	Description											
<i>disable</i>	Disable quarantine for infected files.											
<i>enable</i>	Enable quarantine for infected files.											
archive-block	Select the archive types to block.	option	-									

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Block encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Block corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Block partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Block multipart archives.</td></tr><tr><td><i>nested</i></td><td>Block nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Block mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Block scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Block archives that FortiProxy cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Block mail bomb archives.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiProxy cannot open.			
	Option	Description																				
	<i>encrypted</i>	Block encrypted archives.																				
	<i>corrupted</i>	Block corrupted archives.																				
	<i>partiallycorrupted</i>	Block partially corrupted archives.																				
	<i>multipart</i>	Block multipart archives.																				
	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.																				
	<i>mailbomb</i>	Block mail bomb archives.																				
	<i>timeout</i>	Block scan timeout.																				
<i>unhandled</i>	Block archives that FortiProxy cannot open.																					
archive-log	Select the archive types to log.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Log encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Log corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Log partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Log multipart archives.</td></tr><tr><td><i>nested</i></td><td>Log nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Log mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Log scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Log archives that FortiProxy cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Log mail bomb archives.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiProxy cannot open.			
	Option	Description																				
	<i>encrypted</i>	Log encrypted archives.																				
	<i>corrupted</i>	Log corrupted archives.																				
	<i>partiallycorrupted</i>	Log partially corrupted archives.																				
	<i>multipart</i>	Log multipart archives.																				
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.																				
	<i>mailbomb</i>	Log mail bomb archives.																				
	<i>timeout</i>	Log scan timeout.																				
<i>unhandled</i>	Log archives that FortiProxy cannot open.																					
emulator	Enable/disable the virus emulator.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the virus emulator.</td></tr><tr><td><i>disable</i></td><td>Disable the virus emulator.</td></tr></table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.															
	Option	Description																				
	<i>enable</i>	Enable the virus emulator.																				
<i>disable</i>	Disable the virus emulator.																					
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Perform standard AntiVirus scanning of Windows executable files.</td></tr><tr><td><i>virus</i></td><td>Treat Windows executables as viruses.</td></tr></table>	Option	Description	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.	<i>virus</i>	Treat Windows executables as viruses.															
	Option	Description																				
	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.																				
<i>virus</i>	Treat Windows executables as viruses.																					

Parameter	Description	Type	Size	Default
content-disarm	Enable/disable Content Disarm and Reconstruction when performing AntiVirus scan.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable Content Disarm and Reconstruction when performing AntiVirus scan.		
	<i>enable</i>	Enable Content Disarm and Reconstruction when performing AntiVirus scan.		

config mapi

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the virus infected files.		
	<i>monitor</i>	Log the virus infected files.		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
fortindr	Enable scanning of files by FortiNDR.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiNDR detected infections.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>monitor</i>	Log the FortiNDR detected infections.		
fortisandbox	Enable scanning of files by FortiSandbox.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiSandbox detected infections.		
	<i>monitor</i>	Log the FortiSandbox detected infections.		
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable quarantine for infected files.		
	<i>enable</i>	Enable quarantine for infected files.		
archive-block	Select the archive types to block.	option	-	
	Option	Description		
	<i>encrypted</i>	Block encrypted archives.		
	<i>corrupted</i>	Block corrupted archives.		
	<i>partiallycorrupted</i>	Block partially corrupted archives.		
	<i>multipart</i>	Block multipart archives.		
	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Block mail bomb archives.		
	<i>timeout</i>	Block scan timeout.		
	<i>unhandled</i>	Block archives that FortiProxy cannot open.		
archive-log	Select the archive types to log.	option	-	
	Option	Description		
	<i>encrypted</i>	Log encrypted archives.		
	<i>corrupted</i>	Log corrupted archives.		
	<i>partiallycorrupted</i>	Log partially corrupted archives.		
	<i>multipart</i>	Log multipart archives.		
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mailbomb</i></td><td>Log mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Log scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Log archives that FortiProxy cannot open.</td></tr></table>	Option	Description	<i>mailbomb</i>	Log mail bomb archives.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiProxy cannot open.			
Option	Description											
<i>mailbomb</i>	Log mail bomb archives.											
<i>timeout</i>	Log scan timeout.											
<i>unhandled</i>	Log archives that FortiProxy cannot open.											
emulator	Enable/disable the virus emulator.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the virus emulator.</td></tr><tr><td><i>disable</i></td><td>Disable the virus emulator.</td></tr></table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.					
Option	Description											
<i>enable</i>	Enable the virus emulator.											
<i>disable</i>	Disable the virus emulator.											
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Perform standard AntiVirus scanning of Windows executable files.</td></tr><tr><td><i>virus</i></td><td>Treat Windows executables as viruses.</td></tr></table>	Option	Description	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.	<i>virus</i>	Treat Windows executables as viruses.					
Option	Description											
<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.											
<i>virus</i>	Treat Windows executables as viruses.											

config nntp

Parameter	Description	Type	Size	Default								
av-scan	Enable AntiVirus scan service.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the virus infected files.</td></tr><tr><td><i>monitor</i></td><td>Log the virus infected files.</td></tr></table>				Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the virus infected files.	<i>monitor</i>	Log the virus infected files.
	Option	Description										
	<i>disable</i>	Disable.										
	<i>block</i>	Block the virus infected files.										
<i>monitor</i>	Log the virus infected files.											
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the matched files.</td></tr><tr><td><i>monitor</i></td><td>Log the matched files.</td></tr></table>				Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the matched files.	<i>monitor</i>	Log the matched files.
	Option	Description										
	<i>disable</i>	Disable.										
	<i>block</i>	Block the matched files.										
<i>monitor</i>	Log the matched files.											
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
fortindr	Enable scanning of files by FortiNDR.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiNDR detected infections.		
	<i>monitor</i>	Log the FortiNDR detected infections.		
fortisandbox	Enable scanning of files by FortiSandbox.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiSandbox detected infections.		
	<i>monitor</i>	Log the FortiSandbox detected infections.		
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable quarantine for infected files.		
	<i>enable</i>	Enable quarantine for infected files.		
archive-block	Select the archive types to block.	option	-	
	Option	Description		
	<i>encrypted</i>	Block encrypted archives.		
	<i>corrupted</i>	Block corrupted archives.		
	<i>partiallycorrupted</i>	Block partially corrupted archives.		
	<i>multipart</i>	Block multipart archives.		
	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Block mail bomb archives.		
	<i>timeout</i>	Block scan timeout.		
	<i>unhandled</i>	Block archives that FortiProxy cannot open.		

Parameter	Description	Type	Size	Default																		
archive-log	Select the archive types to log.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Log encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Log corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Log partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Log multipart archives.</td></tr><tr><td><i>nested</i></td><td>Log nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Log mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Log scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Log archives that FortiProxy cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Log mail bomb archives.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiProxy cannot open.			
Option	Description																					
<i>encrypted</i>	Log encrypted archives.																					
<i>corrupted</i>	Log corrupted archives.																					
<i>partiallycorrupted</i>	Log partially corrupted archives.																					
<i>multipart</i>	Log multipart archives.																					
<i>nested</i>	Log nested archives that exceed uncompressed nest limit.																					
<i>mailbomb</i>	Log mail bomb archives.																					
<i>timeout</i>	Log scan timeout.																					
<i>unhandled</i>	Log archives that FortiProxy cannot open.																					
emulator	Enable/disable the virus emulator.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the virus emulator.</td></tr><tr><td><i>disable</i></td><td>Disable the virus emulator.</td></tr></table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.															
Option	Description																					
<i>enable</i>	Enable the virus emulator.																					
<i>disable</i>	Disable the virus emulator.																					

config cifs

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the virus infected files.		
	<i>monitor</i>	Log the virus infected files.		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
fortindr	Enable scanning of files by FortiNDR.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiNDR detected infections.		
	<i>monitor</i>	Log the FortiNDR detected infections.		
fortisandbox	Enable scanning of files by FortiSandbox.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiSandbox detected infections.		
	<i>monitor</i>	Log the FortiSandbox detected infections.		
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable quarantine for infected files.		
	<i>enable</i>	Enable quarantine for infected files.		
archive-block	Select the archive types to block.	option	-	
	Option	Description		
	<i>encrypted</i>	Block encrypted archives.		
	<i>corrupted</i>	Block corrupted archives.		
	<i>partiallycorrupted</i>	Block partially corrupted archives.		
	<i>multipart</i>	Block multipart archives.		
	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Block mail bomb archives.		
	<i>timeout</i>	Block scan timeout.		
	<i>unhandled</i>	Block archives that FortiProxy cannot open.		

Parameter	Description	Type	Size	Default																		
archive-log	Select the archive types to log.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Log encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Log corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Log partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Log multipart archives.</td></tr><tr><td><i>nested</i></td><td>Log nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Log mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Log scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Log archives that FortiProxy cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Log mail bomb archives.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiProxy cannot open.			
Option	Description																					
<i>encrypted</i>	Log encrypted archives.																					
<i>corrupted</i>	Log corrupted archives.																					
<i>partiallycorrupted</i>	Log partially corrupted archives.																					
<i>multipart</i>	Log multipart archives.																					
<i>nested</i>	Log nested archives that exceed uncompressed nest limit.																					
<i>mailbomb</i>	Log mail bomb archives.																					
<i>timeout</i>	Log scan timeout.																					
<i>unhandled</i>	Log archives that FortiProxy cannot open.																					
emulator	Enable/disable the virus emulator.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the virus emulator.</td></tr><tr><td><i>disable</i></td><td>Disable the virus emulator.</td></tr></table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.															
Option	Description																					
<i>enable</i>	Enable the virus emulator.																					
<i>disable</i>	Disable the virus emulator.																					

config ssh

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the virus infected files.		
	<i>monitor</i>	Log the virus infected files.		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
fortindr	Enable scanning of files by FortiNDR.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiNDR detected infections.		
	<i>monitor</i>	Log the FortiNDR detected infections.		
fortisandbox	Enable scanning of files by FortiSandbox.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiSandbox detected infections.		
	<i>monitor</i>	Log the FortiSandbox detected infections.		
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable quarantine for infected files.		
	<i>enable</i>	Enable quarantine for infected files.		
archive-block	Select the archive types to block.	option	-	
	Option	Description		
	<i>encrypted</i>	Block encrypted archives.		
	<i>corrupted</i>	Block corrupted archives.		
	<i>partiallycorrupted</i>	Block partially corrupted archives.		
	<i>multipart</i>	Block multipart archives.		
	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Block mail bomb archives.		
	<i>timeout</i>	Block scan timeout.		
	<i>unhandled</i>	Block archives that FortiProxy cannot open.		

Parameter	Description	Type	Size	Default																		
archive-log	Select the archive types to log.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Log encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Log corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Log partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Log multipart archives.</td></tr><tr><td><i>nested</i></td><td>Log nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Log mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Log scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Log archives that FortiProxy cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Log mail bomb archives.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiProxy cannot open.			
Option	Description																					
<i>encrypted</i>	Log encrypted archives.																					
<i>corrupted</i>	Log corrupted archives.																					
<i>partiallycorrupted</i>	Log partially corrupted archives.																					
<i>multipart</i>	Log multipart archives.																					
<i>nested</i>	Log nested archives that exceed uncompressed nest limit.																					
<i>mailbomb</i>	Log mail bomb archives.																					
<i>timeout</i>	Log scan timeout.																					
<i>unhandled</i>	Log archives that FortiProxy cannot open.																					
emulator	Enable/disable the virus emulator.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the virus emulator.</td></tr><tr><td><i>disable</i></td><td>Disable the virus emulator.</td></tr></table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.															
Option	Description																					
<i>enable</i>	Enable the virus emulator.																					
<i>disable</i>	Disable the virus emulator.																					

config nac-quar

Parameter	Description	Type	Size	Default						
infected	Enable/Disable quarantining infected hosts to the banned user list.	option	-	none						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Do not quarantine infected hosts.</td></tr><tr><td><i>quar-src-ip</i></td><td>Quarantine all traffic from the infected hosts source IP.</td></tr></table>				Option	Description	<i>none</i>	Do not quarantine infected hosts.	<i>quar-src-ip</i>	Quarantine all traffic from the infected hosts source IP.
Option	Description									
<i>none</i>	Do not quarantine infected hosts.									
<i>quar-src-ip</i>	Quarantine all traffic from the infected hosts source IP.									
expiry	Duration of quarantine.	user	Not Specified	5m						
log	Enable/disable AntiVirus quarantine logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AntiVirus quarantine logging.</td></tr><tr><td><i>disable</i></td><td>Disable AntiVirus quarantine logging.</td></tr></table>				Option	Description	<i>enable</i>	Enable AntiVirus quarantine logging.	<i>disable</i>	Disable AntiVirus quarantine logging.
Option	Description									
<i>enable</i>	Enable AntiVirus quarantine logging.									
<i>disable</i>	Disable AntiVirus quarantine logging.									

config content-disarm

Parameter	Description	Type	Size	Default								
original-file-destination	Destination to send original file if active content is removed.	option	-	discard								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortisandbox</i></td><td>Send original file to configured FortiSandbox.</td></tr><tr><td><i>quarantine</i></td><td>Send original file to quarantine.</td></tr><tr><td><i>discard</i></td><td>Original file will be discarded after content disarm.</td></tr></table>	Option	Description	<i>fortisandbox</i>	Send original file to configured FortiSandbox.	<i>quarantine</i>	Send original file to quarantine.	<i>discard</i>	Original file will be discarded after content disarm.			
Option	Description											
<i>fortisandbox</i>	Send original file to configured FortiSandbox.											
<i>quarantine</i>	Send original file to quarantine.											
<i>discard</i>	Original file will be discarded after content disarm.											
error-action	Action to be taken if CDR engine encounters an unrecoverable error.	option	-	log-only								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Block file on CDR error.</td></tr><tr><td><i>log-only</i></td><td>Log CDR error, but allow file.</td></tr><tr><td><i>ignore</i></td><td>Do nothing on CDR error.</td></tr></table>	Option	Description	<i>block</i>	Block file on CDR error.	<i>log-only</i>	Log CDR error, but allow file.	<i>ignore</i>	Do nothing on CDR error.			
Option	Description											
<i>block</i>	Block file on CDR error.											
<i>log-only</i>	Log CDR error, but allow file.											
<i>ignore</i>	Do nothing on CDR error.											
office-macro	Enable/disable stripping of macros in Microsoft Office documents.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td><i>enable</i></td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.					
Option	Description											
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.											
<i>enable</i>	Enable this Content Disarm and Reconstruction feature.											
office-hylink	Enable/disable stripping of hyperlinks in Microsoft Office documents.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td><i>enable</i></td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.					
Option	Description											
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.											
<i>enable</i>	Enable this Content Disarm and Reconstruction feature.											
office-linked	Enable/disable stripping of linked objects in Microsoft Office documents.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this Content Disarm and Reconstruction feature.</td></tr><tr><td><i>enable</i></td><td>Enable this Content Disarm and Reconstruction feature.</td></tr></table>	Option	Description	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.					
Option	Description											
<i>disable</i>	Disable this Content Disarm and Reconstruction feature.											
<i>enable</i>	Enable this Content Disarm and Reconstruction feature.											
office-embed	Enable/disable stripping of embedded objects in Microsoft Office documents.	option	-	enable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
office-dde	Enable/disable stripping of Dynamic Data Exchange events in Microsoft Office documents.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
office-action	Enable/disable stripping of PowerPoint action events in Microsoft Office documents.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-javacode	Enable/disable stripping of JavaScript code in PDF documents.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-embedfile	Enable/disable stripping of embedded files in PDF documents.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-hyperlink	Enable/disable stripping of hyperlinks from PDF documents.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-gotor	Enable/disable stripping of PDF document actions that access other PDF documents.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-launch	Enable/disable stripping of PDF document actions that launch other applications.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-sound	Enable/disable stripping of PDF document actions that play a sound.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-movie	Enable/disable stripping of PDF document actions that play a movie.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-java	Enable/disable stripping of PDF document actions that execute JavaScript code.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-form	Enable/disable stripping of PDF document actions that submit data to other targets.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
cover-page	Enable/disable inserting a cover page into the disarmed document.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
detect-only	Enable/disable only detect disarmable files, do not alter content.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		

config antivirus quarantine

Configure quarantine options.

```
config antivirus quarantine
  Description: Configure quarantine options.
  set agelimit {integer}
  set maxfilesize {integer}
  set quarantine-quota {integer}
  set drop-infected {option1}, {option2}, ...
  set store-infected {option1}, {option2}, ...
  set drop-blocked {option1}, {option2}, ...
  set store-blocked {option1}, {option2}, ...
  set drop-machine-learning {option1}, {option2}, ...
  set store-machine-learning {option1}, {option2}, ...
  set lowspace [drop-new|ovrw-old]
  set destination [NULL|disk|...]
end
```

config antivirus quarantine

Parameter	Description	Type	Size	Default
agelimit	Age limit for quarantined files.	integer	Minimum value: 0 Maximum value: 479	0
maxfilesize	Maximum file size to quarantine.	integer	Minimum value: 0 Maximum value: 500	0

Parameter	Description	Type	Size	Default																														
quarantine-quota	The amount of disk space to reserve for quarantining files.	integer	Minimum value: 0 Maximum value: 4294967295	0																														
drop-infected	Do not quarantine infected files found in sessions using the selected protocols. Dropped files are deleted instead of being quarantined.	option	-																															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>imap</td><td>IMAP.</td></tr><tr><td>smtp</td><td>SMTP.</td></tr><tr><td>pop3</td><td>POP3.</td></tr><tr><td>http</td><td>HTTP.</td></tr><tr><td>ftp</td><td>FTP.</td></tr><tr><td>nntp</td><td>NNTP.</td></tr><tr><td>imaps</td><td>IMAPS.</td></tr><tr><td>smtps</td><td>SMTPS.</td></tr><tr><td>pop3s</td><td>POP3S.</td></tr><tr><td>https</td><td>HTTPS.</td></tr><tr><td>ftps</td><td>FTPS.</td></tr><tr><td>mapi</td><td>MAPI.</td></tr><tr><td>cifs</td><td>CIFS.</td></tr><tr><td>ssh</td><td>SSH.</td></tr></table>				Option	Description	imap	IMAP.	smtp	SMTP.	pop3	POP3.	http	HTTP.	ftp	FTP.	nntp	NNTP.	imaps	IMAPS.	smtps	SMTPS.	pop3s	POP3S.	https	HTTPS.	ftps	FTPS.	mapi	MAPI.	cifs	CIFS.	ssh	SSH.
	Option	Description																																
	imap	IMAP.																																
	smtp	SMTP.																																
	pop3	POP3.																																
	http	HTTP.																																
	ftp	FTP.																																
	nntp	NNTP.																																
	imaps	IMAPS.																																
	smtps	SMTPS.																																
	pop3s	POP3S.																																
	https	HTTPS.																																
	ftps	FTPS.																																
	mapi	MAPI.																																
	cifs	CIFS.																																
ssh	SSH.																																	
store-infected	Quarantine infected files found in sessions using the selected protocols.	option	-	imap smtp pop3 http ftp nntp imaps smtps pop3s https ftps mapi cifs ssh																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>imap</td><td>IMAP.</td></tr></table>				Option	Description	imap	IMAP.																										
	Option	Description																																
imap	IMAP.																																	

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>smtp</i></td><td>SMTP.</td></tr><tr><td><i>pop3</i></td><td>POP3.</td></tr><tr><td><i>http</i></td><td>HTTP.</td></tr><tr><td><i>ftp</i></td><td>FTP.</td></tr><tr><td><i>nntp</i></td><td>NNTP.</td></tr><tr><td><i>imaps</i></td><td>IMAPS.</td></tr><tr><td><i>smtps</i></td><td>SMTPS.</td></tr><tr><td><i>pop3s</i></td><td>POP3S.</td></tr><tr><td><i>https</i></td><td>HTTPS.</td></tr><tr><td><i>ftps</i></td><td>FTPS.</td></tr><tr><td><i>mapi</i></td><td>MAPI.</td></tr><tr><td><i>cifs</i></td><td>CIFS.</td></tr><tr><td><i>ssh</i></td><td>SSH.</td></tr></table>	Option	Description	<i>smtp</i>	SMTP.	<i>pop3</i>	POP3.	<i>http</i>	HTTP.	<i>ftp</i>	FTP.	<i>nntp</i>	NNTP.	<i>imaps</i>	IMAPS.	<i>smtps</i>	SMTPS.	<i>pop3s</i>	POP3S.	<i>https</i>	HTTPS.	<i>ftps</i>	FTPS.	<i>mapi</i>	MAPI.	<i>cifs</i>	CIFS.	<i>ssh</i>	SSH.			
	Option	Description																														
	<i>smtp</i>	SMTP.																														
	<i>pop3</i>	POP3.																														
	<i>http</i>	HTTP.																														
	<i>ftp</i>	FTP.																														
	<i>nntp</i>	NNTP.																														
	<i>imaps</i>	IMAPS.																														
	<i>smtps</i>	SMTPS.																														
	<i>pop3s</i>	POP3S.																														
	<i>https</i>	HTTPS.																														
	<i>ftps</i>	FTPS.																														
	<i>mapi</i>	MAPI.																														
	<i>cifs</i>	CIFS.																														
	<i>ssh</i>	SSH.																														
drop-blocked	Do not quarantine dropped files found in sessions using the selected protocols. Dropped files are deleted instead of being quarantined.	option	-																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>imap</i></td><td>IMAP.</td></tr><tr><td><i>smtp</i></td><td>SMTP.</td></tr><tr><td><i>pop3</i></td><td>POP3.</td></tr><tr><td><i>http</i></td><td>HTTP.</td></tr><tr><td><i>ftp</i></td><td>FTP.</td></tr><tr><td><i>nntp</i></td><td>NNTP.</td></tr><tr><td><i>imaps</i></td><td>IMAPS.</td></tr><tr><td><i>smtps</i></td><td>SMTPS.</td></tr><tr><td><i>pop3s</i></td><td>POP3S.</td></tr><tr><td><i>ftps</i></td><td>FTPS.</td></tr><tr><td><i>mapi</i></td><td>MAPI.</td></tr><tr><td><i>cifs</i></td><td>CIFS.</td></tr><tr><td><i>ssh</i></td><td>SSH.</td></tr></table>	Option	Description	<i>imap</i>	IMAP.	<i>smtp</i>	SMTP.	<i>pop3</i>	POP3.	<i>http</i>	HTTP.	<i>ftp</i>	FTP.	<i>nntp</i>	NNTP.	<i>imaps</i>	IMAPS.	<i>smtps</i>	SMTPS.	<i>pop3s</i>	POP3S.	<i>ftps</i>	FTPS.	<i>mapi</i>	MAPI.	<i>cifs</i>	CIFS.	<i>ssh</i>	SSH.			
	Option	Description																														
	<i>imap</i>	IMAP.																														
	<i>smtp</i>	SMTP.																														
	<i>pop3</i>	POP3.																														
	<i>http</i>	HTTP.																														
	<i>ftp</i>	FTP.																														
	<i>nntp</i>	NNTP.																														
	<i>imaps</i>	IMAPS.																														
	<i>smtps</i>	SMTPS.																														
	<i>pop3s</i>	POP3S.																														
	<i>ftps</i>	FTPS.																														
	<i>mapi</i>	MAPI.																														
	<i>cifs</i>	CIFS.																														
	<i>ssh</i>	SSH.																														

Parameter	Description	Type	Size	Default																												
store-blocked	Quarantine blocked files found in sessions using the selected protocols.	option	-	imap smtp pop3 http ftp nntp imaps smtps pop3s ftps mapi cifs ssh																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>imap</td><td>IMAP.</td></tr><tr><td>smtp</td><td>SMTP.</td></tr><tr><td>pop3</td><td>POP3.</td></tr><tr><td>http</td><td>HTTP.</td></tr><tr><td>ftp</td><td>FTP.</td></tr><tr><td>nntp</td><td>NNTP.</td></tr><tr><td>imaps</td><td>IMAPS.</td></tr><tr><td>smtps</td><td>SMTPS.</td></tr><tr><td>pop3s</td><td>POP3S.</td></tr><tr><td>ftps</td><td>FTPS.</td></tr><tr><td>mapi</td><td>MAPI.</td></tr><tr><td>cifs</td><td>CIFS.</td></tr><tr><td>ssh</td><td>SSH.</td></tr></table>	Option	Description	imap	IMAP.	smtp	SMTP.	pop3	POP3.	http	HTTP.	ftp	FTP.	nntp	NNTP.	imaps	IMAPS.	smtps	SMTPS.	pop3s	POP3S.	ftps	FTPS.	mapi	MAPI.	cifs	CIFS.	ssh	SSH.			
	Option	Description																														
	imap	IMAP.																														
	smtp	SMTP.																														
	pop3	POP3.																														
	http	HTTP.																														
	ftp	FTP.																														
	nntp	NNTP.																														
	imaps	IMAPS.																														
	smtps	SMTPS.																														
	pop3s	POP3S.																														
	ftps	FTPS.																														
	mapi	MAPI.																														
	cifs	CIFS.																														
ssh	SSH.																															
drop-machine-learning	Do not quarantine files detected by machine learning found in sessions using the selected protocols. Dropped files are deleted instead of being quarantined.	option	-																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>imap</td><td>IMAP.</td></tr><tr><td>smtp</td><td>SMTP.</td></tr><tr><td>pop3</td><td>POP3.</td></tr><tr><td>http</td><td>HTTP.</td></tr><tr><td>ftp</td><td>FTP.</td></tr><tr><td>nntp</td><td>NNTP.</td></tr></table>	Option	Description	imap	IMAP.	smtp	SMTP.	pop3	POP3.	http	HTTP.	ftp	FTP.	nntp	NNTP.																	
	Option	Description																														
	imap	IMAP.																														
	smtp	SMTP.																														
	pop3	POP3.																														
	http	HTTP.																														
	ftp	FTP.																														
nntp	NNTP.																															

Parameter	Description	Type	Size	Default																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>imaps</i></td><td>IMAPS.</td></tr><tr><td><i>smtps</i></td><td>SMTPS.</td></tr><tr><td><i>pop3s</i></td><td>POP3S.</td></tr><tr><td><i>https</i></td><td>HTTPS.</td></tr><tr><td><i>ftps</i></td><td>FTPS.</td></tr><tr><td><i>mapi</i></td><td>MAPI.</td></tr><tr><td><i>cifs</i></td><td>CIFS.</td></tr><tr><td><i>ssh</i></td><td>SSH.</td></tr></table>	Option	Description	<i>imaps</i>	IMAPS.	<i>smtps</i>	SMTPS.	<i>pop3s</i>	POP3S.	<i>https</i>	HTTPS.	<i>ftps</i>	FTPS.	<i>mapi</i>	MAPI.	<i>cifs</i>	CIFS.	<i>ssh</i>	SSH.															
	Option	Description																																
	<i>imaps</i>	IMAPS.																																
	<i>smtps</i>	SMTPS.																																
	<i>pop3s</i>	POP3S.																																
	<i>https</i>	HTTPS.																																
	<i>ftps</i>	FTPS.																																
	<i>mapi</i>	MAPI.																																
	<i>cifs</i>	CIFS.																																
<i>ssh</i>	SSH.																																	
store-machine-learning	Quarantine files detected by machine learning found in sessions using the selected protocols.	option	-	imap smtp pop3 http ftp nntp imaps smtps pop3s https ftps mapi cifs ssh																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>imap</i></td><td>IMAP.</td></tr><tr><td><i>smtp</i></td><td>SMTP.</td></tr><tr><td><i>pop3</i></td><td>POP3.</td></tr><tr><td><i>http</i></td><td>HTTP.</td></tr><tr><td><i>ftp</i></td><td>FTP.</td></tr><tr><td><i>nntp</i></td><td>NNTP.</td></tr><tr><td><i>imaps</i></td><td>IMAPS.</td></tr><tr><td><i>smtps</i></td><td>SMTPS.</td></tr><tr><td><i>pop3s</i></td><td>POP3S.</td></tr><tr><td><i>https</i></td><td>HTTPS.</td></tr><tr><td><i>ftps</i></td><td>FTPS.</td></tr><tr><td><i>mapi</i></td><td>MAPI.</td></tr><tr><td><i>cifs</i></td><td>CIFS.</td></tr><tr><td><i>ssh</i></td><td>SSH.</td></tr></table>	Option	Description	<i>imap</i>	IMAP.	<i>smtp</i>	SMTP.	<i>pop3</i>	POP3.	<i>http</i>	HTTP.	<i>ftp</i>	FTP.	<i>nntp</i>	NNTP.	<i>imaps</i>	IMAPS.	<i>smtps</i>	SMTPS.	<i>pop3s</i>	POP3S.	<i>https</i>	HTTPS.	<i>ftps</i>	FTPS.	<i>mapi</i>	MAPI.	<i>cifs</i>	CIFS.	<i>ssh</i>	SSH.			
	Option	Description																																
	<i>imap</i>	IMAP.																																
	<i>smtp</i>	SMTP.																																
	<i>pop3</i>	POP3.																																
	<i>http</i>	HTTP.																																
	<i>ftp</i>	FTP.																																
	<i>nntp</i>	NNTP.																																
	<i>imaps</i>	IMAPS.																																
	<i>smtps</i>	SMTPS.																																
	<i>pop3s</i>	POP3S.																																
	<i>https</i>	HTTPS.																																
	<i>ftps</i>	FTPS.																																
	<i>mapi</i>	MAPI.																																
	<i>cifs</i>	CIFS.																																
<i>ssh</i>	SSH.																																	

Parameter	Description	Type	Size	Default
lowspace	Select the method for handling additional files when running low on disk space.	option	-	ovrw-old
	Option	Description		
	<i>drop-new</i>	Drop (delete) the most recently quarantined files.		
	<i>ovrw-old</i>	Overwrite the oldest quarantined files. That is, the files that are closest to being deleted from the quarantine.		
destination	Choose whether to quarantine files to the FortiProxy disk or to FortiAnalyzer or to delete them instead of quarantining them.	option	-	disk
	Option	Description		
	<i>NULL</i>	Files that would be quarantined are deleted.		
	<i>disk</i>	Quarantine files to the FortiProxy hard disk.		
	<i>FortiAnalyzer</i>	FortiAnalyzer		

config antivirus settings

Configure AntiVirus settings.

```
config antivirus settings
    Description: Configure AntiVirus settings.
    set machine-learning-detection [enable|monitor|...]
    set use-extreme-db [enable|disable]
    set grayware [enable|disable]
    set override-timeout {integer}
    set cache-infected-result [enable|disable]
end
```

config antivirus settings

Parameter	Description	Type	Size	Default				
machine-learning-detection	Use machine learning based malware detection.	option	-	enable				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable machine learning based malware detection.</td></tr></table>				Option	Description	<i>enable</i>	Enable machine learning based malware detection.
Option	Description							
<i>enable</i>	Enable machine learning based malware detection.							

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>monitor</i>	Enable machine learning based malware detection for monitoring only.		
	<i>disable</i>	Disable machine learning based malware detection.		
use-extreme-db	Enable/disable the use of Extreme AVDB.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable extreme AVDB.		
	<i>disable</i>	Disable extreme AVDB.		
grayware	Enable/disable grayware detection when an AntiVirus profile is applied to traffic.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable grayware detection.		
	<i>disable</i>	Disable grayware detection.		
override-timeout	Override the large file scan timeout value in seconds. Zero is the default value and is used to disable this command. When disabled, the daemon adjusts the large file scan timeout based on the file size.	integer	Minimum value: 30 Maximum value: 3600	0
cache-infected-result	Enable/disable cache of infected scan results.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable cache of infected scan results.		
	<i>disable</i>	Disable cache of infected scan results.		

application

This section includes syntax for the following commands:

- [config application custom on page 72](#)
- [config application group on page 73](#)
- [config application list on page 74](#)
- [config application name on page 83](#)
- [config application rule-settings on page 85](#)

config application custom

Configure custom application signatures.

```
config application custom
  Description: Configure custom application signatures.
  edit <tag>
    set id {integer}
    set comment {string}
    set signature {var-string}
    set category {integer}
    set protocol {user}
    set technology {user}
    set behavior {user}
    set vendor {user}
  next
end
```

config application custom

Parameter	Description	Type	Size	Default
tag	Signature tag.	string	Maximum length: 63	
id	Custom application category ID (use ? to view available options).	integer	Minimum value: 0 Maximum value: 4294967295	0
comment	Comment.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
signature	The text that makes up the actual custom application signature.	var-string	Maximum length: 4095	
category	Custom application category ID (use ? to view available options).	integer	Minimum value: 0 Maximum value: 4294967295	0
protocol	Custom application signature protocol.	user	Not Specified	
technology	Custom application signature technology.	user	Not Specified	
behavior	Custom application signature behavior.	user	Not Specified	
vendor	Custom application signature vendor.	user	Not Specified	

config application group

Configure firewall application groups.

```

config application group
    Description: Configure firewall application groups.
    edit <name>
        set comment {var-string}
        set type [application|filter]
        set application <id1>, <id2>, ...
        set category <id1>, <id2>, ...
        set risk <level1>, <level2>, ...
        set protocols {user}
        set vendor {user}
        set technology {user}
        set behavior {user}
        set popularity {option1}, {option2}, ...
    next
end

```

config application group

Parameter	Description	Type	Size	Default
name	Application group name.	string	Maximum length: 63	
comment	Comments.	var-string	Maximum length: 255	
type	Application group type.	option	-	application

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>application</i></td><td>Application ID.</td></tr><tr><td><i>filter</i></td><td>Application filter.</td></tr></table>	Option	Description	<i>application</i>	Application ID.	<i>filter</i>	Application filter.									
	Option	Description														
	<i>application</i>	Application ID.														
<i>filter</i>	Application filter.															
application <id>	Application ID list. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295													
category <id>	Application category ID list. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295													
risk <level>	Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical). Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical).	integer	Minimum value: 0 Maximum value: 4294967295													
protocols	Application protocol filter.	user	Not Specified	all												
vendor	Application vendor filter.	user	Not Specified	all												
technology	Application technology filter.	user	Not Specified	all												
behavior	Application behavior filter.	user	Not Specified	all												
popularity	Application popularity filter.	option	-	1 2 3 4 5												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Popularity level 1.</td></tr><tr><td>2</td><td>Popularity level 2.</td></tr><tr><td>3</td><td>Popularity level 3.</td></tr><tr><td>4</td><td>Popularity level 4.</td></tr><tr><td>5</td><td>Popularity level 5.</td></tr></table>	Option	Description	1	Popularity level 1.	2	Popularity level 2.	3	Popularity level 3.	4	Popularity level 4.	5	Popularity level 5.			
	Option	Description														
	1	Popularity level 1.														
	2	Popularity level 2.														
	3	Popularity level 3.														
	4	Popularity level 4.														
5	Popularity level 5.															

config application list

Configure application control lists.

```

config application list
  Description: Configure application control lists.
  edit <name>
    set comment {var-string}
    set replacemsg-group {string}
    set extended-log [enable|disable]
    set other-application-action [pass|block]
    set app-replacemsg [disable|enable]
    set other-application-log [disable|enable]
    set enforce-default-app-port [disable|enable]
    set force-inclusion-ssl-di-sigs [disable|enable]
    set unknown-application-action [pass|block]
    set unknown-application-log [disable|enable]
    set p2p-block-list {option1}, {option2}, ...
    set deep-app-inspection [disable|enable]
    set options {option1}, {option2}, ...
  config entries
    Description: Application list entries.
    edit <id>
      set risk <level1>, <level2>, ...
      set category <id1>, <id2>, ...
      set application <id1>, <id2>, ...
      set protocols {user}
      set vendor {user}
      set technology {user}
      set behavior {user}
      set popularity {option1}, {option2}, ...
      set exclusion <id1>, <id2>, ...
    config parameters
      Description: Application parameters.
      edit <id>
        config members
          Description: Parameter tuple members.
          edit <id>
            set name {string}
            set value {string}
          next
        end
      next
    end
    set action [pass|block|...]
    set log [disable|enable]
    set log-packet [disable|enable]
    set rate-count {integer}
    set rate-duration {integer}
    set rate-mode [periodical|continuous]
    set rate-track [none|src-ip|...]
    set session-ttl {integer}
    set shaper {string}
    set quarantine [none|attacker]
    set quarantine-expiry {user}
    set quarantine-log [disable|enable]
  next
end
set control-default-network-services [disable|enable]
config default-network-services

```

```

Description: Default network service entries.
edit <id>
    set port {integer}
    set services {option1}, {option2}, ...
    set violation-action [pass|monitor|...]
next
end
next
end

```

config application list

Parameter	Description	Type	Size	Default
name	List name.	string	Maximum length: 35	
comment	Comments.	var-string	Maximum length: 255	
replacemsg-group	Replacement message group.	string	Maximum length: 35	
extended-log	Enable/disable extended logging.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
other-application-action	Action for other applications.	option	-	pass
	Option	Description		
	pass	Allow sessions matching an application in this application list.		
	block	Block sessions matching an application in this application list.		
app-replacemsg	Enable/disable replacement messages for blocked applications.	option	-	enable
	Option	Description		
	disable	Disable replacement messages for blocked applications.		
	enable	Enable replacement messages for blocked applications.		
other-application-log	Enable/disable logging for other applications.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable logging for other applications.		
	<i>enable</i>	Enable logging for other applications.		
enforce-default-app-port	Enable/disable default application port enforcement for allowed applications.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable default application port enforcement.		
	<i>enable</i>	Enable default application port enforcement.		
force-inclusion-ssl-di-sigs	Enable/disable forced inclusion of SSL deep inspection signatures.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable forced inclusion of signatures which normally require SSL deep inspection.		
	<i>enable</i>	Enable forced inclusion of signatures which normally require SSL deep inspection.		
unknown-application-action	Pass or block traffic from unknown applications.	option	-	pass
	Option	Description		
	<i>pass</i>	Pass or allow unknown applications.		
	<i>block</i>	Drop or block unknown applications.		
unknown-application-log	Enable/disable logging for unknown applications.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable logging for unknown applications.		
	<i>enable</i>	Enable logging for unknown applications.		
p2p-block-list	P2P applications to be block listed.	option	-	

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>skype</td><td>Skype.</td></tr><tr><td>edonkey</td><td>Edonkey.</td></tr><tr><td>bittorrent</td><td>Bit torrent.</td></tr></table>	Option	Description	skype	Skype.	edonkey	Edonkey.	bittorrent	Bit torrent.					
	Option	Description												
	skype	Skype.												
	edonkey	Edonkey.												
bittorrent	Bit torrent.													
deep-app-inspection	Enable/disable deep application inspection.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable deep application inspection.</td></tr><tr><td>enable</td><td>Enable deep application inspection.</td></tr></table>	Option	Description	disable	Disable deep application inspection.	enable	Enable deep application inspection.							
	Option	Description												
	disable	Disable deep application inspection.												
enable	Enable deep application inspection.													
options	Basic application protocol signatures allowed by default.	option	-	allow-dns										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow-dns</td><td>Allow DNS.</td></tr><tr><td>allow-icmp</td><td>Allow ICMP.</td></tr><tr><td>allow-http</td><td>Allow generic HTTP web browsing.</td></tr><tr><td>allow-ssl</td><td>Allow generic SSL communication.</td></tr></table>	Option	Description	allow-dns	Allow DNS.	allow-icmp	Allow ICMP.	allow-http	Allow generic HTTP web browsing.	allow-ssl	Allow generic SSL communication.			
	Option	Description												
	allow-dns	Allow DNS.												
	allow-icmp	Allow ICMP.												
	allow-http	Allow generic HTTP web browsing.												
allow-ssl	Allow generic SSL communication.													
control-default-network-services	Enable/disable enforcement of protocols over selected ports.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable protocol enforcement over selected ports.</td></tr><tr><td>enable</td><td>Enable protocol enforcement over selected ports.</td></tr></table>	Option	Description	disable	Disable protocol enforcement over selected ports.	enable	Enable protocol enforcement over selected ports.							
	Option	Description												
	disable	Disable protocol enforcement over selected ports.												
enable	Enable protocol enforcement over selected ports.													

config entries

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default												
risk <level>	Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical). Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical).	integer	Minimum value: 0 Maximum value: 4294967295													
category <id>	Category ID list. Application category ID.	integer	Minimum value: 0 Maximum value: 4294967295													
application <id>	ID of allowed applications. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295													
protocols	Application protocol filter.	user	Not Specified	all												
vendor	Application vendor filter.	user	Not Specified	all												
technology	Application technology filter.	user	Not Specified	all												
behavior	Application behavior filter.	user	Not Specified	all												
popularity	Application popularity filter.	option	-	1 2 3 4 5												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Popularity level 1.</td></tr><tr><td>2</td><td>Popularity level 2.</td></tr><tr><td>3</td><td>Popularity level 3.</td></tr><tr><td>4</td><td>Popularity level 4.</td></tr><tr><td>5</td><td>Popularity level 5.</td></tr></table>				Option	Description	1	Popularity level 1.	2	Popularity level 2.	3	Popularity level 3.	4	Popularity level 4.	5	Popularity level 5.
Option	Description															
1	Popularity level 1.															
2	Popularity level 2.															
3	Popularity level 3.															
4	Popularity level 4.															
5	Popularity level 5.															
exclusion <id>	ID of excluded applications. Excluded application IDs.	integer	Minimum value: 0 Maximum value: 4294967295													
action	Pass or block traffic, or reset connection for traffic from this application.	option	-	block												

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>pass</i>	Pass or allow matching traffic.		
	<i>block</i>	Block or drop matching traffic.		
	<i>reset</i>	Reset sessions for matching traffic.		
log	Enable/disable logging for this application list.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable logging.		
	<i>enable</i>	Enable logging.		
log-packet	Enable/disable packet logging.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable packet logging.		
	<i>enable</i>	Enable packet logging.		
rate-count	Count of the rate.	integer	Minimum value: 0 Maximum value: 65535	0
rate-duration	Duration (sec) of the rate.	integer	Minimum value: 1 Maximum value: 65535	60
rate-mode	Rate limit mode.	option	-	continuous
	Option	Description		
	<i>periodical</i>	Allow configured number of packets every rate-duration.		
	<i>continuous</i>	Block packets once the rate is reached.		
rate-track	Track the packet protocol field.	option	-	none
	Option	Description		
	<i>none</i>	none		
	<i>src-ip</i>	Source IP.		
	<i>dest-ip</i>	Destination IP.		
	<i>dhcp-client-mac</i>	DHCP client.		
	<i>dns-domain</i>	DNS domain.		

Parameter	Description	Type	Size	Default						
session-ttl	Session TTL.	integer	Minimum value: 0 Maximum value: 4294967295	0						
shaper	Traffic shaper.	string	Maximum length: 35							
quarantine	Quarantine method.	option	-	none						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Quarantine is disabled.</td></tr><tr><td><i>attacker</i></td><td>Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.</td></tr></table>				Option	Description	<i>none</i>	Quarantine is disabled.	<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.
	Option	Description								
	<i>none</i>	Quarantine is disabled.								
<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.									
quarantine-expiry	Duration of quarantine. Requires quarantine set to attacker.	user	Not Specified	5m						
quarantine-log	Enable/disable quarantine logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable quarantine logging.</td></tr><tr><td><i>enable</i></td><td>Enable quarantine logging.</td></tr></table>				Option	Description	<i>disable</i>	Disable quarantine logging.	<i>enable</i>	Enable quarantine logging.
	Option	Description								
	<i>disable</i>	Disable quarantine logging.								
<i>enable</i>	Enable quarantine logging.									

config parameters

Parameter	Description	Type	Size	Default
id	Parameter tuple ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config members

Parameter	Description	Type	Size	Default
id	Parameter.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
name	Parameter name.	string	Maximum length: 31	
value	Parameter value.	string	Maximum length: 199	

config default-network-services

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
port	Port number.	integer	Minimum value: 0 Maximum value: 65535	0
services	Network protocols.	option	-	
	Option Description			
	<i>http</i>	HTTP.		
	<i>ssh</i>	SSH.		
	<i>telnet</i>	TELNET.		
	<i>ftp</i>	FTP.		
	<i>dns</i>	DNS.		
	<i>smtp</i>	SMTP.		
	<i>pop3</i>	POP3.		
	<i>imap</i>	IMAP.		
	<i>snmp</i>	SNMP.		
	<i>nntp</i>	NNTP.		
	<i>https</i>	HTTPS.		
violation-action	Action for protocols not in the allowlist for selected port.	option	-	block

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>pass</i>	Allow protocols not in the allowlist for selected port.		
	<i>monitor</i>	Monitor protocols not in the allowlist for selected port.		
	<i>block</i>	Block protocols not in the allowlist for selected port.		

config application name

Configure application signatures.

```

config application name
    Description: Configure application signatures.
    edit <name>
        set id {integer}
        set category {integer}
        set popularity {integer}
        set risk {integer}
        set weight {integer}
        set protocol {user}
        set technology {user}
        set behavior {user}
        set vendor {user}
    config parameters
        Description: Application parameters.
        edit <name>
            set default value {string}
        next
    end
    config metadata
        Description: Meta data.
        edit <id>
            set metaid {integer}
            set valueid {integer}
        next
    end
next
end

```

config application name

Parameter	Description	Type	Size	Default
name	Application name.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
id	Application ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Application category ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
popularity	Application popularity.	integer	Minimum value: 0 Maximum value: 255	0
risk	Application risk.	integer	Minimum value: 0 Maximum value: 255	0
weight	Application weight.	integer	Minimum value: 0 Maximum value: 255	0
protocol	Application protocol.	user	Not Specified	
technology	Application technology.	user	Not Specified	
behavior	Application behavior.	user	Not Specified	
vendor	Application vendor.	user	Not Specified	

config parameters

Parameter	Description	Type	Size	Default
name	Parameter name.	string	Maximum length: 31	
default value	Parameter default value.	string	Maximum length: 199	

config metadata

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
metaid	Meta ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
valueid	Value ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config application rule-settings

Configure application rule settings.

```
config application rule-settings
    Description: Configure application rule settings.
    edit <id>
    next
end
```

config application rule-settings

Parameter	Description	Type	Size	Default
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

authentication

This section includes syntax for the following commands:

- [config authentication rule on page 86](#)
- [config authentication scheme on page 89](#)
- [config authentication setting on page 91](#)

config authentication rule

Configure Authentication Rules.

```
config authentication rule
  Description: Configure Authentication Rules.
  edit <name>
    set status [enable|disable]
    set protocol [http|ftp|...]
    set web-proxy {string}
    set srcintf <name1>, <name2>, ...
    set srcaddr <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
    set srcaddr6 <name1>, <name2>, ...
    set dstaddr6 <name1>, <name2>, ...
    set ip-based [enable|disable]
    set active-auth-method {string}
    set sso-auth-method {string}
    set web-auth-cookie [enable|disable]
    set cors-stateful [enable|disable]
    set cors-depth {integer}
    set transaction-based [enable|disable]
    set web-portal [enable|disable]
    set comments {var-string}
    set form-auth-fallback [enable|disable]
  next
end
```

config authentication rule

Parameter	Description	Type	Size	Default
name	Authentication rule name.	string	Maximum length: 35	
status	Enable/disable this authentication rule.	option	-	enable

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this authentication rule.</td></tr><tr><td><i>disable</i></td><td>Disable this authentication rule.</td></tr></table>	Option	Description	<i>enable</i>	Enable this authentication rule.	<i>disable</i>	Disable this authentication rule.							
	Option	Description												
	<i>enable</i>	Enable this authentication rule.												
<i>disable</i>	Disable this authentication rule.													
protocol	Authentication is required for the selected protocol.	option	-	http										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>HTTP traffic is matched and authentication is required.</td></tr><tr><td><i>ftp</i></td><td>FTP traffic is matched and authentication is required.</td></tr><tr><td><i>socks</i></td><td>SOCKS traffic is matched and authentication is required.</td></tr><tr><td><i>ssh</i></td><td>SSH traffic is matched and authentication is required.</td></tr></table>	Option	Description	<i>http</i>	HTTP traffic is matched and authentication is required.	<i>ftp</i>	FTP traffic is matched and authentication is required.	<i>socks</i>	SOCKS traffic is matched and authentication is required.	<i>ssh</i>	SSH traffic is matched and authentication is required.			
	Option	Description												
	<i>http</i>	HTTP traffic is matched and authentication is required.												
	<i>ftp</i>	FTP traffic is matched and authentication is required.												
	<i>socks</i>	SOCKS traffic is matched and authentication is required.												
<i>ssh</i>	SSH traffic is matched and authentication is required.													
web-proxy	Web-Proxy profile.	string	Maximum length: 35											
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79											
srcaddr <name>	Authentication is required for the selected IPv4 source address. Address name.	string	Maximum length: 79											
dstaddr <name>	Select an IPv4 destination address from available options. Required for web proxy authentication. Address name.	string	Maximum length: 79											
srcaddr6 <name>	Authentication is required for the selected IPv6 source address. Address name.	string	Maximum length: 79											
dstaddr6 <name>	Select an IPv6 destination address from available options. Required for web proxy authentication. Address name.	string	Maximum length: 79											
ip-based	Enable/disable IP-based authentication. When enabled, previously authenticated users from the same IP address will be exempted.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IP-based authentication.</td></tr><tr><td><i>disable</i></td><td>Disable IP-based authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable IP-based authentication.	<i>disable</i>	Disable IP-based authentication.							
	Option	Description												
	<i>enable</i>	Enable IP-based authentication.												
<i>disable</i>	Disable IP-based authentication.													
active-auth-method	Select an active authentication method.	string	Maximum length: 35											

Parameter	Description	Type	Size	Default						
sso-auth-method	Select a single-sign on (SSO) authentication method.	string	Maximum length: 35							
web-auth-cookie	Enable/disable Web authentication cookies.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Web authentication cookie.</td></tr><tr><td><i>disable</i></td><td>Disable Web authentication cookie.</td></tr></table>	Option	Description	<i>enable</i>	Enable Web authentication cookie.	<i>disable</i>	Disable Web authentication cookie.			
Option	Description									
<i>enable</i>	Enable Web authentication cookie.									
<i>disable</i>	Disable Web authentication cookie.									
cors-stateful	Enable/disable allowance of CORS access.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable allowance of CORS access</td></tr><tr><td><i>disable</i></td><td>Disable allowance of CORS access</td></tr></table>	Option	Description	<i>enable</i>	Enable allowance of CORS access	<i>disable</i>	Disable allowance of CORS access			
Option	Description									
<i>enable</i>	Enable allowance of CORS access									
<i>disable</i>	Disable allowance of CORS access									
cors-depth	Depth to allow CORS access.	integer	Minimum value: 1 Maximum value: 8	3						
transaction-based	Enable/disable transaction based authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable transaction based authentication.</td></tr><tr><td><i>disable</i></td><td>Disable transaction based authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable transaction based authentication.	<i>disable</i>	Disable transaction based authentication.			
Option	Description									
<i>enable</i>	Enable transaction based authentication.									
<i>disable</i>	Disable transaction based authentication.									
web-portal	Enable/disable web portal for proxy transparent policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable web-portal.</td></tr><tr><td><i>disable</i></td><td>Disable web-portal.</td></tr></table>	Option	Description	<i>enable</i>	Enable web-portal.	<i>disable</i>	Disable web-portal.			
Option	Description									
<i>enable</i>	Enable web-portal.									
<i>disable</i>	Disable web-portal.									
comments	Comment.	var-string	Maximum length: 1023							
form-auth-fallback	Enable/disable to use FORM authentication if needed.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Form Authentication Fallback</td></tr><tr><td><i>disable</i></td><td>Disable Form Authentication Fallback</td></tr></table>	Option	Description	<i>enable</i>	Enable Form Authentication Fallback	<i>disable</i>	Disable Form Authentication Fallback			
Option	Description									
<i>enable</i>	Enable Form Authentication Fallback									
<i>disable</i>	Disable Form Authentication Fallback									

config authentication scheme

Configure Authentication Schemes.

```
config authentication scheme
    Description: Configure Authentication Schemes.
    edit <name>
        set method {option1}, {option2}, ...
        set negotiate-ntlm [enable|disable]
        set kerberos-keytab {string}
        set domain-controller {string}
        set saml-server {string}
        set saml-timeout {integer}
        set fsso-agent-for-ntlm {string}
        set require-tfa [enable|disable]
        set fsso-guest [enable|disable]
        set user-cert [enable|disable]
        set search-all-ldap-databases [enable|disable]
        set user-database <name1>, <name2>, ...
        set ssh-ca {string}
    next
end
```

config authentication scheme

Parameter	Description	Type	Size	Default																								
name	Authentication scheme name.	string	Maximum length: 35																									
method	Authentication methods.	option	-																									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ntlm</i></td><td>NTLM authentication.</td></tr><tr><td><i>basic</i></td><td>Basic HTTP authentication.</td></tr><tr><td><i>digest</i></td><td>Digest HTTP authentication.</td></tr><tr><td><i>form</i></td><td>Form-based HTTP authentication.</td></tr><tr><td><i>negotiate</i></td><td>Negotiate authentication.</td></tr><tr><td><i>fsso</i></td><td>Fortinet Single Sign-On (FSSO) authentication.</td></tr><tr><td><i>rsso</i></td><td>RADIUS Single Sign-On (RSSO) authentication.</td></tr><tr><td><i>ssh-publickey</i></td><td>Public key based SSH authentication.</td></tr><tr><td><i>cert</i></td><td>Client certificate authentication.</td></tr><tr><td><i>saml</i></td><td>SAML authentication.</td></tr><tr><td><i>x-auth-user</i></td><td>User from HTTP x-authenticated-user header.</td></tr></table>				Option	Description	<i>ntlm</i>	NTLM authentication.	<i>basic</i>	Basic HTTP authentication.	<i>digest</i>	Digest HTTP authentication.	<i>form</i>	Form-based HTTP authentication.	<i>negotiate</i>	Negotiate authentication.	<i>fsso</i>	Fortinet Single Sign-On (FSSO) authentication.	<i>rsso</i>	RADIUS Single Sign-On (RSSO) authentication.	<i>ssh-publickey</i>	Public key based SSH authentication.	<i>cert</i>	Client certificate authentication.	<i>saml</i>	SAML authentication.	<i>x-auth-user</i>	User from HTTP x-authenticated-user header.
Option	Description																											
<i>ntlm</i>	NTLM authentication.																											
<i>basic</i>	Basic HTTP authentication.																											
<i>digest</i>	Digest HTTP authentication.																											
<i>form</i>	Form-based HTTP authentication.																											
<i>negotiate</i>	Negotiate authentication.																											
<i>fsso</i>	Fortinet Single Sign-On (FSSO) authentication.																											
<i>rsso</i>	RADIUS Single Sign-On (RSSO) authentication.																											
<i>ssh-publickey</i>	Public key based SSH authentication.																											
<i>cert</i>	Client certificate authentication.																											
<i>saml</i>	SAML authentication.																											
<i>x-auth-user</i>	User from HTTP x-authenticated-user header.																											

Parameter	Description	Type	Size	Default
negotiate-ntlm	Enable/disable negotiate authentication for NTLM.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable negotiate authentication for NTLM.		
	<i>disable</i>	Disable negotiate authentication for NTLM.		
kerberos-keytab	Kerberos keytab setting.	string	Maximum length: 35	
domain-controller	Domain controller setting.	string	Maximum length: 35	
saml-server	SAML configuration.	string	Maximum length: 35	
saml-timeout	SAML authentication timeout in seconds.	integer	Minimum value: 30 Maximum value: 1200	120
fsso-agent-for-ntlm	FSSO agent to use for NTLM authentication.	string	Maximum length: 35	
require-tfa	Enable/disable two-factor authentication.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable two-factor authentication.		
	<i>disable</i>	Disable two-factor authentication.		
fsso-guest	Enable/disable user fsso-guest authentication.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable user fsso-guest authentication.		
	<i>disable</i>	Disable user fsso-guest authentication.		
user-cert	Enable/disable authentication with user certificate.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable client certificate field authentication.		
	<i>disable</i>	Disable client certificate field authentication.		
search-all-ldap-databases	Enable/disable searching all LDAP databases to find groups.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable searching for groups in all LDAP databases.		
	<i>disable</i>	Disable searching for groups in all LDAP databases.		
user-database <name>	Authentication server to contain user information; "local" (default) or "123" (for LDAP). Authentication server name.	string	Maximum length: 79	
ssh-ca	SSH CA name.	string	Maximum length: 35	

config authentication setting

Configure authentication setting.

```

config authentication setting
    Description: Configure authentication setting.
    set active-auth-scheme {string}
    set sso-auth-scheme {string}
    set update-time {user}
    set persistent-cookie [enable|disable]
    set ip-auth-cookie [enable|disable]
    set cookie-max-age {integer}
    set cookie-refresh-div {integer}
    set captive-portal-type [fqdn|ip]
    set captive-portal-ip {ipv4-address-any}
    set captive-portal-ip6 {ipv6-address}
    set captive-portal {string}
    set captive-portal6 {string}
    set cert-auth [enable|disable]
    set cert-captive-portal {string}
    set cert-captive-portal-ip {ipv4-address-any}
    set cert-captive-portal-port {integer}
    set captive-portal-port {integer}
    set auth-https [enable|disable]
    set captive-portal-ssl-port {integer}
    set user-cert-ca <name1>, <name2>, ...
    set dev-range <name1>, <name2>, ...
    set log-auth-request [enable|disable]
end

```

config authentication setting

Parameter	Description	Type	Size	Default						
active-auth-scheme	Active authentication method (scheme name).	string	Maximum length: 35							
sso-auth-scheme	Single-Sign-On authentication method (scheme name).	string	Maximum length: 35							
update-time	Time of the last update.	user	Not Specified							
persistent-cookie	Enable/disable persistent cookie on web portal authentication.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable persistent cookie.</td></tr><tr><td><i>disable</i></td><td>Disable persistent cookie.</td></tr></table>				Option	Description	<i>enable</i>	Enable persistent cookie.	<i>disable</i>	Disable persistent cookie.
	Option	Description								
	<i>enable</i>	Enable persistent cookie.								
<i>disable</i>	Disable persistent cookie.									
ip-auth-cookie	Enable/disable persistent cookie on IP based web portal authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable persistent cookie for IP-based authentication.</td></tr><tr><td><i>disable</i></td><td>Disable persistent cookie for IP-based authentication.</td></tr></table>				Option	Description	<i>enable</i>	Enable persistent cookie for IP-based authentication.	<i>disable</i>	Disable persistent cookie for IP-based authentication.
	Option	Description								
	<i>enable</i>	Enable persistent cookie for IP-based authentication.								
<i>disable</i>	Disable persistent cookie for IP-based authentication.									
cookie-max-age	Persistent web portal cookie maximum age in minutes.	integer	Minimum value: 30 Maximum value: 10080	480						
cookie-refresh-div	Refresh rate divider of persistent web portal cookie. Refresh value = cookie-max-age/cookie-refresh-div.	integer	Minimum value: 2 Maximum value: 4	2						
captive-portal-type	Captive portal type.	option	-	fqdn						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fqdn</i></td><td>Use FQDN for captive portal.</td></tr><tr><td><i>ip</i></td><td>Use an IP address for captive portal.</td></tr></table>				Option	Description	<i>fqdn</i>	Use FQDN for captive portal.	<i>ip</i>	Use an IP address for captive portal.
	Option	Description								
	<i>fqdn</i>	Use FQDN for captive portal.								
<i>ip</i>	Use an IP address for captive portal.									
captive-portal-ip	Captive portal IP address.	ipv4-address-any	Not Specified	0.0.0.0						

Parameter	Description	Type	Size	Default						
captive-portal-ip6	Captive portal IPv6 address.	ipv6-address	Not Specified	::						
captive-portal	Captive portal host name.	string	Maximum length: 255							
captive-portal6	IPv6 captive portal host name.	string	Maximum length: 255							
cert-auth	Enable/disable redirecting certificate authentication to HTTPS portal.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
cert-captive-portal	Certificate captive portal host name.	string	Maximum length: 255							
cert-captive-portal-ip	Certificate captive portal IP address.	ipv4-address-any	Not Specified	0.0.0.0						
cert-captive-portal-port	Certificate captive portal port number.	integer	Minimum value: 1 Maximum value: 65535	7832						
captive-portal-port	Captive portal port number.	integer	Minimum value: 1 Maximum value: 65535	7830						
auth-https	Enable/disable redirecting HTTP user authentication to HTTPS.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
captive-portal-ssl-port	Captive portal SSL port number.	integer	Minimum value: 1 Maximum value: 65535	7831						

Parameter	Description	Type	Size	Default
user-cert-ca <name>	CA certificate used for client certificate verification. CA certificate list.	string	Maximum length: 79	
dev-range <name>	Address range for the IP based device query. Address name.	string	Maximum length: 79	
log-auth- request	Enable/disable to log authentication request.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

automation

This section includes syntax for the following commands:

- [config automation setting on page 95](#)

config automation setting

Automation setting configuration.

```
config automation setting
    Description: Automation setting configuration.
    set max-concurrent-stitches {integer}
    set fabric-sync [enable|disable]
end
```

config automation setting

Parameter	Description	Type	Size	Default
max-concurrent-stitches	Maximum number of automation stitches that are allowed to run concurrently.	integer	Minimum value: 32 Maximum value: 1024	512
fabric-sync	Enable/disable synchronization of automation settings with security fabric.	option	-	enable
	Option	Description		
	enable	Synchronize automation setting with security fabric.		
	disable	Do not synchronize automation setting with security fabric.		

casb

This section includes syntax for the following commands:

- [config casb profile on page 96](#)
- [config casb saas-application on page 99](#)
- [config casb user-activity on page 100](#)

config casb profile

Configure CASB profile.

```
config casb profile
  Description: Configure CASB profile.
  edit <name>
    set comment {var-string}
    config saas-application
      Description: CASB profile SaaS application.
      edit <name>
        set status [enable|disable]
        set safe-search [enable|disable]
        set safe-search-control <name1>, <name2>, ...
        set tenant-control [enable|disable]
        set tenant-control-tenants <name1>, <name2>, ...
        set domain-control [enable|disable]
        set domain-control-domains <name1>, <name2>, ...
        set log [enable|disable]
        config access-rule
          Description: CASB profile access rule.
          edit <name>
            set bypass {option1}, {option2}, ...
            set action [monitor|bypass|...]
          next
        end
      end
    config custom-control
      Description: CASB profile custom control.
      edit <name>
        config option
          Description: CASB custom control option.
          edit <name>
            set user-input <value1>, <value2>, ...
          next
        end
      next
    end
  next
end
next
end
next
end
end
```


config casb profile

Parameter	Description	Type	Size	Default
name	CASB profile name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	

config saas-application

Parameter	Description	Type	Size	Default
name	CASB profile SaaS application name.	string	Maximum length: 79	
status	Enable/disable setting.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
safe-search	Enable/disable safe search.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
safe-search-control <name>	CASB profile safe search control. Safe search control name.	string	Maximum length: 79	
tenant-control	Enable/disable tenant control.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
tenant-control-tenants <name>	CASB profile tenant control tenants. Tenant control tenants name.	string	Maximum length: 79	
domain-control	Enable/disable domain control.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
domain-control-domains <name>	CASB profile domain control domains. Domain control domain name.	string	Maximum length: 79	
log	Enable/disable log settings.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable log setting.		
	<i>disable</i>	Disable log setting.		

config access-rule

Parameter	Description	Type	Size	Default
name	CASB access rule activity name.	string	Maximum length: 79	
bypass	CASB bypass options.	option	-	
	Option	Description		
	<i>av</i>	Exempt from AV scanning.		
	<i>dlp</i>	Exempt from data leak prevention (DLP).		
	<i>web-filter</i>	Exempt from web filter.		
	<i>file-filter</i>	Exempt from file filter.		
	<i>video-filter</i>	Exempt from video filter.		
action	CASB access rule action.	option	-	monitor
	Option	Description		
	<i>monitor</i>	Log when log is enabled.		
	<i>bypass</i>	Apply bypass options.		
	<i>block</i>	Block the request.		

config custom-control

Parameter	Description	Type	Size	Default
name	CASB custom control user activity name.	string	Maximum length: 79	

config option

Parameter	Description	Type	Size	Default
name	CASB custom control option name.	string	Maximum length: 79	
user-input <value>	CASB custom control user input. user input value.	string	Maximum length: 79	

config casb saas-application

Configure CASB SaaS application.

```
config casb saas-application
  Description: Configure CASB SaaS application.
  edit <name>
    set uuid {string}
    set status [enable|disable]
    set type [built-in|customized]
    set casb-name {string}
    set description {string}
    set domains <domain1>, <domain2>, ...
  next
end
```

config casb saas-application

Parameter	Description	Type	Size	Default
name	SaaS application name.	string	Maximum length: 79	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	string	Maximum length: 36	
status	Enable/disable setting.	option	-	enable
		Option	Description	
		enable	Enable setting.	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable setting.		
type	SaaS application type.	option	-	customized
	Option	Description		
	<i>built-in</i>	Built-in SaaS application.		
	<i>customized</i>	User customized SaaS appliciation.		
casb-name	SaaS application signature name.	string	Maximum length: 79	
description	SaaS application description.	string	Maximum length: 63	
domains	SaaS application domain list.	string	Maximum length: 127	
<domain>	Domain list separated by space.			

config casb user-activity

Configure CASB user activity.

```
config casb user-activity
  Description: Configure CASB user activity.
  edit <name>
    set uuid {string}
    set status [enable|disable]
    set description {string}
    set type [built-in|customized]
    set casb-name {string}
    set application {string}
    set category [activity-control|tenant-control|...]
    set match-strategy [and|or]
    config match
      Description: CASB user activity match rules.
      edit <id>
        set strategy [and|or]
        config rules
          Description: CASB user activity rules.
          edit <id>
            set type [domains|host|...]
            set domains <domain1>, <domain2>, ...
            set methods <method1>, <method2>, ...
            set match-pattern [simple|substr|...]
            set match-value {string}
            set header-name {string}
            set case-sensitive [enable|disable]
            set negate [enable|disable]
```

```

        next
    end
    next
end
config control-options
    Description: CASB control options.
    edit <name>
        set status [enable|disable]
        config operations
            Description: CASB control option operations.
            edit <name>
                set target [header|path]
                set action [append|prepend|...]
                set direction {option}
                set header-name {string}
                set search-pattern [simple|substr|...]
                set search-key {string}
                set case-sensitive [enable|disable]
                set value-from-input [enable|disable]
                set values <value1>, <value2>, ...
            next
        end
    next
end
next
end
end

```

config casb user-activity

Parameter	Description	Type	Size	Default						
name	CASB user activity name.	string	Maximum length: 79							
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	string	Maximum length: 36							
status	CASB user activity status.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
description	CASB user activity description.	string	Maximum length: 63							
type	CASB user activity type.	option	-	customized						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>built-in</i></td><td>Built-in CASB user-activity.</td></tr><tr><td><i>customized</i></td><td>User customized CASB user-activity.</td></tr></table>				Option	Description	<i>built-in</i>	Built-in CASB user-activity.	<i>customized</i>	User customized CASB user-activity.
	Option	Description								
	<i>built-in</i>	Built-in CASB user-activity.								
<i>customized</i>	User customized CASB user-activity.									

Parameter	Description	Type	Size	Default												
casb-name	CASB user activity signature name.	string	Maximum length: 79													
application	CASB SaaS application name.	string	Maximum length: 79													
category	CASB user activity category.	option	-	activity-control												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>activity-control</i></td><td>Activity control.</td></tr><tr><td><i>tenant-control</i></td><td>Tenant control.</td></tr><tr><td><i>domain-control</i></td><td>Domain control.</td></tr><tr><td><i>safe-search-control</i></td><td>Safe search control.</td></tr><tr><td><i>other</i></td><td>User customized category.</td></tr></table>				Option	Description	<i>activity-control</i>	Activity control.	<i>tenant-control</i>	Tenant control.	<i>domain-control</i>	Domain control.	<i>safe-search-control</i>	Safe search control.	<i>other</i>	User customized category.
	Option	Description														
	<i>activity-control</i>	Activity control.														
	<i>tenant-control</i>	Tenant control.														
	<i>domain-control</i>	Domain control.														
	<i>safe-search-control</i>	Safe search control.														
<i>other</i>	User customized category.															
match-strategy	CASB user activity match strategy.	option	-	or												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>and</i></td><td>Match user activity using a logical AND operator.</td></tr><tr><td><i>or</i></td><td>Match user activity using a logical OR operator.</td></tr></table>				Option	Description	<i>and</i>	Match user activity using a logical AND operator.	<i>or</i>	Match user activity using a logical OR operator.						
	Option	Description														
	<i>and</i>	Match user activity using a logical AND operator.														
<i>or</i>	Match user activity using a logical OR operator.															

config match

Parameter	Description	Type	Size	Default
id	CASB user activity match rules ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
strategy	CASB user activity rules strategy.	option	-	and
	Option	Description		
	and	Match user activity using a logical AND operator.		
	or	Match user activity using a logical OR operator.		

config rules

Parameter	Description	Type	Size	Default
id	CASB user activity rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
type	CASB user activity rule type.	option	-	host
	Option	Description		
	<i>domains</i>	Domains.		
	<i>host</i>	Host.		
	<i>path</i>	Path.		
	<i>header</i>	HTTP header.		
	<i>header-value</i>	HTTP header and value.		
	<i>method</i>	HTTP method.		
domains <domain>	CASB user activity domain list. Domain list separated by space.	string	Maximum length: 127	
methods <method>	CASB user activity method list. User activity method.	string	Maximum length: 79	
match-pattern	CASB user activity rule match pattern.	option	-	simple
	Option	Description		
	<i>simple</i>	Exact string match pattern.		
	<i>substr</i>	Sub-string pattern.		
	<i>regex</i>	Regular expression pattern.		
match-value	CASB user activity rule match value.	string	Maximum length: 1023	
header-name	CASB user activity rule header name.	string	Maximum length: 255	
case-sensitive	CASB user activity match case sensitive.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable value case sensitive match.		
	<i>disable</i>	Disable value case sensitive match.		

Parameter	Description	Type	Size	Default
negate	Enable/disable what the matching strategy must not be.	option	-	disable
	Option	Description		
	<i>enable</i>	Matching strategy is negated.		
	<i>disable</i>	Matching strategy is not negated.		

config control-options

Parameter	Description	Type	Size	Default
name	CASB control option name.	string	Maximum length: 79	
status	CASB control option status.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config operations

Parameter	Description	Type	Size	Default
name	CASB control option operation name.	string	Maximum length: 79	
target	CASB operation target.	option	-	header
	Option	Description		
	<i>header</i>	Header.		
	<i>path</i>	Path.		
action	CASB operation action.	option	-	append
	Option	Description		
	<i>append</i>	Append the values after the target.		
	<i>prepend</i>	Prepend the values before the target.		
	<i>replace</i>	Replace the target by the value.		
	<i>new</i>	Create a new header regardless if existing header is found or not.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>new-on-not-found</i></td><td>Create new header only if existing HTTP header is not found.</td></tr><tr><td><i>delete</i></td><td>Delete the target.</td></tr></table>	Option	Description	<i>new-on-not-found</i>	Create new header only if existing HTTP header is not found.	<i>delete</i>	Delete the target.					
	Option	Description										
	<i>new-on-not-found</i>	Create new header only if existing HTTP header is not found.										
<i>delete</i>	Delete the target.											
direction	CASB operation direction.	option	-	request								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>request</i></td><td>Request.</td></tr></table>	Option	Description	<i>request</i>	Request.							
	Option	Description										
	<i>request</i>	Request.										
header-name	CASB operation header name to search.	string	Maximum length: 255									
search-pattern	CASB operation search pattern.	option	-	simple								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>simple</i></td><td>Exact string match pattern.</td></tr><tr><td><i>substr</i></td><td>Sub-string pattern.</td></tr><tr><td><i>regexp</i></td><td>Regular expression pattern.</td></tr></table>	Option	Description	<i>simple</i>	Exact string match pattern.	<i>substr</i>	Sub-string pattern.	<i>regexp</i>	Regular expression pattern.			
	Option	Description										
	<i>simple</i>	Exact string match pattern.										
	<i>substr</i>	Sub-string pattern.										
<i>regexp</i>	Regular expression pattern.											
search-key	CASB operation key to search.	string	Maximum length: 1023									
case-sensitive	CASB operation search case sensitive.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable case sensitive search.</td></tr><tr><td><i>disable</i></td><td>Disable case sensitive search.</td></tr></table>	Option	Description	<i>enable</i>	Enable case sensitive search.	<i>disable</i>	Disable case sensitive search.					
	Option	Description										
	<i>enable</i>	Enable case sensitive search.										
<i>disable</i>	Disable case sensitive search.											
value-from-input	Enable/disable value from user input.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable value from input.</td></tr><tr><td><i>disable</i></td><td>Disable value from input.</td></tr></table>	Option	Description	<i>enable</i>	Enable value from input.	<i>disable</i>	Disable value from input.					
	Option	Description										
	<i>enable</i>	Enable value from input.										
<i>disable</i>	Disable value from input.											
values <value>	CASB operation new values. Operation value.	string	Maximum length: 79									

certificate

This section includes syntax for the following commands:

- [config certificate ca on page 106](#)
- [config certificate crt on page 107](#)
- [config certificate local on page 109](#)
- [config certificate remote on page 113](#)

config certificate ca

CA certificate.

```
config certificate ca
  Description: CA certificate.
  edit <name>
    set ca {user}
    set range [global|vdom]
    set source [factory|user|...]
    set ssl-inspection-trusted [enable|disable]
    set scep-url {string}
    set auto-update-days {integer}
    set auto-update-days-warning {integer}
    set source-ip {ipv4-address}
    set ca-identifier {string}
    set obsolete [disable|enable]
  next
end
```

config certificate ca

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 79	
ca	CA certificate as a PEM file.	user	Not Specified	
range	Either global or VDOM IP address range for the CA certificate.	option	-	global
		Option	Description	
		<i>global</i>	Global range.	
		<i>vdom</i>	VDOM IP address range.	

Parameter	Description	Type	Size	Default
source	CA certificate source type.	option	-	user
	Option	Description		
	<i>factory</i>	Factory installed certificate.		
	<i>user</i>	User generated certificate.		
	<i>bundle</i>	Bundle file certificate.		
ssl-inspection-trusted	Enable/disable this CA as a trusted CA for SSL inspection.	option	-	enable
	Option	Description		
	<i>enable</i>	Trusted CA for SSL inspection.		
	<i>disable</i>	Untrusted CA for SSL inspection.		
scep-url	URL of the SCEP server.	string	Maximum length: 255	
auto-update-days	Number of days to wait before requesting an updated CA certificate.	integer	Minimum value: 0 Maximum value: 4294967295	0
auto-update-days-warning	Number of days before an expiry-warning message is generated.	integer	Minimum value: 0 Maximum value: 4294967295	0
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0
ca-identifier	CA identifier of the SCEP server.	string	Maximum length: 255	
obsolete	Enable/disable this CA as obsolete.	option	-	disable
	Option	Description		
	<i>disable</i>	Alive.		
	<i>enable</i>	Obsolete.		

config certificate crt

Certificate Revocation List as a PEM file.

```

config certificate crt
  Description: Certificate Revocation List as a PEM file.
  edit <name>
    set crt {user}
    set range [global|vdom]
    set source [factory|user|...]
    set update-vdom {string}
    set ldap-server {string}
    set ldap-username {string}
    set ldap-password {password}
    set http-url {string}
    set scep-url {string}
    set scep-cert {string}
    set update-interval {integer}
    set source-ip {ipv4-address}
  next
end

```

config certificate crt

Parameter	Description	Type	Size	Default								
name	Name.	string	Maximum length: 35									
crl	Certificate Revocation List as a PEM file.	user	Not Specified									
range	Either global or VDOM IP address range for the certificate.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Global range.</td></tr><tr><td><i>vdom</i></td><td>VDOM IP address range.</td></tr></table>				Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.		
Option	Description											
<i>global</i>	Global range.											
<i>vdom</i>	VDOM IP address range.											
source	Certificate source type.	option	-	user								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>factory</i></td><td>Factory installed certificate.</td></tr><tr><td><i>user</i></td><td>User generated certificate.</td></tr><tr><td><i>bundle</i></td><td>Bundle file certificate.</td></tr></table>				Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.
Option	Description											
<i>factory</i>	Factory installed certificate.											
<i>user</i>	User generated certificate.											
<i>bundle</i>	Bundle file certificate.											
update-vdom	VDOM for CRL update.	string	Maximum length: 31	root								
ldap-server	LDAP server name for CRL auto-update.	string	Maximum length: 35									
ldap-username	LDAP server user name.	string	Maximum length: 63									

Parameter	Description	Type	Size	Default
ldap-password	LDAP server user password.	password	Not Specified	
http-url	HTTP server URL for CRL auto-update.	string	Maximum length: 255	
scep-url	SCEP server URL for CRL auto-update.	string	Maximum length: 255	
scep-cert	Local certificate for SCEP communication for CRL auto-update.	string	Maximum length: 35	Fortinet_CA_SSL
update-interval	Time in seconds before the FortiProxy checks for an updated CRL. Set to 0 to update only when it expires.	integer	Minimum value: 0 Maximum value: 4294967295	0
source-ip	Source IP address for communications to a HTTP or SCEP CA server.	ipv4-address	Not Specified	0.0.0.0

config certificate local

Local keys and certificates.

```

config certificate local
    Description: Local keys and certificates.
    edit <name>
        set type [normal|hsm]
        set password {password}
        set hsm-vendor [safenet|primus]
        set hsm-slot {string}
        set hsm-keytype [rsa|ec]
        set comments {string}
        set private-key {user}
        set certificate {user}
        set csr {user}
        set state {user}
        set scep-url {string}
        set range [global|vdom]
        set source [factory|user|...]
        set auto-regenerate-days {integer}
        set auto-regenerate-days-warning {integer}
        set scep-password {password}
        set ca-identifier {string}
        set name-encoding [printable|utf8]
        set source-ip {ipv4-address}
        set ike-localid {string}
        set ike-localid-type [asn1dn|fqdn]
        set enroll-protocol [none|scep|...]
        set private-key-retain [enable|disable]

```

```

    set cmp-server {string}
    set cmp-path {string}
    set cmp-server-cert {string}
    set cmp-regeneration-method [keyupdate|renewal]
    set acme-ca-url {string}
    set acme-domain {string}
    set acme-email {string}
    set acme-rsa-key-size {integer}
    set acme-renew-window {integer}
next
end

```

config certificate local

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
type	Type.	option	-	normal
	Option	Description		
	normal	Normal		
	hsm	HSM		
password	Password as a PEM file.	password	Not Specified	
hsm-vendor	HSM vendor.	option	-	safenet
	Option	Description		
	safenet	Safenet HSM.		
	primus	Securosys Primus HSM.		
hsm-slot	HSM slot to use with this certificate.	string	Maximum length: 35	
hsm-keytype	HSM certificate key type.	option	-	rsa
	Option	Description		
	rsa	RSA key type.		
	ec	EC key type.		
comments	Comment.	string	Maximum length: 511	
private-key	PEM format key encrypted with a password.	user	Not Specified	
certificate	PEM format certificate.	user	Not Specified	

Parameter	Description	Type	Size	Default								
csr	Certificate Signing Request.	user	Not Specified									
state	Certificate Signing Request State.	user	Not Specified									
scep-url	SCEP server URL.	string	Maximum length: 255									
range	Either a global or VDOM IP address range for the certificate.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Global range.</td></tr><tr><td><i>vdom</i></td><td>VDOM IP address range.</td></tr></table>				Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.		
	Option	Description										
	<i>global</i>	Global range.										
<i>vdom</i>	VDOM IP address range.											
source	Certificate source type.	option	-	user								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>factory</i></td><td>Factory installed certificate.</td></tr><tr><td><i>user</i></td><td>User generated certificate.</td></tr><tr><td><i>bundle</i></td><td>Bundle file certificate.</td></tr></table>				Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.
	Option	Description										
	<i>factory</i>	Factory installed certificate.										
	<i>user</i>	User generated certificate.										
<i>bundle</i>	Bundle file certificate.											
auto-regenerate-days	Number of days to wait before expiry of an updated local certificate is requested (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0								
auto-regenerate-days-warning	Number of days to wait before an expiry warning message is generated (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0								
scep-password	SCEP server challenge password for auto-regeneration.	password	Not Specified									
ca-identifier	CA identifier of the CA server for signing via SCEP.	string	Maximum length: 255									
name-encoding	Name encoding method for auto-regeneration.	option	-	printable								

Parameter	Description	Type	Size	Default
	Option	Description		
	printable	Printable encoding (default).		
	utf8	UTF-8 encoding.		
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0
ike-localid	Local ID the FortiProxy uses for authentication as a VPN client.	string	Maximum length: 63	
ike-localid-type	IKE local ID type.	option	-	asn1dn
	Option	Description		
	asn1dn	ASN.1 distinguished name.		
	fqdn	Fully qualified domain name.		
enroll-protocol	Certificate enrollment protocol.	option	-	none
	Option	Description		
	none	None (default).		
	scep	Simple Certificate Enrollment Protocol.		
	cmpv2	Certificate Management Protocol Version 2.		
	acme2	Automated Certificate Management Environment Version 2.		
private-key-retain	Enable/disable retention of private key during SCEP renewal.	option	-	disable
	Option	Description		
	enable	Keep the existing private key during SCEP renewal.		
	disable	Generate a new private key during SCEP renewal.		
cmp-server	Address and port for CMP server (format = address:port).	string	Maximum length: 63	
cmp-path	Path location inside CMP server.	string	Maximum length: 255	

Parameter	Description	Type	Size	Default						
cmp-server-cert	CMP server certificate.	string	Maximum length: 79							
cmp-regeneration-method	CMP auto-regeneration method.	option	-	keyupate						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>keyupate</td><td>Key Update.</td></tr><tr><td>renewal</td><td>Renewal.</td></tr></table>				Option	Description	keyupate	Key Update.	renewal	Renewal.
Option	Description									
keyupate	Key Update.									
renewal	Renewal.									
acme-ca-url	The URL for the ACME CA server.	string	Maximum length: 255	https://acme-v02.api.letsencrypt.org/directory						
acme-domain	A valid domain that resolves to this FortiProxy unit.	string	Maximum length: 255							
acme-email	Contact email address that is required by some CAs like LetsEncrypt.	string	Maximum length: 255							
acme-rsa-key-size	Length of the RSA private key of the generated cert (Minimum 2048 bits).	integer	Minimum value: 2048 Maximum value: 4096	2048						
acme-renew-window	Beginning of the renewal window.	integer	Minimum value: 1 Maximum value: 60	30						

config certificate remote

Remote certificate as a PEM file.

```
config certificate remote
    Description: Remote certificate as a PEM file.
    edit <name>
        set remote {user}
        set range [global|vdom]
        set source [factory|user|...]
    next
end
```

config certificate remote

Parameter	Description	Type	Size	Default								
name	Name.	string	Maximum length: 35									
remote	Remote certificate.	user	Not Specified									
range	Either the global or VDOM IP address range for the remote certificate.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Global range.</td></tr><tr><td><i>vdom</i></td><td>VDOM IP address range.</td></tr></table>	Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.					
Option	Description											
<i>global</i>	Global range.											
<i>vdom</i>	VDOM IP address range.											
source	Remote certificate source type.	option	-	user								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>factory</i></td><td>Factory installed certificate.</td></tr><tr><td><i>user</i></td><td>User generated certificate.</td></tr><tr><td><i>bundle</i></td><td>Bundle file certificate.</td></tr></table>	Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.			
Option	Description											
<i>factory</i>	Factory installed certificate.											
<i>user</i>	User generated certificate.											
<i>bundle</i>	Bundle file certificate.											

dlp

This section includes syntax for the following commands:

- [config dlp data-type on page 115](#)
- [config dlp dictionary on page 116](#)
- [config dlp exact-data-match on page 118](#)
- [config dlp filepattern on page 119](#)
- [config dlp fp-doc-source on page 123](#)
- [config dlp profile on page 126](#)
- [config dlp sensitivity on page 130](#)
- [config dlp sensor on page 131](#)
- [config dlp settings on page 132](#)

config dlp data-type

Configure predefined data type used by DLP blocking.

```
config dlp data-type
    Description: Configure predefined data type used by DLP blocking.
    edit <name>
        set pattern {string}
        set verify {string}
        set verify2 {string}
        set match-around {string}
        set look-back {integer}
        set look-ahead {integer}
        set match-back {integer}
        set match-ahead {integer}
        set transform {string}
        set verify-transformed-pattern [enable|disable]
        set comment {var-string}
    next
end
```

config dlp data-type

Parameter	Description	Type	Size	Default
name	Name of table containing the data type.	string	Maximum length: 35	
pattern	Regular expression pattern string without look around.	string	Maximum length: 255	

Parameter	Description	Type	Size	Default						
verify	Regular expression pattern string used to verify the data type.	string	Maximum length: 255							
verify2	Extra regular expression pattern string used to verify the data type.	string	Maximum length: 255							
match-around	Dictionary to check whether it has a match around (Only support match-any and basic types, no repeat supported).	string	Maximum length: 35							
look-back	Number of characters required to save for verification.	integer	Minimum value: 1 Maximum value: 255	1						
look-ahead	Number of characters to obtain in advance for verification.	integer	Minimum value: 1 Maximum value: 255	1						
match-back	Number of characters in front for match-around.	integer	Minimum value: 1 Maximum value: 4096	1						
match-ahead	Number of characters behind for match-around.	integer	Minimum value: 1 Maximum value: 4096	1						
transform	Template to transform user input to a pattern using capture group from 'pattern'.	string	Maximum length: 255							
verify-transformed-pattern	Enable/disable verification for transformed pattern.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable verification for transformed pattern.</td></tr><tr><td><i>disable</i></td><td>Disable verification for transformed pattern.</td></tr></table>				Option	Description	<i>enable</i>	Enable verification for transformed pattern.	<i>disable</i>	Disable verification for transformed pattern.
Option	Description									
<i>enable</i>	Enable verification for transformed pattern.									
<i>disable</i>	Disable verification for transformed pattern.									
comment	Optional comments.	var-string	Maximum length: 255							

config dlp dictionary

Configure dictionaries used by DLP blocking.

```

config dlp dictionary
  Description: Configure dictionaries used by DLP blocking.
  edit <name>
    set uuid {uuid}
    set match-type [match-all|match-any]
    set match-around [enable|disable]
    set comment {var-string}
    config entries
      Description: DLP dictionary entries.
      edit <id>
        set type {string}
        set pattern {string}
        set ignore-case [enable|disable]
        set repeat [enable|disable]
        set status [enable|disable]
        set comment {var-string}
      next
    end
  next
end

```

config dlp dictionary

Parameter	Description	Type	Size	Default						
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
name	Name of table containing the dictionary.	string	Maximum length: 35							
match-type	Logical relation between entries.	option	-	match-any						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>match-all</i></td><td>Match all entries.</td></tr><tr><td><i>match-any</i></td><td>Match any entries.</td></tr></table>				Option	Description	<i>match-all</i>	Match all entries.	<i>match-any</i>	Match any entries.
Option	Description									
<i>match-all</i>	Match all entries.									
<i>match-any</i>	Match any entries.									
match-around	Enable/disable match-around support.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable match-around support.</td></tr><tr><td><i>disable</i></td><td>Disable match-around support.</td></tr></table>				Option	Description	<i>enable</i>	Enable match-around support.	<i>disable</i>	Disable match-around support.
Option	Description									
<i>enable</i>	Enable match-around support.									
<i>disable</i>	Disable match-around support.									
comment	Optional comments.	var-string	Maximum length: 255							

config entries

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
type	Pattern type to match.	string	Maximum length: 35	
pattern	Pattern to match.	string	Maximum length: 255	
ignore-case	Enable/disable ignore case.	option	-	disable
	OptionDescription			
	enable	Enable ignore case.		
	disable	Disable ignore case.		
repeat	Enable/disable repeat match.	option	-	disable
	OptionDescription			
	enable	Enable repeat match.		
	disable	Disable repeat match.		
status	Enable/disable this pattern.	option	-	enable
	OptionDescription			
	enable	Enable this pattern.		
	disable	Disable this pattern.		
comment	Optional comments.	var-string	Maximum length: 255	

config dlp exact-data-match

Configure exact-data-match template used by DLP scan.

```
config dlp exact-data-match
  Description: Configure exact-data-match template used by DLP scan.
  edit <name>
    set optional {integer}
    set data {string}
    config columns
```

```

        Description: DLP exact-data-match column types.
        edit <index>
            set type {string}
            set optional [enable|disable]
        next
    end
next
end

```

config dlp exact-data-match

Parameter	Description	Type	Size	Default
name	Name of table containing the exact-data-match template.	string	Maximum length: 35	
optional	Number of optional columns need to match.	integer	Minimum value: 0 Maximum value: 32	0
data	External resource for exact data match.	string	Maximum length: 35	

config columns

Parameter	Description	Type	Size	Default						
index	Column index.	integer	Minimum value: 1 Maximum value: 32	0						
type	Data-type for this column.	string	Maximum length: 35							
optional	Enable/disable optional match.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable optional match.</td></tr><tr><td><i>disable</i></td><td>Disable optional match.</td></tr></table>	Option	Description	<i>enable</i>	Enable optional match.	<i>disable</i>	Disable optional match.			
Option	Description									
<i>enable</i>	Enable optional match.									
<i>disable</i>	Disable optional match.									

config dlp filepattern

Configure file patterns used by DLP blocking.

```

config dlp filepattern
  Description: Configure file patterns used by DLP blocking.
  edit <id>
    set name {string}
    set comment {var-string}
    config entries
      Description: Configure file patterns used by DLP blocking.
      edit <pattern>
        set filter-type [pattern|type]
        set file-type [7z|arj|...]
      next
    end
  next
end

```

config dlp filepattern

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table containing the file pattern list.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

config entries

Parameter	Description	Type	Size	Default						
filter-type	Filter by file name pattern or by file type.	option	-	pattern						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pattern</i></td><td>Filter by file name pattern.</td></tr><tr><td><i>type</i></td><td>Filter by file type.</td></tr></table>	Option	Description	<i>pattern</i>	Filter by file name pattern.	<i>type</i>	Filter by file type.			
Option	Description									
<i>pattern</i>	Filter by file name pattern.									
<i>type</i>	Filter by file type.									
pattern	Add a file name pattern.	string	Maximum length: 79							
file-type	Select a file type.	option	-	unknown						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>7z</td><td>Match 7-zip files.</td></tr></table>	Option	Description	7z	Match 7-zip files.					
Option	Description									
7z	Match 7-zip files.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>arj</i>	Match arj compressed files.		
	<i>cab</i>	Match Windows cab files.		
	<i>lzh</i>	Match lzh compressed files.		
	<i>rar</i>	Match rar archives.		
	<i>tar</i>	Match tar files.		
	<i>zip</i>	Match zip files.		
	<i>bzip</i>	Match bzip files.		
	<i>gzip</i>	Match gzip files.		
	<i>bzip2</i>	Match bzip2 files.		
	<i>xz</i>	Match xz files.		
	<i>bat</i>	Match Windows batch files.		
	<i>uue</i>	Match uue files.		
	<i>mime</i>	Match mime files.		
	<i>base64</i>	Match base64 files.		
	<i>binhex</i>	Match binhex files.		
	<i>elf</i>	Match elf files.		
	<i>exe</i>	Match Windows executable files.		
	<i>hta</i>	Match hta files.		
	<i>html</i>	Match html files.		
	<i>jad</i>	Match jad files.		
	<i>class</i>	Match class files.		
	<i>cod</i>	Match cod files.		
	<i>javascript</i>	Match javascript files.		
	<i>msoffice</i>	Match MS-Office files. For example, doc, xls, ppt, and so on.		
	<i>msofficex</i>	Match MS-Office XML files. For example, docx, xlsx, pptx, and so on.		
	<i>fsg</i>	Match fsg files.		
	<i>upx</i>	Match upx files.		
	<i>petite</i>	Match petite files.		
	<i>aspack</i>	Match aspack files.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>sis</i>	Match sis files.		
	<i>hlp</i>	Match Windows help files.		
	<i>activemime</i>	Match activemime files.		
	<i>jpeg</i>	Match jpeg files.		
	<i>gif</i>	Match gif files.		
	<i>tiff</i>	Match tiff files.		
	<i>png</i>	Match png files.		
	<i>bmp</i>	Match bmp files.		
	<i>unknown</i>	Match unknown files.		
	<i>mpeg</i>	Match mpeg files.		
	<i>mov</i>	Match mov files.		
	<i>mp3</i>	Match mp3 files.		
	<i>wma</i>	Match wma files.		
	<i>wav</i>	Match wav files.		
	<i>pdf</i>	Match Acrobat PDF files.		
	<i>avi</i>	Match avi files.		
	<i>rm</i>	Match rm files.		
	<i>torrent</i>	Match torrent files.		
	<i>hibun</i>	Match special-file-23-support files.		
	<i>msi</i>	Match Windows Installer msi files.		
	<i>mach-o</i>	Match Mach object files.		
	<i>dmg</i>	Match Apple disk image files.		
	<i>.net</i>	Match .NET files.		
	<i>xar</i>	Match xar archive files.		
	<i>chm</i>	Match Windows compiled HTML help files.		
	<i>iso</i>	Match ISO archive files.		
	<i>crx</i>	Match Chrome extension files.		
	<i>flac</i>	Match flac files.		

config dlp fp-doc-source

Create a DLP fingerprint database by allowing the FortiProxy to access a file server containing files from which to create fingerprints.

```
config dlp fp-doc-source
    Description: Create a DLP fingerprint database by allowing the FortiProxy to access a
    file server containing files from which to create fingerprints.
    edit <name>
        set server-type {option}
        set server {string}
        set period [none|daily|...]
        set vdom [mgmt|current]
        set scan-subdirectories [enable|disable]
        set scan-on-creation [enable|disable]
        set remove-deleted [enable|disable]
        set keep-modified [enable|disable]
        set username {string}
        set password {password}
        set file-path {string}
        set file-pattern {string}
        set sensitivity {string}
        set tod-hour {integer}
        set tod-min {integer}
        set weekday [sunday|monday|...]
        set date {integer}
    next
end
```

config dlp fp-doc-source

Parameter	Description	Type	Size	Default				
name	Name of the DLP fingerprint database.	string	Maximum length: 35					
server-type	Protocol used to communicate with the file server. Currently only Samba (SMB) servers are supported.	option	-	samba				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>samba</td><td>SAMBA server.</td></tr></table>				Option	Description	samba	SAMBA server.
Option	Description							
samba	SAMBA server.							
server	IPv4 or IPv6 address of the server.	string	Maximum length: 35					
period	Frequency for which the FortiProxy checks the server for new or changed files.	option	-	none				

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Check the server when the FortiProxy starts up.</td></tr><tr><td><i>daily</i></td><td>Check the server once a day.</td></tr><tr><td><i>weekly</i></td><td>Check the server once a week.</td></tr><tr><td><i>monthly</i></td><td>Check the server once a month.</td></tr></table>	Option	Description	<i>none</i>	Check the server when the FortiProxy starts up.	<i>daily</i>	Check the server once a day.	<i>weekly</i>	Check the server once a week.	<i>monthly</i>	Check the server once a month.			
	Option	Description												
	<i>none</i>	Check the server when the FortiProxy starts up.												
	<i>daily</i>	Check the server once a day.												
	<i>weekly</i>	Check the server once a week.												
<i>monthly</i>	Check the server once a month.													
vdom	Select the VDOM that can communicate with the file server.	option	-	mgmt										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mgmt</i></td><td>Communicate with the file server through the management VDOM.</td></tr><tr><td><i>current</i></td><td>Communicate with the file server through the VDOM containing this DLP fingerprint database configuration.</td></tr></table>	Option	Description	<i>mgmt</i>	Communicate with the file server through the management VDOM.	<i>current</i>	Communicate with the file server through the VDOM containing this DLP fingerprint database configuration.							
	Option	Description												
	<i>mgmt</i>	Communicate with the file server through the management VDOM.												
<i>current</i>	Communicate with the file server through the VDOM containing this DLP fingerprint database configuration.													
scan-subdirectories	Enable/disable scanning subdirectories to find files to create fingerprints from.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Scan subdirectories.</td></tr><tr><td><i>disable</i></td><td>Do not scan subdirectories.</td></tr></table>	Option	Description	<i>enable</i>	Scan subdirectories.	<i>disable</i>	Do not scan subdirectories.							
	Option	Description												
	<i>enable</i>	Scan subdirectories.												
<i>disable</i>	Do not scan subdirectories.													
scan-on-creation	Enable to keep the fingerprint database up to date when a file is added or changed on the server.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Keep the fingerprint database up to date when a file is added or changed on the server.</td></tr><tr><td><i>disable</i></td><td>Do not check for added or changed files on the server. Saves system resources.</td></tr></table>	Option	Description	<i>enable</i>	Keep the fingerprint database up to date when a file is added or changed on the server.	<i>disable</i>	Do not check for added or changed files on the server. Saves system resources.							
	Option	Description												
	<i>enable</i>	Keep the fingerprint database up to date when a file is added or changed on the server.												
<i>disable</i>	Do not check for added or changed files on the server. Saves system resources.													
remove-deleted	Enable to keep the fingerprint database up to date when a file is deleted from the server.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Keep the fingerprint database up to date when a file is deleted from the server.</td></tr><tr><td><i>disable</i></td><td>Do not check for deleted files on the server. Saves system resources.</td></tr></table>	Option	Description	<i>enable</i>	Keep the fingerprint database up to date when a file is deleted from the server.	<i>disable</i>	Do not check for deleted files on the server. Saves system resources.							
	Option	Description												
	<i>enable</i>	Keep the fingerprint database up to date when a file is deleted from the server.												
<i>disable</i>	Do not check for deleted files on the server. Saves system resources.													
keep-modified	Enable so that when a file is changed on the server the FortiProxy keeps the old fingerprint and adds a new fingerprint to the database.	option	-	enable										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Keep the old fingerprint and add a new fingerprint when a file is changed on the server.		
	<i>disable</i>	Replace the old fingerprint with the new fingerprint when a file is changed on the server.		
username	User name required to log into the file server.	string	Maximum length: 35	
password	Password required to log into the file server.	password	Not Specified	
file-path	Path on the server to the fingerprint files (max 119 characters).	string	Maximum length: 119	
file-pattern	Files matching this pattern on the server are fingerprinted. Optionally use the * and ? wildcards.	string	Maximum length: 35	*
sensitivity	Select a sensitivity or threat level for matches with this fingerprint database. Add sensitivities using sensitivity.	string	Maximum length: 35	
tod-hour	Hour of the day on which to scan the server.	integer	Minimum value: 0 Maximum value: 23	1
tod-min	Minute of the hour on which to scan the server.	integer	Minimum value: 0 Maximum value: 59	0
weekday	Day of the week on which to scan the server.	option	-	sunday
	Option	Description		
	<i>sunday</i>	Sunday		
	<i>monday</i>	Monday		
	<i>tuesday</i>	Tuesday		
	<i>wednesday</i>	Wednesday		
	<i>thursday</i>	Thursday		
	<i>friday</i>	Friday		
	<i>saturday</i>	Saturday		

Parameter	Description	Type	Size	Default
date	Day of the month on which to scan the server.	integer	Minimum value: 1 Maximum value: 31	1

config dlp profile

Configure DLP profiles.

```
config dlp profile
  Description: Configure DLP profiles.
  edit <name>
    set comment {var-string}
    set feature-set [flow|proxy]
    set replacemsg-group {string}
    config rule
      Description: Set up DLP rules for this profile.
      edit <id>
        set name {string}
        set severity [info|low|...]
        set type [file|message]
        set proto {option1}, {option2}, ...
        set filter-by [sensor|mip|...]
        set file-size {integer}
        set sensitivity <name1>, <name2>, ...
        set match-percentage {integer}
        set file-type {integer}
        set sensor <name1>, <name2>, ...
        set label {string}
        set archive [disable|enable]
        set action [allow|log-only|...]
        set expiry {user}
      next
    end
    set dlp-log [enable|disable]
    set nac-quar-log [enable|disable]
    set full-archive-proto {option1}, {option2}, ...
    set summary-proto {option1}, {option2}, ...
  next
end
```

config dlp profile

Parameter	Description	Type	Size	Default
name	Name of the DLP profile.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default																						
comment	Comment.	var-string	Maximum length: 255																							
feature-set	Flow/proxy feature set.	option	-	proxy																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>flow</i></td><td>Flow feature set.</td></tr><tr><td><i>proxy</i></td><td>Proxy feature set.</td></tr></table>				Option	Description	<i>flow</i>	Flow feature set.	<i>proxy</i>	Proxy feature set.																
	Option	Description																								
	<i>flow</i>	Flow feature set.																								
	<i>proxy</i>	Proxy feature set.																								
replacemsg-group	Replacement message group used by this DLP profile.	string	Maximum length: 35																							
dlp-log	Enable/disable DLP logging.	option	-	enable																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DLP logging.</td></tr><tr><td><i>disable</i></td><td>Disable DLP logging.</td></tr></table>				Option	Description	<i>enable</i>	Enable DLP logging.	<i>disable</i>	Disable DLP logging.																
	Option	Description																								
	<i>enable</i>	Enable DLP logging.																								
	<i>disable</i>	Disable DLP logging.																								
nac-quar-log	Enable/disable NAC quarantine logging.	option	-	disable																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NAC quarantine logging.</td></tr><tr><td><i>disable</i></td><td>Disable NAC quarantine logging.</td></tr></table>				Option	Description	<i>enable</i>	Enable NAC quarantine logging.	<i>disable</i>	Disable NAC quarantine logging.																
	Option	Description																								
	<i>enable</i>	Enable NAC quarantine logging.																								
	<i>disable</i>	Disable NAC quarantine logging.																								
full-archive-proto	Protocols to always content archive.	option	-																							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>smtp</i></td><td>SMTP.</td></tr><tr><td><i>pop3</i></td><td>POP3.</td></tr><tr><td><i>imap</i></td><td>IMAP.</td></tr><tr><td><i>http-get</i></td><td>HTTP GET.</td></tr><tr><td><i>http-post</i></td><td>HTTP POST.</td></tr><tr><td><i>ftp</i></td><td>FTP.</td></tr><tr><td><i>nntp</i></td><td>NNTP.</td></tr><tr><td><i>mapi</i></td><td>MAPI.</td></tr><tr><td><i>ssh</i></td><td>SFTP and SCP.</td></tr><tr><td><i>cifs</i></td><td>CIFS.</td></tr></table>				Option	Description	<i>smtp</i>	SMTP.	<i>pop3</i>	POP3.	<i>imap</i>	IMAP.	<i>http-get</i>	HTTP GET.	<i>http-post</i>	HTTP POST.	<i>ftp</i>	FTP.	<i>nntp</i>	NNTP.	<i>mapi</i>	MAPI.	<i>ssh</i>	SFTP and SCP.	<i>cifs</i>	CIFS.
	Option	Description																								
	<i>smtp</i>	SMTP.																								
	<i>pop3</i>	POP3.																								
	<i>imap</i>	IMAP.																								
	<i>http-get</i>	HTTP GET.																								
	<i>http-post</i>	HTTP POST.																								
	<i>ftp</i>	FTP.																								
	<i>nntp</i>	NNTP.																								
	<i>mapi</i>	MAPI.																								
	<i>ssh</i>	SFTP and SCP.																								
	<i>cifs</i>	CIFS.																								

Parameter	Description	Type	Size	Default
summary-proto	Protocols to always log summary.	option	-	
	Option	Description		
	<i>smtp</i>	SMTP.		
	<i>pop3</i>	POP3.		
	<i>imap</i>	IMAP.		
	<i>http-get</i>	HTTP GET.		
	<i>http-post</i>	HTTP POST.		
	<i>ftp</i>	FTP.		
	<i>nntp</i>	NNTP.		
	<i>mapi</i>	MAPI.		
	<i>ssh</i>	SFTP and SCP.		
	<i>cifs</i>	CIFS.		

config rule

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Filter name.	string	Maximum length: 35	
severity	Select the severity or threat level that matches this filter.	option	-	medium
	Option	Description		
	<i>info</i>	Informational.		
	<i>low</i>	Low.		
	<i>medium</i>	Medium.		
	<i>high</i>	High.		
	<i>critical</i>	Critical.		

Parameter	Description	Type	Size	Default																						
type	Select whether to check the content of messages (an email message) or files (downloaded files or email attachments).	option	-	file																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>file</td><td>Check the contents of downloaded or attached files.</td></tr><tr><td>message</td><td>Check the contents of email messages, web pages, etc.</td></tr></table>	Option	Description	file	Check the contents of downloaded or attached files.	message	Check the contents of email messages, web pages, etc.																			
Option	Description																									
file	Check the contents of downloaded or attached files.																									
message	Check the contents of email messages, web pages, etc.																									
proto	Check messages or files over one or more of these protocols.	option	-																							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>smtp</td><td>SMTP.</td></tr><tr><td>pop3</td><td>POP3.</td></tr><tr><td>imap</td><td>IMAP.</td></tr><tr><td>http-get</td><td>HTTP GET.</td></tr><tr><td>http-post</td><td>HTTP POST.</td></tr><tr><td>ftp</td><td>FTP.</td></tr><tr><td>nntp</td><td>NNTP.</td></tr><tr><td>mapi</td><td>MAPI.</td></tr><tr><td>ssh</td><td>SFTP and SCP.</td></tr><tr><td>cifs</td><td>CIFS.</td></tr></table>	Option	Description	smtp	SMTP.	pop3	POP3.	imap	IMAP.	http-get	HTTP GET.	http-post	HTTP POST.	ftp	FTP.	nntp	NNTP.	mapi	MAPI.	ssh	SFTP and SCP.	cifs	CIFS.			
Option	Description																									
smtp	SMTP.																									
pop3	POP3.																									
imap	IMAP.																									
http-get	HTTP GET.																									
http-post	HTTP POST.																									
ftp	FTP.																									
nntp	NNTP.																									
mapi	MAPI.																									
ssh	SFTP and SCP.																									
cifs	CIFS.																									
filter-by	Select the type of content to match.	option	-	none																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sensor</td><td>Use DLP sensors to match content.</td></tr><tr><td>mip</td><td>Use MIP label dictionary to match content.</td></tr><tr><td>fingerprint</td><td>Match against a fingerprint sensitivity.</td></tr><tr><td>encrypted</td><td>Look for encrypted files.</td></tr><tr><td>none</td><td>No content scan.</td></tr></table>	Option	Description	sensor	Use DLP sensors to match content.	mip	Use MIP label dictionary to match content.	fingerprint	Match against a fingerprint sensitivity.	encrypted	Look for encrypted files.	none	No content scan.													
Option	Description																									
sensor	Use DLP sensors to match content.																									
mip	Use MIP label dictionary to match content.																									
fingerprint	Match against a fingerprint sensitivity.																									
encrypted	Look for encrypted files.																									
none	No content scan.																									
file-size	Match files this size or larger.	integer	Minimum value: 0 Maximum value: 4294967295	0																						

Parameter	Description	Type	Size	Default										
sensitivity <name>	Select a DLP file pattern sensitivity to match. Select a DLP sensitivity.	string	Maximum length: 35											
match- percentage	Percentage of fingerprints in the fingerprint databases designated with the selected sensitivity to match.	integer	Minimum value: 1 Maximum value: 100	10										
file-type	Select the number of a DLP file pattern table to match.	integer	Minimum value: 0 Maximum value: 4294967295	0										
sensor <name>	Select DLP sensors. Address name.	string	Maximum length: 35											
label	MIP label dictionary.	string	Maximum length: 35											
archive	Enable/disable DLP archiving.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>No DLP archiving.</td></tr><tr><td>enable</td><td>Enable full DLP archiving.</td></tr></table>				Option	Description	disable	No DLP archiving.	enable	Enable full DLP archiving.				
Option	Description													
disable	No DLP archiving.													
enable	Enable full DLP archiving.													
action	Action to take with content that this DLP profile matches.	option	-	allow										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow the content to pass through the FortiProxy and do not create a log message.</td></tr><tr><td>log-only</td><td>Allow the content to pass through the FortiProxy, but write a log message.</td></tr><tr><td>block</td><td>Block the content and write a log message.</td></tr><tr><td>quarantine-ip</td><td>Quarantine all traffic from the IP address and write a log message.</td></tr></table>				Option	Description	allow	Allow the content to pass through the FortiProxy and do not create a log message.	log-only	Allow the content to pass through the FortiProxy, but write a log message.	block	Block the content and write a log message.	quarantine-ip	Quarantine all traffic from the IP address and write a log message.
Option	Description													
allow	Allow the content to pass through the FortiProxy and do not create a log message.													
log-only	Allow the content to pass through the FortiProxy, but write a log message.													
block	Block the content and write a log message.													
quarantine-ip	Quarantine all traffic from the IP address and write a log message.													
expiry	Quarantine duration in days, hours, minutes (format = dddhmm).	user	Not Specified	5m										

config dlp sensitivity

Create self-explanatory DLP sensitivity levels to be used when setting sensitivity under config fp-doc-source.

```
config dlp sensitivity
    Description: Create self-explanatory DLP sensitivity levels to be used when setting
```

```
sensitivity under config fp-doc-source.
edit <name>
next
end
```

config dlp sensitivity

Parameter	Description	Type	Size	Default
name	DLP Sensitivity Levels.	string	Maximum length: 35	

config dlp sensor

Configure sensors used by DLP blocking.

```
config dlp sensor
  Description: Configure sensors used by DLP blocking.
  edit <name>
    set match-type [match-all|match-any|...]
    set eval {string}
    set comment {var-string}
    config entries
      Description: DLP sensor entries.
      edit <id>
        set dictionary {string}
        set count {integer}
        set status [enable|disable]
      next
    end
  next
end
```

config dlp sensor

Parameter	Description	Type	Size	Default								
name	Name of table containing the sensor.	string	Maximum length: 35									
match-type	Logical relation between entries.	option	-	match-any								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>match-all</i></td><td>Match all entries.</td></tr><tr><td><i>match-any</i></td><td>Match any entries.</td></tr><tr><td><i>match-eval</i></td><td>Match an expression evaluation.</td></tr></table>				Option	Description	<i>match-all</i>	Match all entries.	<i>match-any</i>	Match any entries.	<i>match-eval</i>	Match an expression evaluation.
Option	Description											
<i>match-all</i>	Match all entries.											
<i>match-any</i>	Match any entries.											
<i>match-eval</i>	Match an expression evaluation.											

Parameter	Description	Type	Size	Default
eval	Expression to evaluate.	string	Maximum length: 255	
comment	Optional comments.	var-string	Maximum length: 255	

config entries

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 1 Maximum value: 32	0
dictionary	Select a DLP dictionary.	string	Maximum length: 35	
count	Count of dictionary matches to trigger sensor entry match.	integer	Minimum value: 1 Maximum value: 255	1
status	Enable/disable this entry.	option	-	enable
	Option	Description		
	enable	Enable this entry.		
	disable	Disable this entry.		

config dlp settings

Designate logical storage for DLP fingerprint database.

```

config dlp settings
    Description: Designate logical storage for DLP fingerprint database.
    set storage-device {string}
    set size {integer}
    set db-mode [stop-adding|remove-modified-then-oldest|...]
    set cache-mem-percent {integer}
    set chunk-size {integer}
end

```

config dlp settings

Parameter	Description	Type	Size	Default
storage-device	Storage device name.	string	Maximum length: 35	
size	Maximum total size of files within the storage (MB).	integer	Minimum value: 16 Maximum value: 4294967295	16
db-mode	Behavior when the maximum size is reached.	option	-	stop-adding
	Option	Description		
	stop-adding	Stop adding entries.		
	remove-modified-then-oldest	Remove modified chunks first, then oldest file entries.		
	remove-oldest	Remove the oldest files first.		
cache-mem-percent	Maximum percentage of available memory allocated to caching.	integer	Minimum value: 1 Maximum value: 15	2
chunk-size	Maximum fingerprint chunk size. Caution, changing this setting will flush the entire database.	integer	Minimum value: 100 Maximum value: 100000	2800

dnsfilter

This section includes syntax for the following commands:

- [config dnsfilter domain-filter on page 134](#)
- [config dnsfilter profile on page 135](#)

config dnsfilter domain-filter

Configure DNS domain filters.

```
config dnsfilter domain-filter
  Description: Configure DNS domain filters.
  edit <id>
    set name {string}
    set comment {var-string}
    config entries
      Description: DNS domain filter entries.
      edit <id>
        set domain {string}
        set type [simple|regex|...]
        set action [block|allow|...]
        set status [enable|disable]
      next
    end
  next
end
```

config dnsfilter domain-filter

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

config entries

Parameter	Description	Type	Size	Default								
id	Id.	integer	Minimum value: 0 Maximum value: 4294967295	0								
domain	Domain entries to be filtered.	string	Maximum length: 511									
type	DNS domain filter type.	option	-	simple								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>simple</i></td><td>Simple domain string.</td></tr><tr><td><i>regex</i></td><td>Regular expression domain string.</td></tr><tr><td><i>wildcard</i></td><td>Wildcard domain string.</td></tr></table>				Option	Description	<i>simple</i>	Simple domain string.	<i>regex</i>	Regular expression domain string.	<i>wildcard</i>	Wildcard domain string.
Option	Description											
<i>simple</i>	Simple domain string.											
<i>regex</i>	Regular expression domain string.											
<i>wildcard</i>	Wildcard domain string.											
action	Action to take for domain filter matches.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Block DNS requests matching the domain filter.</td></tr><tr><td><i>allow</i></td><td>Allow DNS requests matching the domain filter without logging.</td></tr><tr><td><i>monitor</i></td><td>Allow DNS requests matching the domain filter with logging.</td></tr></table>				Option	Description	<i>block</i>	Block DNS requests matching the domain filter.	<i>allow</i>	Allow DNS requests matching the domain filter without logging.	<i>monitor</i>	Allow DNS requests matching the domain filter with logging.
Option	Description											
<i>block</i>	Block DNS requests matching the domain filter.											
<i>allow</i>	Allow DNS requests matching the domain filter without logging.											
<i>monitor</i>	Allow DNS requests matching the domain filter with logging.											
status	Enable/disable this domain filter.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this domain filter.</td></tr><tr><td><i>disable</i></td><td>Disable this domain filter.</td></tr></table>				Option	Description	<i>enable</i>	Enable this domain filter.	<i>disable</i>	Disable this domain filter.		
Option	Description											
<i>enable</i>	Enable this domain filter.											
<i>disable</i>	Disable this domain filter.											

config dnsfilter profile

Configure DNS domain filter profile.

```
config dnsfilter profile
  Description: Configure DNS domain filter profile.
  edit <name>
    set comment {var-string}
    config domain-filter
      Description: Domain filter settings.
      set domain-filter-table {integer}
    end
```

```

config ftgd-dns
    Description: FortiGuard DNS Filter settings.
    set options {option1}, {option2}, ...
    config filters
        Description: FortiGuard DNS domain filters.
        edit <id>
            set category {integer}
            set action [block|monitor]
            set log [enable|disable]
        next
    end
end
set log-all-domain [enable|disable]
set sdns-ftgd-err-log [enable|disable]
set sdns-domain-log [enable|disable]
set block-action [block|redirect|...]
set redirect-portal {ipv4-address}
set redirect-portal6 {ipv6-address}
set block-botnet [disable|enable]
set safe-search [disable|enable]
set youtube-restrict [strict|moderate]
set external-ip-blocklist <name1>, <name2>, ...
config dns-translation
    Description: DNS translation settings.
    edit <id>
        set addr-type [ipv4|ipv6]
        set src {ipv4-address}
        set dst {ipv4-address}
        set netmask {ipv4-netmask}
        set status [enable|disable]
        set src6 {ipv6-address}
        set dst6 {ipv6-address}
        set prefix {integer}
    next
end
set strip-ech [disable|enable]
next
end

```

config dnsfilter profile

Parameter	Description	Type	Size	Default
name	Profile name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
log-all-domain	Enable/disable logging of all domains visited (detailed DNS logging).	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable logging of all domains visited.		
	<i>disable</i>	Disable logging of all domains visited.		
sdns-ftgd-err-log	Enable/disable FortiGuard SDNS rating error logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable FortiGuard SDNS rating error logging.		
	<i>disable</i>	Disable FortiGuard SDNS rating error logging.		
sdns-domain-log	Enable/disable domain filtering and botnet domain logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable domain filtering and botnet domain logging.		
	<i>disable</i>	Disable domain filtering and botnet domain logging.		
block-action	Action to take for blocked domains.	option	-	redirect
	Option	Description		
	<i>block</i>	Return NXDOMAIN for blocked domains.		
	<i>redirect</i>	Redirect blocked domains to SDNS portal.		
	<i>block-sevrfail</i>	Return SERVFAIL for blocked domains.		
redirect-portal	IPv4 address of the SDNS redirect portal.	ipv4-address	Not Specified	0.0.0.0
redirect-portal6	IPv6 address of the SDNS redirect portal.	ipv6-address	Not Specified	::
block-botnet	Enable/disable blocking botnet C&C DNS lookups.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable blocking botnet C&C DNS lookups.		
	<i>enable</i>	Enable blocking botnet C&C DNS lookups.		
safe-search	Enable/disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.		
	<i>enable</i>	Enable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.		
youtube-restrict	Set safe search for YouTube restriction level.	option	-	strict
	Option	Description		
	<i>strict</i>	Enable strict safe search for YouTube.		
	<i>moderate</i>	Enable moderate safe search for YouTube.		
external-ip-blocklist <name>	One or more external IP block lists. External domain block list name.	string	Maximum length: 79	
strip-ech	Enable/disable removal of the encrypted client hello service parameter from supporting DNS RRs.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable removal of the encrypted client hello service parameter from supporting DNS RRs.		
	<i>enable</i>	Enable removal of the encrypted client hello service parameter from supporting DNS RRs.		

config domain-filter

Parameter	Description	Type	Size	Default
domain-filter-table	DNS domain filter table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config ftgd-dns

Parameter	Description	Type	Size	Default
options	FortiGuard DNS filter options.	option	-	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>error-allow</i>	Allow all domains when FortiGuard DNS servers fail.		
	<i>ftgd-disable</i>	Disable FortiGuard DNS domain rating.		

config filters

Parameter	Description	Type	Size	Default
id	ID number.	integer	Minimum value: 0 Maximum value: 255	0
category	Category number.	integer	Minimum value: 0 Maximum value: 255	0
action	Action to take for DNS requests matching the category.	option	-	monitor
	Option	Description		
	<i>block</i>	Block DNS requests matching the category.		
	<i>monitor</i>	Allow DNS requests matching the category and log the result.		
log	Enable/disable DNS filter logging for this DNS profile.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable DNS filter logging.		
	<i>disable</i>	Disable DNS filter logging.		

config dns-translation

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
addr-type	DNS translation type (IPv4 or IPv6).	option	-	ipv4

Parameter	Description	Type	Size	Default							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ipv4</i></td><td>IPv4 address type.</td></tr><tr><td><i>ipv6</i></td><td>IPv6 address type.</td></tr></table>		Option	Description	<i>ipv4</i>	IPv4 address type.	<i>ipv6</i>	IPv6 address type.			
	Option	Description									
	<i>ipv4</i>	IPv4 address type.									
<i>ipv6</i>	IPv6 address type.										
src	IPv4 address or subnet on the internal network to compare with the resolved address in DNS query replies. If the resolved address matches, the resolved address is substituted with dst.	ipv4-address	Not Specified	0.0.0.0							
dst	IPv4 address or subnet on the external network to substitute for the resolved address in DNS query replies. Can be single IP address or subnet on the external network, but number of addresses must equal number of mapped IP addresses in src.	ipv4-address	Not Specified	0.0.0.0							
netmask	If src and dst are subnets rather than single IP addresses, enter the netmask for both src and dst.	ipv4-netmask	Not Specified	255.255.255.255							
status	Enable/disable this DNS translation entry.	option	-	enable							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this DNS translation.</td></tr><tr><td><i>disable</i></td><td>Disable this DNS translation.</td></tr></table>		Option	Description	<i>enable</i>	Enable this DNS translation.	<i>disable</i>	Disable this DNS translation.			
	Option	Description									
	<i>enable</i>	Enable this DNS translation.									
<i>disable</i>	Disable this DNS translation.										
src6	IPv6 address or subnet on the internal network to compare with the resolved address in DNS query replies. If the resolved address matches, the resolved address is substituted with dst6.	ipv6-address	Not Specified	::							
dst6	IPv6 address or subnet on the external network to substitute for the resolved address in DNS query replies. Can be single IP address or subnet on the external network, but number of addresses must equal number of mapped IP addresses in src6.	ipv6-address	Not Specified	::							
prefix	If src6 and dst6 are subnets rather than single IP addresses, enter the prefix for both src6 and dst6.	integer	Minimum value: 1 Maximum value: 128	128							

emailfilter

This section includes syntax for the following commands:

- [config emailfilter block-allow-list on page 141](#)
- [config emailfilter bword on page 143](#)
- [config emailfilter dnsbl on page 145](#)
- [config emailfilter fortishield on page 147](#)
- [config emailfilter iptrust on page 147](#)
- [config emailfilter mheader on page 149](#)
- [config emailfilter options on page 150](#)
- [config emailfilter profile on page 151](#)

config emailfilter block-allow-list

Configure anti-spam block/allow list.

```
config emailfilter block-allow-list
  Description: Configure anti-spam block/allow list.
  edit <id>
    set name {string}
    set comment {var-string}
    config entries
      Description: Anti-spam block/allow entries.
      edit <id>
        set status [enable|disable]
        set type [ip|email-to|...]
        set action [reject|spam|...]
        set addr-type [ipv4|ipv6]
        set ip4-subnet {ipv4-classnet}
        set ip6-subnet {ipv6-network}
        set pattern-type [wildcard|regexp]
        set pattern {string}
      next
    end
  next
end
```

config emailfilter block-allow-list

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

config entries

Parameter	Description	Type	Size	Default
status	Enable/disable status.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable status.		
	<i>disable</i>	Disable status.		
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
type	Entry type.	option	-	ip
	Option	Description		
	<i>ip</i>	By IP address.		
	<i>email-to</i>	By email recipient.		
	<i>email-from</i>	By email sender.		
	<i>subject</i>	By email subject.		
action	Reject, mark as spam or good email.	option	-	spam
	Option	Description		
	<i>reject</i>	Reject the connection.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>spam</i>	Mark as spam email.		
	<i>clear</i>	Mark as good email.		
addr-type	IP address type.	option	-	ipv4
	Option	Description		
	<i>ipv4</i>	IPv4 Address type.		
	<i>ipv6</i>	IPv6 Address type.		
ip4-subnet	IPv4 network address/subnet mask bits.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
ip6-subnet	IPv6 network address/subnet mask bits.	ipv6-network	Not Specified	::/128
pattern-type	Wildcard pattern or regular expression.	option	-	wildcard
	Option	Description		
	<i>wildcard</i>	Wildcard pattern.		
	<i>regexp</i>	Perl regular expression.		
pattern	Pattern to match.	string	Maximum length: 127	

config emailfilter bword

Configure AntiSpam banned word list.

```
config emailfilter bword
  Description: Configure AntiSpam banned word list.
  edit <id>
    set name {string}
    set comment {var-string}
    config entries
      Description: Spam filter banned word.
      edit <id>
        set status [enable|disable]
        set pattern {string}
        set pattern-type [wildcard|regexp]
        set action [spam|clear]
        set where [subject|body|...]
        set language [western|simch|...]
        set score {integer}
      next
    end
```

```

    next
end

```

config emailfilter bword

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

config entries

Parameter	Description	Type	Size	Default
status	Enable/disable status.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable status.		
	<i>disable</i>	Disable status.		
id	Banned word entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
pattern	Pattern for the banned word.	string	Maximum length: 127	
pattern-type	Wildcard pattern or regular expression.	option	-	wildcard
	Option	Description		
	<i>wildcard</i>	Wildcard pattern.		
	<i>regex</i>	Perl regular expression.		
action	Mark spam or good.	option	-	spam

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>spam</i></td><td>Mark as spam email.</td></tr><tr><td><i>clear</i></td><td>Mark as good email.</td></tr></table>	Option	Description	<i>spam</i>	Mark as spam email.	<i>clear</i>	Mark as good email.															
	Option	Description																				
	<i>spam</i>	Mark as spam email.																				
<i>clear</i>	Mark as good email.																					
where	Component of the email to be scanned.	option	-	all																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>subject</i></td><td>Banned word in email subject.</td></tr><tr><td><i>body</i></td><td>Banned word in email body.</td></tr><tr><td><i>all</i></td><td>Banned word in both subject and body.</td></tr></table>	Option	Description	<i>subject</i>	Banned word in email subject.	<i>body</i>	Banned word in email body.	<i>all</i>	Banned word in both subject and body.													
	Option	Description																				
	<i>subject</i>	Banned word in email subject.																				
	<i>body</i>	Banned word in email body.																				
<i>all</i>	Banned word in both subject and body.																					
language	Language for the banned word.	option	-	western																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>western</i></td><td>Western.</td></tr><tr><td><i>simch</i></td><td>Simplified Chinese.</td></tr><tr><td><i>trach</i></td><td>Traditional Chinese.</td></tr><tr><td><i>japanese</i></td><td>Japanese.</td></tr><tr><td><i>korean</i></td><td>Korean.</td></tr><tr><td><i>french</i></td><td>French.</td></tr><tr><td><i>thai</i></td><td>Thai.</td></tr><tr><td><i>spanish</i></td><td>Spanish.</td></tr></table>	Option	Description	<i>western</i>	Western.	<i>simch</i>	Simplified Chinese.	<i>trach</i>	Traditional Chinese.	<i>japanese</i>	Japanese.	<i>korean</i>	Korean.	<i>french</i>	French.	<i>thai</i>	Thai.	<i>spanish</i>	Spanish.			
	Option	Description																				
	<i>western</i>	Western.																				
	<i>simch</i>	Simplified Chinese.																				
	<i>trach</i>	Traditional Chinese.																				
	<i>japanese</i>	Japanese.																				
	<i>korean</i>	Korean.																				
	<i>french</i>	French.																				
<i>thai</i>	Thai.																					
<i>spanish</i>	Spanish.																					
score	Score value.	integer	Minimum value: 1 Maximum value: 99999	10																		

config emailfilter dnsbl

Configure AntiSpam DNSBL/ORBL.

```
config emailfilter dnsbl
  Description: Configure AntiSpam DNSBL/ORBL.
  edit <id>
    set name {string}
    set comment {var-string}
    config entries
      Description: Spam filter DNSBL and ORBL server.
    edit <id>
```

```

        set status [enable|disable]
        set server {string}
        set action [reject|spam]
    next
end
next
end

```

config emailfilter dnsbl

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

config entries

Parameter	Description	Type	Size	Default
status	Enable/disable status.	option	-	enable
	Option	Description		
	enable	Enable status.		
	disable	Disable status.		
id	DNSBL/ORBL entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
server	DNSBL or ORBL server name.	string	Maximum length: 127	
action	Reject connection or mark as spam email.	option	-	spam
	Option	Description		
	reject	Reject the connection.		
	spam	Mark as spam email.		

config emailfilter fortishield

Configure FortiGuard - AntiSpam.

```
config emailfilter fortishield
    Description: Configure FortiGuard - AntiSpam.
    set spam-submit-srv {string}
    set spam-submit-force [enable|disable]
    set spam-submit-txt2htm [enable|disable]
end
```

config emailfilter fortishield

Parameter	Description	Type	Size	Default
spam-submit-srv	Hostname of the spam submission server.	string	Maximum length: 63	www.nospammer.net
spam-submit-force	Enable/disable force insertion of a new mime entity for the submission text.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
spam-submit-txt2htm	Enable/disable conversion of text email to HTML email.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config emailfilter iptrust

Configure AntiSpam IP trust.

```
config emailfilter iptrust
    Description: Configure AntiSpam IP trust.
    edit <id>
        set name {string}
        set comment {var-string}
    config entries
        Description: Spam filter trusted IP addresses.
        edit <id>
            set status [enable|disable]
            set addr-type [ipv4|ipv6]
```

```

        set ip4-subnet {ipv4-classnet}
        set ip6-subnet {ipv6-network}
    next
end
next
end

```

config emailfilter iptrust

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

config entries

Parameter	Description	Type	Size	Default
status	Enable/disable status.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable status.		
	<i>disable</i>	Disable status.		
id	Trusted IP entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
addr-type	Type of address.	option	-	ipv4
	Option	Description		
	<i>ipv4</i>	IPv4 Address type.		
	<i>ipv6</i>	IPv6 Address type.		
ip4-subnet	IPv4 network address or network address/subnet mask bits.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

Parameter	Description	Type	Size	Default
ipv6-subnet	IPv6 network address/subnet mask bits.	ipv6-network	Not Specified	::/128

config emailfilter mheader

Configure AntiSpam MIME header.

```
config emailfilter mheader
    Description: Configure AntiSpam MIME header.
    edit <id>
        set name {string}
        set comment {var-string}
        config entries
            Description: Spam filter mime header content.
            edit <id>
                set status [enable|disable]
                set fieldname {string}
                set fieldbody {string}
                set pattern-type [wildcard|regexp]
                set action [spam|clear]
            next
        end
    next
end
```

config emailfilter mheader

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

config entries

Parameter	Description	Type	Size	Default
status	Enable/disable status.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable status.		
	<i>disable</i>	Disable status.		
id	Mime header entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
fieldname	Pattern for header field name.	string	Maximum length: 63	
fieldbody	Pattern for the header field body.	string	Maximum length: 127	
pattern-type	Wildcard pattern or regular expression.	option	-	wildcard
	Option	Description		
	<i>wildcard</i>	Wildcard pattern.		
	<i>regexp</i>	Perl regular expression.		
action	Mark spam or good.	option	-	spam
	Option	Description		
	<i>spam</i>	Mark as spam email.		
	<i>clear</i>	Mark as good email.		

config emailfilter options

Configure AntiSpam options.

```
config emailfilter options
    Description: Configure AntiSpam options.
    set dns-timeout {integer}
end
```

config emailfilter options

Parameter	Description	Type	Size	Default
dns-timeout	DNS query time out.	integer	Minimum value: 1 Maximum value: 30	7

config emailfilter profile

Configure Email Filter profiles.

```
config emailfilter profile
  Description: Configure Email Filter profiles.
  edit <name>
    set comment {var-string}
    set replacemsg-group {string}
    set spam-log [disable|enable]
    set spam-log-fortiguard-response [disable|enable]
    set spam-filtering [enable|disable]
    set external [enable|disable]
    set options {option1}, {option2}, ...
  config imap
    Description: IMAP.
    set log-all [disable|enable]
    set action [pass|tag]
    set tag-type {option1}, {option2}, ...
    set tag-msg {string}
  end
  config pop3
    Description: POP3.
    set log-all [disable|enable]
    set action [pass|tag]
    set tag-type {option1}, {option2}, ...
    set tag-msg {string}
  end
  config smtp
    Description: SMTP.
    set log-all [disable|enable]
    set action [pass|tag|...]
    set tag-type {option1}, {option2}, ...
    set tag-msg {string}
    set hdrp [disable|enable]
    set local-override [disable|enable]
  end
  config mapi
    Description: MAPI.
    set log-all [disable|enable]
    set action [pass|discard]
  end
  config msn-hotmail
```

```

        Description: MSN Hotmail.
        set log-all [disable|enable]
    end
    config yahoo-mail
        Description: Yahoo! Mail.
        set log-all [disable|enable]
    end
    config gmail
        Description: Gmail.
        set log-all [disable|enable]
    end
    config other-webmails
        Description: Other supported webmails.
        set log-all [disable|enable]
    end
    set spam-bword-threshold {integer}
    set spam-bword-table {integer}
    set spam-bal-table {integer}
    set spam-mheader-table {integer}
    set spam-rbl-table {integer}
    set spam-iptrust-table {integer}
next
end

```

config emailfilter profile

Parameter	Description	Type	Size	Default
name	Profile name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
replacemsg-group	Replacement message group.	string	Maximum length: 35	
spam-log	Enable/disable spam logging for email filtering.	option	-	enable
	OptionDescription			
	disableDisable spam logging for email filtering.			
	enableEnable spam logging for email filtering.			
spam-log-fortiguard-response	Enable/disable logging FortiGuard spam response.	option	-	disable
	OptionDescription			
	disableDisable logging FortiGuard spam response.			
	enableEnable logging FortiGuard spam response.			

Parameter	Description	Type	Size	Default																								
spam-filtering	Enable/disable spam filtering.	option	-	disable																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																					
	Option	Description																										
	<i>enable</i>	Enable setting.																										
<i>disable</i>	Disable setting.																											
external	Enable/disable external Email inspection.	option	-	disable																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																					
	Option	Description																										
	<i>enable</i>	Enable setting.																										
<i>disable</i>	Disable setting.																											
options	Options.	option	-																									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bannedword</i></td><td>Content block.</td></tr><tr><td><i>spambal</i></td><td>Block/allow list.</td></tr><tr><td><i>spamfsip</i></td><td>Email IP address FortiGuard AntiSpam block list check.</td></tr><tr><td><i>spamfssubmit</i></td><td>Add FortiGuard AntiSpam spam submission text.</td></tr><tr><td><i>spamfschksum</i></td><td>Email checksum FortiGuard AntiSpam check.</td></tr><tr><td><i>spamfsurl</i></td><td>Email content URL FortiGuard AntiSpam check.</td></tr><tr><td><i>spamhelodns</i></td><td>Email helo/ehlo domain DNS check.</td></tr><tr><td><i>spamraddrdns</i></td><td>Email return address DNS check.</td></tr><tr><td><i>spamrbl</i></td><td>Email DNSBL & ORBL check.</td></tr><tr><td><i>spamhdrcheck</i></td><td>Email mime header check.</td></tr><tr><td><i>spamfsphish</i></td><td>Email content phishing URL FortiGuard AntiSpam check.</td></tr></table>	Option	Description	<i>bannedword</i>	Content block.	<i>spambal</i>	Block/allow list.	<i>spamfsip</i>	Email IP address FortiGuard AntiSpam block list check.	<i>spamfssubmit</i>	Add FortiGuard AntiSpam spam submission text.	<i>spamfschksum</i>	Email checksum FortiGuard AntiSpam check.	<i>spamfsurl</i>	Email content URL FortiGuard AntiSpam check.	<i>spamhelodns</i>	Email helo/ehlo domain DNS check.	<i>spamraddrdns</i>	Email return address DNS check.	<i>spamrbl</i>	Email DNSBL & ORBL check.	<i>spamhdrcheck</i>	Email mime header check.	<i>spamfsphish</i>	Email content phishing URL FortiGuard AntiSpam check.			
	Option	Description																										
	<i>bannedword</i>	Content block.																										
	<i>spambal</i>	Block/allow list.																										
	<i>spamfsip</i>	Email IP address FortiGuard AntiSpam block list check.																										
	<i>spamfssubmit</i>	Add FortiGuard AntiSpam spam submission text.																										
	<i>spamfschksum</i>	Email checksum FortiGuard AntiSpam check.																										
	<i>spamfsurl</i>	Email content URL FortiGuard AntiSpam check.																										
	<i>spamhelodns</i>	Email helo/ehlo domain DNS check.																										
	<i>spamraddrdns</i>	Email return address DNS check.																										
	<i>spamrbl</i>	Email DNSBL & ORBL check.																										
<i>spamhdrcheck</i>	Email mime header check.																											
<i>spamfsphish</i>	Email content phishing URL FortiGuard AntiSpam check.																											
spam-bword-threshold	Spam banned word threshold.	integer	Minimum value: 0 Maximum value: 2147483647	10																								
spam-bword-table	Anti-spam banned word table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0																								

Parameter	Description	Type	Size	Default
spam-bal-table	Anti-spam block/allow list table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
spam-mheader-table	Anti-spam MIME header table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
spam-rbl-table	Anti-spam DNSBL table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
spam-iptrust-table	Anti-spam IP trust table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config imap

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable logging of all email traffic.		
	<i>enable</i>	Enable logging of all email traffic.		
action	Action for spam email.	option	-	tag
	Option	Description		
	<i>pass</i>	Allow spam email to pass through.		
	<i>tag</i>	Tag spam email with configured text in subject or header.		
tag-type	Tag subject or header for spam email.	option	-	subject spaminfo

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>subject</i>	Prepend text to spam email subject.		
	<i>header</i>	Append a user defined mime header to spam email.		
	<i>spaminfo</i>	Append spam info to spam email header.		
tag-msg	Subject text or header added to spam email.	string	Maximum length: 63	Spam

config pop3

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable logging of all email traffic.		
	<i>enable</i>	Enable logging of all email traffic.		
action	Action for spam email.	option	-	tag
	Option	Description		
	<i>pass</i>	Allow spam email to pass through.		
	<i>tag</i>	Tag spam email with configured text in subject or header.		
tag-type	Tag subject or header for spam email.	option	-	subject spaminfo
	Option	Description		
	<i>subject</i>	Prepend text to spam email subject.		
	<i>header</i>	Append a user defined mime header to spam email.		
	<i>spaminfo</i>	Append spam info to spam email header.		
tag-msg	Subject text or header added to spam email.	string	Maximum length: 63	Spam

config smtp

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable logging of all email traffic.		
	<i>enable</i>	Enable logging of all email traffic.		
action	Action for spam email.	option	-	discard
	Option	Description		
	<i>pass</i>	Allow spam email to pass through.		
	<i>tag</i>	Tag spam email with configured text in subject or header.		
	<i>discard</i>	Discard (block) spam email.		
tag-type	Tag subject or header for spam email.	option	-	subject spaminfo
	Option	Description		
	<i>subject</i>	Prepend text to spam email subject.		
	<i>header</i>	Append a user defined mime header to spam email.		
	<i>spaminfo</i>	Append spam info to spam email header.		
tag-msg	Subject text or header added to spam email.	string	Maximum length: 63	Spam
hdrip	Enable/disable SMTP email header IP checks for spamfsip, spamrbl, and spambal filters.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable SMTP email header IP checks for spamfsip, spamrbl, and spambal filters.		
	<i>enable</i>	Enable SMTP email header IP checks for spamfsip, spamrbl, and spambal filters.		
local-override	Enable/disable local filter to override SMTP remote check result.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable local filter to override SMTP remote check result.		
	<i>enable</i>	Enable local filter to override SMTP remote check result.		

config mapi

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable logging of all email traffic.		
	<i>enable</i>	Enable logging of all email traffic.		
action	Action for spam email.	option	-	pass
	Option	Description		
	<i>pass</i>	Allow spam email to pass through.		
	<i>discard</i>	Discard (block) spam email.		

config msn-hotmail

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable logging of all email traffic.		
	<i>enable</i>	Enable logging of all email traffic.		

config yahoo-mail

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable logging of all email traffic.		
	<i>enable</i>	Enable logging of all email traffic.		

config gmail

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable logging of all email traffic.		
	<i>enable</i>	Enable logging of all email traffic.		

config other-webmails

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable logging of all email traffic.		
	<i>enable</i>	Enable logging of all email traffic.		

endpoint-control

This section includes syntax for the following commands:

- [config endpoint-control fctems on page 159](#)

config endpoint-control fctems

Configure FortiClient Enterprise Management Server (EMS) entries.

```
config endpoint-control fctems
  Description: Configure FortiClient Enterprise Management Server (EMS) entries.
  edit <ems-id>
    set status [enable|disable]
    set name {string}
    set dirty-reason [none|mismatched-ems-sn]
    set fortinetone-cloud-authentication [enable|disable]
    set server {string}
    set https-port {integer}
    set serial-number {string}
    set tenant-id {string}
    set source-ip {ipv4-address-any}
    set pull-sysinfo [enable|disable]
    set pull-vulnerabilities [enable|disable]
    set pull-avatars [enable|disable]
    set pull-tags [enable|disable]
    set pull-malware-hash [enable|disable]
    set cloud-server-type [production|alpha|...]
    set capabilities {option1}, {option2}, ...
    set call-timeout {integer}
    set out-of-sync-threshold {integer}
    set websocket-override [disable|enable]
    set preserve-ssl-session [enable|disable]
    set interface-select-method [auto|specify]
    set interface {string}
    set trust-ca-cn [enable|disable]
  next
end
```

config endpoint-control fctems

Parameter	Description	Type	Size	Default
ems-id	EMS ID in order.	integer	Minimum value: 1 Maximum value: 7	0
status	Enable or disable this EMS configuration.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable EMS configuration and operation.	
	<i>disable</i>		Disable EMS configuration and operation.	
name	FortiClient Enterprise Management Server (EMS) name.	string	Maximum length: 35	
dirty-reason	Dirty Reason for FortiClient EMS.	option	-	none
	Option		Description	
	<i>none</i>		FortiClient EMS entry not dirty.	
	<i>mismatched-ems-sn</i>		FortiClient EMS entry dirty because EMS SN is mismatched with configured SN.	
fortinetone-cloud-authentication	Enable/disable authentication of FortiClient EMS Cloud through FortiCloud account.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable authentication of FortiClient EMS Cloud through the use of FortiCloud account.	
	<i>disable</i>		Disable authentication of FortiClient EMS Cloud through the use of FortiCloud account.	
server	FortiClient EMS FQDN or IPv4 address.	string	Maximum length: 255	
https-port	FortiClient EMS HTTPS access port number.	integer	Minimum value: 1 Maximum value: 65535	443
serial-number	EMS Serial Number.	string	Maximum length: 16	

Parameter	Description	Type	Size	Default
tenant-id	EMS Tenant ID.	string	Maximum length: 32	
source-ip	REST API call source IP.	ipv4-address-any	Not Specified	0.0.0.0
pull-sysinfo	Enable/disable pulling SysInfo from EMS.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable pulling FortiClient user SysInfo from EMS.		
	<i>disable</i>	Disable pulling FortiClient user SysInfo from EMS.		
pull-vulnerabilities	Enable/disable pulling vulnerabilities from EMS.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable pulling client vulnerabilities from EMS.		
	<i>disable</i>	Disable pulling client vulnerabilities from EMS.		
pull-avatars	Enable/disable pulling avatars from EMS.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable pulling FortiClient user avatars from EMS.		
	<i>disable</i>	Disable pulling FortiClient user avatars from EMS.		
pull-tags	Enable/disable pulling FortiClient user tags from EMS.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable pulling FortiClient user tags from EMS.		
	<i>disable</i>	Disable pulling FortiClient user tags from EMS.		
pull-malware-hash	Enable/disable pulling FortiClient malware hash from EMS.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable pulling FortiClient malware hash from EMS.		
	<i>disable</i>	Disable pulling FortiClient malware hash from EMS.		
cloud-server-type	Cloud server type.	option	-	production

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>production</i></td><td>Production FortiClient EMS Cloud Controller.</td></tr><tr><td><i>alpha</i></td><td>Alpha FortiClient EMS Cloud Controller.</td></tr><tr><td><i>beta</i></td><td>Beta FortiClient EMS Cloud Controller.</td></tr></table>	Option	Description	<i>production</i>	Production FortiClient EMS Cloud Controller.	<i>alpha</i>	Alpha FortiClient EMS Cloud Controller.	<i>beta</i>	Beta FortiClient EMS Cloud Controller.									
	Option	Description																
	<i>production</i>	Production FortiClient EMS Cloud Controller.																
	<i>alpha</i>	Alpha FortiClient EMS Cloud Controller.																
<i>beta</i>	Beta FortiClient EMS Cloud Controller.																	
capabilities	List of EMS capabilities.	option	-															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fabric-auth</i></td><td>Allow this FortiProxy unit to load the authentication page provided by EMS to authenticate itself with EMS.</td></tr><tr><td><i>silent-approval</i></td><td>Allow silent approval of non-root or FortiProxy HA clusters on EMS in the Security Fabric.</td></tr><tr><td><i>websocket</i></td><td>Enable/disable websockets for this FortiProxy unit. Override behavior using websocket-override.</td></tr><tr><td><i>websocket-malware</i></td><td>Allow this FortiGate unit to request malware hash notifications over websocket.</td></tr><tr><td><i>push-ca-certs</i></td><td>Enable/disable syncing deep inspection certificates with EMS.</td></tr><tr><td><i>common-tags-api</i></td><td>Can receive tag information from New Common Tags API from EMS.</td></tr></table>	Option	Description	<i>fabric-auth</i>	Allow this FortiProxy unit to load the authentication page provided by EMS to authenticate itself with EMS.	<i>silent-approval</i>	Allow silent approval of non-root or FortiProxy HA clusters on EMS in the Security Fabric.	<i>websocket</i>	Enable/disable websockets for this FortiProxy unit. Override behavior using websocket-override.	<i>websocket-malware</i>	Allow this FortiGate unit to request malware hash notifications over websocket.	<i>push-ca-certs</i>	Enable/disable syncing deep inspection certificates with EMS.	<i>common-tags-api</i>	Can receive tag information from New Common Tags API from EMS.			
	Option	Description																
	<i>fabric-auth</i>	Allow this FortiProxy unit to load the authentication page provided by EMS to authenticate itself with EMS.																
	<i>silent-approval</i>	Allow silent approval of non-root or FortiProxy HA clusters on EMS in the Security Fabric.																
	<i>websocket</i>	Enable/disable websockets for this FortiProxy unit. Override behavior using websocket-override.																
	<i>websocket-malware</i>	Allow this FortiGate unit to request malware hash notifications over websocket.																
	<i>push-ca-certs</i>	Enable/disable syncing deep inspection certificates with EMS.																
<i>common-tags-api</i>	Can receive tag information from New Common Tags API from EMS.																	
	<i>tenant-id</i>	Allow this FortiGate to retrieve Tenant-ID from EMS.																
call-timeout	FortiClient EMS call timeout in seconds.	integer	Minimum value: 1 Maximum value: 180	30														
out-of-sync-threshold	Outdated resource threshold in seconds.	integer	Minimum value: 10 Maximum value: 3600	180														
websocket-override	Enable/disable override behavior for how this FortiProxy unit connects to EMS using a WebSocket connection.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not override the WebSocket connection. Connect to WebSocket of this EMS server if it is capable (default).</td></tr><tr><td><i>enable</i></td><td>Override the WebSocket connection. Do not connect to WebSocket even if EMS is capable of a WebSocket connection.</td></tr></table>	Option	Description	<i>disable</i>	Do not override the WebSocket connection. Connect to WebSocket of this EMS server if it is capable (default).	<i>enable</i>	Override the WebSocket connection. Do not connect to WebSocket even if EMS is capable of a WebSocket connection.											
	Option	Description																
<i>disable</i>	Do not override the WebSocket connection. Connect to WebSocket of this EMS server if it is capable (default).																	
<i>enable</i>	Override the WebSocket connection. Do not connect to WebSocket even if EMS is capable of a WebSocket connection.																	

Parameter	Description	Type	Size	Default
preserve-ssl-session	Enable/disable preservation of EMS SSL session connection. Warning, most users should not touch this setting.	option	-	disable
	Option Description			
	<i>enable</i>	Allow preservation of EMS SSL session connection.		
	<i>disable</i>	Don't allow preservation of EMS SSL session connection.		
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option Description			
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
trust-ca-cn	Enable/disable trust of the EMS certificate issuer (CA) and common name(CN) for certificate auto-renewal.	option	-	enable
	Option Description			
	<i>enable</i>	Trust EMS certificate CA & CN to automatically renew certificate.		
	<i>disable</i>	Do not trust EMS certificate CA & CN to automatically renew certificate.		

file-filter

This section includes syntax for the following commands:

- [config file-filter profile on page 164](#)

config file-filter profile

Configure file-filter profiles.

```
config file-filter profile
  Description: Configure file-filter profiles.
  edit <name>
    set comment {var-string}
    set replacemsg-group {string}
    set log [disable|enable]
    set scan-archive-contents [disable|enable]
    config rules
      Description: File filter rules.
      edit <name>
        set comment {var-string}
        set protocol {option1}, {option2}, ...
        set action [log-only|block]
        set direction [incoming|outgoing|...]
        set password-protected [yes|any]
        set file-type <name1>, <name2>, ...
      next
    end
  next
end
```

config file-filter profile

Parameter	Description	Type	Size	Default
name	Profile name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
replacemsg-group	Replacement message group.	string	Maximum length: 35	
log	Enable/disable file-filter logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable logging.		
	<i>enable</i>	Enable logging.		
scan-archive-contents	Enable/disable archive contents scan.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable scanning archive contents.		
	<i>enable</i>	Enable scanning archive contents.		

config rules

Parameter	Description	Type	Size	Default
name	File-filter rule name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
protocol	Protocols to apply rule to.	option	-	http ftp smtp imap pop3 mapi cifs ssh
	Option	Description		
	<i>http</i>	Filter on HTTP.		
	<i>ftp</i>	Filter on FTP.		
	<i>smtp</i>	Filter on SMTP.		
	<i>imap</i>	Filter on IMAP.		
	<i>pop3</i>	Filter on POP3.		
	<i>mapi</i>	Filter on MAPI. (Proxy mode only.)		
	<i>cifs</i>	Filter on CIFS.		
	<i>ssh</i>	Filter on SFTP and SCP. (Proxy mode only.)		
action	Action taken for matched file.	option	-	log-only

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>log-only</i>	Allow the content and write a log message.		
	<i>block</i>	Block the content and write a log message.		
direction	Traffic direction (HTTP, FTP, SSH, CIFS only).	option	-	any
	Option	Description		
	<i>incoming</i>	Match files transmitted in the session's reply direction.		
	<i>outgoing</i>	Match files transmitted in the session's originating direction.		
	<i>any</i>	Match files transmitted in the session's originating and reply directions.		
password-protected	Match password-protected files.	option	-	any
	Option	Description		
	<i>yes</i>	Match only password-protected files.		
	<i>any</i>	Match any file.		
file-type <name>	Select file type. File type name.	string	Maximum length: 39	

firewall

This section includes syntax for the following commands:

- [config firewall access-proxy-ssh-client-cert on page 168](#)
- [config firewall access-proxy-virtual-host on page 171](#)
- [config firewall access-proxy on page 172](#)
- [config firewall access-proxy6 on page 197](#)
- [config firewall address on page 198](#)
- [config firewall address6-template on page 203](#)
- [config firewall address6 on page 205](#)
- [config firewall addrgrp on page 208](#)
- [config firewall addrgrp6 on page 210](#)
- [config firewall auth-portal on page 212](#)
- [config firewall central-snat-map on page 212](#)
- [config firewall city on page 214](#)
- [config firewall country on page 214](#)
- [config firewall decrypted-traffic-mirror on page 215](#)
- [config firewall global on page 216](#)
- [config firewall identity-based-route on page 217](#)
- [config firewall internet-service-addition on page 218](#)
- [config firewall internet-service-append on page 219](#)
- [config firewall internet-service-botnet on page 220](#)
- [config firewall internet-service-custom-group on page 221](#)
- [config firewall internet-service-custom on page 221](#)
- [config firewall internet-service-definition on page 223](#)
- [config firewall internet-service-extension on page 225](#)
- [config firewall internet-service-group on page 229](#)
- [config firewall internet-service-ipbl-reason on page 229](#)
- [config firewall internet-service-ipbl-vendor on page 230](#)
- [config firewall internet-service-list on page 230](#)
- [config firewall internet-service-name on page 231](#)
- [config firewall internet-service-owner on page 232](#)
- [config firewall internet-service-reputation on page 233](#)
- [config firewall internet-service-sld on page 233](#)
- [config firewall internet-service-subapp on page 234](#)
- [config firewall internet-service on page 234](#)
- [config firewall ippool on page 236](#)
- [config firewall ippool6 on page 237](#)
- [config firewall network-service-dynamic on page 238](#)
- [config firewall policy on page 239](#)

- [config firewall profile-group on page 251](#)
- [config firewall profile-protocol-options on page 253](#)
- [config firewall proxy-address on page 278](#)
- [config firewall proxy-address6 on page 282](#)
- [config firewall proxy-addrgroup on page 286](#)
- [config firewall proxy-addrgroup6 on page 288](#)
- [config firewall region on page 289](#)
- [config firewall schedule group on page 289](#)
- [config firewall schedule onetime on page 290](#)
- [config firewall schedule recurring on page 291](#)
- [config firewall service category on page 292](#)
- [config firewall service custom on page 293](#)
- [config firewall service group on page 296](#)
- [config firewall shaper per-ip-shaper on page 297](#)
- [config firewall shaper traffic-shaper on page 299](#)
- [config firewall shaping-policy on page 301](#)
- [config firewall shaping-profile on page 305](#)
- [config firewall sniffer on page 306](#)
- [config firewall ssh host-key on page 308](#)
- [config firewall ssh local-ca on page 309](#)
- [config firewall ssh local-key on page 310](#)
- [config firewall ssh setting on page 311](#)
- [config firewall ssl-server on page 312](#)
- [config firewall ssl-ssh-profile on page 315](#)
- [config firewall ssl default-certificate on page 346](#)
- [config firewall ssl keyring-list on page 346](#)
- [config firewall ssl setting on page 347](#)
- [config firewall traffic-class on page 348](#)
- [config firewall ttl-policy on page 349](#)
- [config firewall vendor-mac-summary on page 350](#)
- [config firewall vendor-mac on page 350](#)
- [config firewall vip on page 351](#)
- [config firewall vipgroup on page 383](#)
- [config firewall wildcard-fqdn custom on page 383](#)
- [config firewall wildcard-fqdn group on page 384](#)

config firewall access-proxy-ssh-client-cert

Configure Access Proxy SSH client certificate.

```
config firewall access-proxy-ssh-client-cert
    Description: Configure Access Proxy SSH client certificate.
```



```

edit <name>
    set source-address [enable|disable]
    set permit-x11-forwarding [enable|disable]
    set permit-agent-forwarding [enable|disable]
    set permit-port-forwarding [enable|disable]
    set permit-pty [enable|disable]
    set permit-user-rc [enable|disable]
    config cert-extension
        Description: Configure certificate extension for user certificate.
        edit <name>
            set critical [no|yes]
            set type [fixed|user]
            set data {string}
        next
    end
    set auth-ca {string}
next
end

```

config firewall access-proxy-ssh-client-cert

Parameter	Description	Type	Size	Default						
name	SSH client certificate name.	string	Maximum length: 79							
source-address	Enable/disable appending source-address certificate critical option. This option ensure certificate only accepted from FortiGate source address.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
permit-x11-forwarding	Enable/disable appending permit-x11-forwarding certificate extension.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
permit-agent-forwarding	Enable/disable appending permit-agent-forwarding certificate extension.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default
permit-port-forwarding	Enable/disable appending permit-port-forwarding certificate extension.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
permit-pty	Enable/disable appending permit-pty certificate extension.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
permit-user-rc	Enable/disable appending permit-user-rc certificate extension.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
auth-ca	Name of the SSH server public key authentication CA.	string	Maximum length: 79	

config cert-extension

Parameter	Description	Type	Size	Default						
name	Name of certificate extension.	string	Maximum length: 127							
critical	Critical option.	option	-	no						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>no</i></td><td>Certificate extension, server ignores the unsupported certificate extension.</td></tr><tr><td><i>yes</i></td><td>Critical option, server refuses to authorize if it cannot recognize the critical option.</td></tr></table>				Option	Description	<i>no</i>	Certificate extension, server ignores the unsupported certificate extension.	<i>yes</i>	Critical option, server refuses to authorize if it cannot recognize the critical option.
	Option	Description								
	<i>no</i>	Certificate extension, server ignores the unsupported certificate extension.								
<i>yes</i>	Critical option, server refuses to authorize if it cannot recognize the critical option.									
type	Type of certificate extension.	option	-	fixed						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fixed</i></td><td>Fixed certificate extension entry.</td></tr></table>				Option	Description	<i>fixed</i>	Fixed certificate extension entry.		
	Option	Description								
<i>fixed</i>	Fixed certificate extension entry.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>user</i>	Certificate extension entry filled with authenticated username.		
data	Data of certificate extension.	string	Maximum length: 127	

config firewall access-proxy-virtual-host

Configure Access Proxy virtual hosts.

```
config firewall access-proxy-virtual-host
  Description: Configure Access Proxy virtual hosts.
  edit <name>
    set ssl-certificate <name1>, <name2>, ...
    set host {string}
    set host-type [sub-string|wildcard]
    set replacemsg-group {string}
  next
end
```

config firewall access-proxy-virtual-host

Parameter	Description	Type	Size	Default
name	Virtual host name.	string	Maximum length: 79	
ssl-certificate <name>	SSL certificates for this host. Certificate list.	string	Maximum length: 79	
host	The host name.	string	Maximum length: 79	
host-type	Type of host pattern.	option	-	sub-string
	Option	Description		
	<i>sub-string</i>	Match the pattern if a string contains the sub-string.		
	<i>wildcard</i>	Match the pattern with wildcards.		
replacemsg-group	Access-proxy-virtual-host replacement message override group.	string	Maximum length: 35	

config firewall access-proxy

Configure IPv4 access proxy.

```
config firewall access-proxy
  Description: Configure IPv4 access proxy.
  edit <name>
    set vip {string}
    set client-cert [disable|enable]
    set user-agent-detect [disable|enable]
    set auth-portal [disable|enable]
    set auth-virtual-host {string}
    set empty-cert-action [accept|block|...]
    set log-blocked-traffic [enable|disable]
    set add-vhost-domain-to-dnsdb [enable|disable]
    set svr-pool-multiplex [enable|disable]
    set svr-pool-ttl {integer}
    set svr-pool-server-max-request {integer}
    set svr-pool-server-max-concurrent-request {integer}
    set decrypted-traffic-mirror {string}
  config api-gateway
    Description: Set IPv4 API Gateway.
    edit <id>
      set url-map {string}
      set service [http|https|...]
      set ldb-method [static|round-robin|...]
      set virtual-host {string}
      set url-map-type [sub-string|wildcard|...]
      set h2-support [enable|disable]
      set h3-support [enable|disable]
    config quic
      Description: QUIC setting.
      set max-idle-timeout {integer}
      set max-udp-payload-size {integer}
      set active-connection-id-limit {integer}
      set ack-delay-exponent {integer}
      set max-ack-delay {integer}
      set max-datagram-frame-size {integer}
      set active-migration [enable|disable]
      set grease-quic-bit [enable|disable]
    end
  config realservers
    Description: Select the real servers that this Access Proxy will
    distribute traffic to.
    edit <id>
      set addr-type [ip|fqdn]
      set address {string}
      set ip {ipv4-address-any}
      set domain {string}
      set port {integer}
      set mappedport {user}
      set status [active|standby|...]
      set type [tcp-forwarding|ssh]
      set weight {integer}
      set http-host {string}
```

```

        set health-check [disable|enable]
        set health-check-proto [ping|http|...]
        set holddown-interval [enable|disable]
        set translate-host [enable|disable]
        set ssh-client-cert {string}
        set ssh-host-key-validation [disable|enable]
        set ssh-host-key <name1>, <name2>, ...
    next
end
set application <name1>, <name2>, ...
set persistence [none|http-cookie]
set http-cookie-domain-from-host [disable|enable]
set http-cookie-domain {string}
set http-cookie-path {string}
set http-cookie-generation {integer}
set http-cookie-age {integer}
set http-cookie-share [disable|same-ip]
set https-cookie-secure [disable|enable]
set saml-server {string}
set saml-redirect [disable|enable]
set ssl-dh-bits [768|1024|...]
set ssl-algorithm [high|medium|...]
config ssl-cipher-suites
    Description: SSL/TLS cipher suites to offer to a server, ordered by
priority.
    edit <priority>
        set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
        set versions {option1}, {option2}, ...
    next
end
set ssl-min-version [tls-1.0|tls-1.1|...]
set ssl-max-version [tls-1.0|tls-1.1|...]
set ssl-renegotiation [enable|disable]
next
end
config api-gateway6
    Description: Set IPv6 API Gateway.
    edit <id>
        set url-map {string}
        set service [http|https|...]
        set ldb-method [static|round-robin|...]
        set virtual-host {string}
        set url-map-type [sub-string|wildcard|...]
        set h2-support [enable|disable]
        set h3-support [enable|disable]
        config quic
            Description: QUIC setting.
            set max-idle-timeout {integer}
            set max-udp-payload-size {integer}
            set active-connection-id-limit {integer}
            set ack-delay-exponent {integer}
            set max-ack-delay {integer}
            set max-datagram-frame-size {integer}
            set active-migration [enable|disable]
            set grease-quic-bit [enable|disable]
        end
    end
end

```

```

        config realservers
            Description: Select the real servers that this Access Proxy will
            distribute traffic to.
            edit <id>
                set addr-type [ip|fqdn]
                set address {string}
                set ip {ipv6-address}
                set domain {string}
                set port {integer}
                set mappedport {user}
                set status [active|standby|...]
                set type [tcp-forwarding|ssh]
                set weight {integer}
                set http-host {string}
                set health-check [disable|enable]
                set health-check-proto [ping|http|...]
                set holddown-interval [enable|disable]
                set translate-host [enable|disable]
                set ssh-client-cert {string}
                set ssh-host-key-validation [disable|enable]
                set ssh-host-key <name1>, <name2>, ...
            next
        end
        set application <name1>, <name2>, ...
        set persistence [none|http-cookie]
        set http-cookie-domain-from-host [disable|enable]
        set http-cookie-domain {string}
        set http-cookie-path {string}
        set http-cookie-generation {integer}
        set http-cookie-age {integer}
        set http-cookie-share [disable|same-ip]
        set https-cookie-secure [disable|enable]
        set saml-server {string}
        set saml-redirect [disable|enable]
        set ssl-dh-bits [768|1024|...]
        set ssl-algorithm [high|medium|...]
        config ssl-cipher-suites
            Description: SSL/TLS cipher suites to offer to a server, ordered by
            priority.
            edit <priority>
                set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
                set versions {option1}, {option2}, ...
            next
        end
        set ssl-min-version [tls-1.0|tls-1.1|...]
        set ssl-max-version [tls-1.0|tls-1.1|...]
        set ssl-renegotiation [enable|disable]
    next
end
next
end

```

config firewall access-proxy

Parameter	Description	Type	Size	Default								
name	Access Proxy name.	string	Maximum length: 79									
vip	Virtual IP name.	string	Maximum length: 79									
client-cert	Enable/disable to request client certificate.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable client certificate request.</td></tr><tr><td><i>enable</i></td><td>Enable client certificate request.</td></tr></table>	Option	Description	<i>disable</i>	Disable client certificate request.	<i>enable</i>	Enable client certificate request.					
Option	Description											
<i>disable</i>	Disable client certificate request.											
<i>enable</i>	Enable client certificate request.											
user-agent-detect	Enable/disable to detect device type by HTTP user-agent if no client certificate provided.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable to detect unknown device by HTTP user-agent if no client certificate provided.</td></tr><tr><td><i>enable</i></td><td>Enable to detect unknown device by HTTP user-agent if no client certificate provided.</td></tr></table>	Option	Description	<i>disable</i>	Disable to detect unknown device by HTTP user-agent if no client certificate provided.	<i>enable</i>	Enable to detect unknown device by HTTP user-agent if no client certificate provided.					
Option	Description											
<i>disable</i>	Disable to detect unknown device by HTTP user-agent if no client certificate provided.											
<i>enable</i>	Enable to detect unknown device by HTTP user-agent if no client certificate provided.											
auth-portal	Enable/disable authentication portal.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable authentication portal.</td></tr><tr><td><i>enable</i></td><td>Enable authentication portal.</td></tr></table>	Option	Description	<i>disable</i>	Disable authentication portal.	<i>enable</i>	Enable authentication portal.					
Option	Description											
<i>disable</i>	Disable authentication portal.											
<i>enable</i>	Enable authentication portal.											
auth-virtual-host	Virtual host for authentication portal.	string	Maximum length: 79									
empty-cert-action	Action of an empty client certificate.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accept</i></td><td>Accept the SSL handshake if the client certificate is empty.</td></tr><tr><td><i>block</i></td><td>Block the SSL handshake if the client certificate is empty.</td></tr><tr><td><i>accept-unmanageable</i></td><td>Accept the SSL handshake only if the end-point is unmanageable.</td></tr></table>	Option	Description	<i>accept</i>	Accept the SSL handshake if the client certificate is empty.	<i>block</i>	Block the SSL handshake if the client certificate is empty.	<i>accept-unmanageable</i>	Accept the SSL handshake only if the end-point is unmanageable.			
Option	Description											
<i>accept</i>	Accept the SSL handshake if the client certificate is empty.											
<i>block</i>	Block the SSL handshake if the client certificate is empty.											
<i>accept-unmanageable</i>	Accept the SSL handshake only if the end-point is unmanageable.											
log-blocked-traffic	Enable/disable logging of blocked traffic.	option	-	enable								

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Log all traffic denied by this access proxy.</td></tr><tr><td><i>disable</i></td><td>Do not log all traffic denied by this access proxy.</td></tr></table>	Option	Description	<i>enable</i>	Log all traffic denied by this access proxy.	<i>disable</i>	Do not log all traffic denied by this access proxy.			
	Option	Description								
	<i>enable</i>	Log all traffic denied by this access proxy.								
<i>disable</i>	Do not log all traffic denied by this access proxy.									
add-vhost-domain-to-dnsdb	Enable/disable adding vhost/domain to dnsdb for ztna dox tunnel.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>add dns entry for all vhosts used by access proxy.</td></tr><tr><td><i>disable</i></td><td>Do not add dns entry for all vhosts used by access proxy.</td></tr></table>	Option	Description	<i>enable</i>	add dns entry for all vhosts used by access proxy.	<i>disable</i>	Do not add dns entry for all vhosts used by access proxy.			
	Option	Description								
	<i>enable</i>	add dns entry for all vhosts used by access proxy.								
<i>disable</i>	Do not add dns entry for all vhosts used by access proxy.									
svr-pool-multiplex	Enable/disable server pool multiplexing. Share connected server in HTTP, HTTPS, and web-portal api-gateway.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable server pool multiplexing. Share connected server.</td></tr><tr><td><i>disable</i></td><td>Disable server pool multiplexing. Do not share connected server.</td></tr></table>	Option	Description	<i>enable</i>	Enable server pool multiplexing. Share connected server.	<i>disable</i>	Disable server pool multiplexing. Do not share connected server.			
	Option	Description								
	<i>enable</i>	Enable server pool multiplexing. Share connected server.								
<i>disable</i>	Disable server pool multiplexing. Do not share connected server.									
svr-pool-ttl	Time-to-live in the server pool for idle connections to servers.	integer	Minimum value: 0 Maximum value: 2147483647	15						
svr-pool-server-max-request	Maximum number of requests that servers in server pool handle before disconnecting.	integer	Minimum value: 0 Maximum value: 2147483647	0						
svr-pool-server-max-concurrent-request	Maximum number of concurrent requests that servers in server pool could handle.	integer	Minimum value: 0 Maximum value: 2147483647	0						
decrypted-traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35							

config api-gateway

Parameter	Description	Type	Size	Default
id	API Gateway ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
url-map	URL pattern to match.	string	Maximum length: 511	/
service	Service.	option	-	https
	Option Description			
	http	HTTP.		
	https	HTTPS.		
	tcp-forwarding	TCP-FORWARDING.		
	samlsp	SAML-SP.		
	saas	SAAS.		
ldb-method	Method used to distribute sessions to real servers.	option	-	static
	Option Description			
	static	Distribute to server based on source IP.		
	round-robin	Distribute to server based round robin order.		
	weighted	Distribute to server based on weight.		
	first-alive	Distribute to the first server that is alive.		
	http-host	Distribute to server based on host field in HTTP header.		
virtual-host	Virtual host.	string	Maximum length: 79	
url-map-type	Type of url-map.	option	-	sub-string
	Option Description			
	sub-string	Match the pattern if a string contains the sub-string.		
	wildcard	Match the pattern with wildcards.		
	regex	Match the pattern with a regular expression.		
h2-support	HTTP2 support, default=Enable.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable HTTP2 support.		
	<i>disable</i>	Disable HTTP2 support.		
h3-support	HTTP3/QUIC support, default=Disable.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable HTTP3/QUIC support.		
	<i>disable</i>	Disable HTTP3/QUIC support.		
application <name>	SaaS application controlled by this Access Proxy. SaaS application name.	string	Maximum length: 79	
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none
	Option	Description		
	<i>none</i>	None.		
	<i>http-cookie</i>	HTTP cookie.		
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).		
	<i>enable</i>	Enable use of HTTP cookie domain from host field in HTTP.		
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35	
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35	
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600	60
http-cookie-share	Control sharing of cookies across API Gateway. Use of same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip
	Option	Description		
	<i>disable</i>	Only allow HTTP cookie to match this API Gateway.		
	<i>same-ip</i>	Allow HTTP cookie to match any API Gateway with same IP.		
https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-	disable
	Option	Description		
	<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.		
	<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.		
saml-server	SAML service provider configuration for VIP authentication.	string	Maximum length: 35	
saml-redirect	Enable/disable SAML redirection after successful authentication.	option	-	disable
	Option	Description		
	<i>disable</i>	Do not support redirection after successful SAML authentication.		
	<i>enable</i>	Support redirection after successful SAML authentication.		
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048
	Option	Description		
	<i>768</i>	768-bit Diffie-Hellman prime.		
	<i>1024</i>	1024-bit Diffie-Hellman prime.		
	<i>1536</i>	1536-bit Diffie-Hellman prime.		
	<i>2048</i>	2048-bit Diffie-Hellman prime.		

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>3072</td><td>3072-bit Diffie-Hellman prime.</td></tr><tr><td>4096</td><td>4096-bit Diffie-Hellman prime.</td></tr></table>	Option	Description	3072	3072-bit Diffie-Hellman prime.	4096	4096-bit Diffie-Hellman prime.							
	Option	Description												
	3072	3072-bit Diffie-Hellman prime.												
4096	4096-bit Diffie-Hellman prime.													
ssl-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-	high										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high</td><td>High encryption. Allow only AES and ChaCha.</td></tr><tr><td>medium</td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td>low</td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr></table>	Option	Description	high	High encryption. Allow only AES and ChaCha.	medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.					
	Option	Description												
	high	High encryption. Allow only AES and ChaCha.												
	medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.												
low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.													
ssl-min-version	Lowest SSL/TLS version acceptable from a server.	option	-	tls-1.1										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tls-1.0</td><td>TLS 1.0.</td></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr><tr><td>tls-1.2</td><td>TLS 1.2.</td></tr><tr><td>tls-1.3</td><td>TLS 1.3.</td></tr></table>	Option	Description	tls-1.0	TLS 1.0.	tls-1.1	TLS 1.1.	tls-1.2	TLS 1.2.	tls-1.3	TLS 1.3.			
	Option	Description												
	tls-1.0	TLS 1.0.												
	tls-1.1	TLS 1.1.												
	tls-1.2	TLS 1.2.												
tls-1.3	TLS 1.3.													
ssl-max-version	Highest SSL/TLS version acceptable from a server.	option	-	tls-1.3										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tls-1.0</td><td>TLS 1.0.</td></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr><tr><td>tls-1.2</td><td>TLS 1.2.</td></tr><tr><td>tls-1.3</td><td>TLS 1.3.</td></tr></table>	Option	Description	tls-1.0	TLS 1.0.	tls-1.1	TLS 1.1.	tls-1.2	TLS 1.2.	tls-1.3	TLS 1.3.			
	Option	Description												
	tls-1.0	TLS 1.0.												
	tls-1.1	TLS 1.1.												
	tls-1.2	TLS 1.2.												
tls-1.3	TLS 1.3.													
ssl-renegotiation	Enable/disable secure renegotiation to comply with RFC 5746.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable secure renegotiation.</td></tr><tr><td>disable</td><td>Disable secure renegotiation.</td></tr></table>	Option	Description	enable	Enable secure renegotiation.	disable	Disable secure renegotiation.							
	Option	Description												
	enable	Enable secure renegotiation.												
disable	Disable secure renegotiation.													

config quic

Parameter	Description	Type	Size	Default
max-idle-timeout	Maximum idle timeout milliseconds.	integer	Minimum value: 1 Maximum value: 60000	30000
max-udp-payload-size	Maximum UDP payload size in bytes.	integer	Minimum value: 1200 Maximum value: 1500	1500
active-connection-id-limit	Active connection ID limit.	integer	Minimum value: 1 Maximum value: 8	2
ack-delay-exponent	ACK delay exponent.	integer	Minimum value: 1 Maximum value: 20	3
max-ack-delay	Maximum ACK delay in milliseconds.	integer	Minimum value: 1 Maximum value: 16383	25
max-datagram-frame-size	Maximum datagram frame size in bytes.	integer	Minimum value: 1 Maximum value: 1500	1500
active-migration	Enable/disable active migration.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable active migration.	
		<i>disable</i>	Disable active migration.	
grease-quic-bit	Enable/disable grease QUIC bit.	option	-	enable
		Option	Description	
		<i>enable</i>	Enable grease QUIC bit.	
		<i>disable</i>	Disable grease QUIC bit.	

config realservers

Parameter	Description	Type	Size	Default								
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
addr-type	Type of address.	option	-	ip								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ip</i></td><td>Standard IPv4 address.</td></tr><tr><td><i>fqdn</i></td><td>Non-wildcard FQDN address object.</td></tr></table>				Option	Description	<i>ip</i>	Standard IPv4 address.	<i>fqdn</i>	Non-wildcard FQDN address object.		
Option	Description											
<i>ip</i>	Standard IPv4 address.											
<i>fqdn</i>	Non-wildcard FQDN address object.											
address	Address or address group of the real server.	string	Maximum length: 79									
ip	IPv6 address of the real server.	ipv6-address	Not Specified	::								
domain	Wildcard domain name of the real server.	string	Maximum length: 255									
port	Port for communicating with the real server.	integer	Minimum value: 1 Maximum value: 65535	443								
mappedport	Port for communicating with the real server.	user	Not Specified									
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-	active								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>active</i></td><td>Server status active.</td></tr><tr><td><i>standby</i></td><td>Server status standby.</td></tr><tr><td><i>disable</i></td><td>Server status disable.</td></tr></table>				Option	Description	<i>active</i>	Server status active.	<i>standby</i>	Server status standby.	<i>disable</i>	Server status disable.
Option	Description											
<i>active</i>	Server status active.											
<i>standby</i>	Server status standby.											
<i>disable</i>	Server status disable.											
type	TCP forwarding server type.	option	-	tcp-forwarding								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tcp-forwarding</i></td><td>TCP forwarding.</td></tr><tr><td><i>ssh</i></td><td>SSH.</td></tr></table>				Option	Description	<i>tcp-forwarding</i>	TCP forwarding.	<i>ssh</i>	SSH.		
Option	Description											
<i>tcp-forwarding</i>	TCP forwarding.											
<i>ssh</i>	SSH.											

Parameter	Description	Type	Size	Default								
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255	1								
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63									
health-check	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable per server health check.</td></tr><tr><td><i>enable</i></td><td>Enable per server health check.</td></tr></table>	Option	Description	<i>disable</i>	Disable per server health check.	<i>enable</i>	Enable per server health check.					
Option	Description											
<i>disable</i>	Disable per server health check.											
<i>enable</i>	Enable per server health check.											
health-check-proto	Protocol of the health check monitor to use when polling to determine server's connectivity status.	option	-	ping								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>Use PING to test the link with the server.</td></tr><tr><td><i>http</i></td><td>Use HTTP-GET to test the link with the server.</td></tr><tr><td><i>tcp-connect</i></td><td>Use a full TCP connection to test the link with the server.</td></tr></table>	Option	Description	<i>ping</i>	Use PING to test the link with the server.	<i>http</i>	Use HTTP-GET to test the link with the server.	<i>tcp-connect</i>	Use a full TCP connection to test the link with the server.			
Option	Description											
<i>ping</i>	Use PING to test the link with the server.											
<i>http</i>	Use HTTP-GET to test the link with the server.											
<i>tcp-connect</i>	Use a full TCP connection to test the link with the server.											
holddown-interval	Enable/disable holddown timer. Server will be considered active and reachable once the holddown period has expired (30 seconds).	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable per server holddown.</td></tr><tr><td><i>disable</i></td><td>Disable per server holddown.</td></tr></table>	Option	Description	<i>enable</i>	Enable per server holddown.	<i>disable</i>	Disable per server holddown.					
Option	Description											
<i>enable</i>	Enable per server holddown.											
<i>disable</i>	Disable per server holddown.											
translate-host	Enable/disable translation of hostname/IP from virtual server to real server.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable virtual hostname/IP translation.</td></tr><tr><td><i>disable</i></td><td>Disable virtual hostname/IP translation.</td></tr></table>	Option	Description	<i>enable</i>	Enable virtual hostname/IP translation.	<i>disable</i>	Disable virtual hostname/IP translation.					
Option	Description											
<i>enable</i>	Enable virtual hostname/IP translation.											
<i>disable</i>	Disable virtual hostname/IP translation.											
ssh-client-cert	Set access-proxy SSH client certificate profile.	string	Maximum length: 79									
ssh-host-key-validation	Enable/disable SSH real server host key validation.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable SSH real server host key validation.		
	<i>enable</i>	Enable SSH real server host key validation.		
ssh-host-key <name>	One or more server host key. Server host key name.	string	Maximum length: 79	

config ssl-cipher-suites

Parameter	Description	Type	Size	Default												
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295	0												
cipher	Cipher suite name.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>TLS-AES-128-GCM-SHA256</td><td>Cipher suite TLS-AES-128-GCM-SHA256.</td></tr><tr><td>TLS-AES-256-GCM-SHA384</td><td>Cipher suite TLS-AES-256-GCM-SHA384.</td></tr><tr><td>TLS-CHACHA20-POLY1305-SHA256</td><td>Cipher suite TLS-CHACHA20-POLY1305-SHA256.</td></tr><tr><td>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</td><td>Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr><tr><td>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr></table>				Option	Description	TLS-AES-128-GCM-SHA256	Cipher suite TLS-AES-128-GCM-SHA256.	TLS-AES-256-GCM-SHA384	Cipher suite TLS-AES-256-GCM-SHA384.	TLS-CHACHA20-POLY1305-SHA256	Cipher suite TLS-CHACHA20-POLY1305-SHA256.	TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.	TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.
Option	Description															
TLS-AES-128-GCM-SHA256	Cipher suite TLS-AES-128-GCM-SHA256.															
TLS-AES-256-GCM-SHA384	Cipher suite TLS-AES-256-GCM-SHA384.															
TLS-CHACHA20-POLY1305-SHA256	Cipher suite TLS-CHACHA20-POLY1305-SHA256.															
TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.															
TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.															

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.		
	TLS-DHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.		
	TLS-DHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.		
	TLS-DHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.		
	TLS-DHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.		
	TLS-DHE-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.		
	TLS-DHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.		
	TLS-DHE-DSS-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.		
	TLS-DHE-DSS-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.		
	TLS-DHE-DSS-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.		
	TLS-DHE-DSS-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.		
TLS-DHE-DSS-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.		
<i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.			

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.		
	TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.		
	TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.		
	TLS-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.		
	TLS-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.		
	TLS-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.		
	TLS-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.		
	TLS-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.		
	TLS-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.		
	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.		

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i></td><td>Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.</td></tr></table>	Option	Description	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.			
Option	Description																									
<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.																									
<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.																									
<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.																									
<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.																									
<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.																									
<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.																									
<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.																									
<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.																									
<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.																									
<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.																									

Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-RSA-WITH-SEED-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr></table>	Option	Description	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.	<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.	<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.	<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.	<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.			
Option	Description																													
<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.																													
<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.																													
<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.																													
<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.																													
<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.																													
<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.																													
<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.																													
<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.																													
<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.																													
<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.																													
<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.																													
<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.																													

Parameter	Description	Type	Size	Default																									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-MD5</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-MD5.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-DES-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.				
	Option	Description																											
	<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.																											
	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.																											
	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.																											
	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.																											
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.																											
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.																											
	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.																											
	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.																											
	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.																											
<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.																												
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.																												
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	tls-1.0 tls-1.1 tls-1.2 tls-1.3																									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>tls-1.0</i>	TLS 1.0.		
	<i>tls-1.1</i>	TLS 1.1.		
	<i>tls-1.2</i>	TLS 1.2.		
	<i>tls-1.3</i>	TLS 1.3.		

config api-gateway6

Parameter	Description	Type	Size	Default
id	API Gateway ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
url-map	URL pattern to match.	string	Maximum length: 511	/
service	Service.	option	-	https
	Option	Description		
	<i>http</i>	HTTP.		
	<i>https</i>	HTTPS.		
	<i>tcp-forwarding</i>	TCP-FORWARDING.		
	<i>samlsp</i>	SAML-SP.		
	<i>saas</i>	SAAS.		
ldb-method	Method used to distribute sessions to real servers.	option	-	static
	Option	Description		
	<i>static</i>	Distribute to server based on source IP.		
	<i>round-robin</i>	Distribute to server based round robin order.		
	<i>weighted</i>	Distribute to server based on weight.		
	<i>first-alive</i>	Distribute to the first server that is alive.		
	<i>http-host</i>	Distribute to server based on host field in HTTP header.		
virtual-host	Virtual host.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
url-map-type	Type of url-map.	option	-	sub-string
	Option	Description		
	sub-string	Match the pattern if a string contains the sub-string.		
	wildcard	Match the pattern with wildcards.		
	regex	Match the pattern with a regular expression.		
h2-support	HTTP2 support, default=Enable.	option	-	enable
	Option	Description		
	enable	Enable HTTP2 support.		
	disable	Disable HTTP2 support.		
h3-support	HTTP3/QUIC support, default=Disable.	option	-	disable
	Option	Description		
	enable	Enable HTTP3/QUIC support.		
	disable	Disable HTTP3/QUIC support.		
application <name>	SaaS application controlled by this Access Proxy. SaaS application name.	string	Maximum length: 79	
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none
	Option	Description		
	none	None.		
	http-cookie	HTTP cookie.		
http-cookie- domain-from- host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable
	Option	Description		
	disable	Disable use of HTTP cookie domain from host field in HTTP (use http-cooke- domain setting).		
	enable	Enable use of HTTP cookie domain from host field in HTTP.		
http-cookie- domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default						
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35							
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295	0						
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600	60						
http-cookie-share	Control sharing of cookies across API Gateway. Use of same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Only allow HTTP cookie to match this API Gateway.</td></tr><tr><td>same-ip</td><td>Allow HTTP cookie to match any API Gateway with same IP.</td></tr></table>				Option	Description	disable	Only allow HTTP cookie to match this API Gateway.	same-ip	Allow HTTP cookie to match any API Gateway with same IP.
Option	Description									
disable	Only allow HTTP cookie to match this API Gateway.									
same-ip	Allow HTTP cookie to match any API Gateway with same IP.									
https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.</td></tr><tr><td>enable</td><td>Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.</td></tr></table>				Option	Description	disable	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.	enable	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.
Option	Description									
disable	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.									
enable	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.									
saml-server	SAML service provider configuration for VIP authentication.	string	Maximum length: 35							
saml-redirect	Enable/disable SAML redirection after successful authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not support redirection after successful SAML authentication.</td></tr><tr><td>enable</td><td>Support redirection after successful SAML authentication.</td></tr></table>				Option	Description	disable	Do not support redirection after successful SAML authentication.	enable	Support redirection after successful SAML authentication.
Option	Description									
disable	Do not support redirection after successful SAML authentication.									
enable	Support redirection after successful SAML authentication.									
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048						

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>768</td><td>768-bit Diffie-Hellman prime.</td></tr><tr><td>1024</td><td>1024-bit Diffie-Hellman prime.</td></tr><tr><td>1536</td><td>1536-bit Diffie-Hellman prime.</td></tr><tr><td>2048</td><td>2048-bit Diffie-Hellman prime.</td></tr><tr><td>3072</td><td>3072-bit Diffie-Hellman prime.</td></tr><tr><td>4096</td><td>4096-bit Diffie-Hellman prime.</td></tr></table>	Option	Description	768	768-bit Diffie-Hellman prime.	1024	1024-bit Diffie-Hellman prime.	1536	1536-bit Diffie-Hellman prime.	2048	2048-bit Diffie-Hellman prime.	3072	3072-bit Diffie-Hellman prime.	4096	4096-bit Diffie-Hellman prime.			
	Option	Description																
	768	768-bit Diffie-Hellman prime.																
	1024	1024-bit Diffie-Hellman prime.																
	1536	1536-bit Diffie-Hellman prime.																
	2048	2048-bit Diffie-Hellman prime.																
	3072	3072-bit Diffie-Hellman prime.																
4096	4096-bit Diffie-Hellman prime.																	
ssl-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-	high														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high</td><td>High encryption. Allow only AES and ChaCha.</td></tr><tr><td>medium</td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td>low</td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr></table>	Option	Description	high	High encryption. Allow only AES and ChaCha.	medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.									
	Option	Description																
	high	High encryption. Allow only AES and ChaCha.																
	medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.																
low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.																	
ssl-min-version	Lowest SSL/TLS version acceptable from a server.	option	-	tls-1.1														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tls-1.0</td><td>TLS 1.0.</td></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr><tr><td>tls-1.2</td><td>TLS 1.2.</td></tr><tr><td>tls-1.3</td><td>TLS 1.3.</td></tr></table>	Option	Description	tls-1.0	TLS 1.0.	tls-1.1	TLS 1.1.	tls-1.2	TLS 1.2.	tls-1.3	TLS 1.3.							
	Option	Description																
	tls-1.0	TLS 1.0.																
	tls-1.1	TLS 1.1.																
	tls-1.2	TLS 1.2.																
tls-1.3	TLS 1.3.																	
ssl-max-version	Highest SSL/TLS version acceptable from a server.	option	-	tls-1.3														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tls-1.0</td><td>TLS 1.0.</td></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr><tr><td>tls-1.2</td><td>TLS 1.2.</td></tr><tr><td>tls-1.3</td><td>TLS 1.3.</td></tr></table>	Option	Description	tls-1.0	TLS 1.0.	tls-1.1	TLS 1.1.	tls-1.2	TLS 1.2.	tls-1.3	TLS 1.3.							
	Option	Description																
	tls-1.0	TLS 1.0.																
	tls-1.1	TLS 1.1.																
tls-1.2	TLS 1.2.																	
tls-1.3	TLS 1.3.																	
ssl-renegotiation	Enable/disable secure renegotiation to comply with RFC 5746.	option	-	enable														

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable secure renegotiation.		
	<i>disable</i>	Disable secure renegotiation.		

config quic

Parameter	Description	Type	Size	Default
max-idle-timeout	Maximum idle timeout milliseconds.	integer	Minimum value: 1 Maximum value: 60000	30000
max-udp-payload-size	Maximum UDP payload size in bytes.	integer	Minimum value: 1200 Maximum value: 1500	1500
active-connection-id-limit	Active connection ID limit.	integer	Minimum value: 1 Maximum value: 8	2
ack-delay-exponent	ACK delay exponent.	integer	Minimum value: 1 Maximum value: 20	3
max-ack-delay	Maximum ACK delay in milliseconds.	integer	Minimum value: 1 Maximum value: 16383	25
max-datagram-frame-size	Maximum datagram frame size in bytes.	integer	Minimum value: 1 Maximum value: 1500	1500
active-migration	Enable/disable active migration.	option	-	disable
grease-quic-bit	Enable/disable grease QUIC bit.	option	-	enable

config realservers

Parameter	Description	Type	Size	Default
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
addr-type	Type of address.	option	-	ip
address	Address or address group of the real server.	string	Maximum length: 79	
ip	IPv6 address of the real server.	ipv6-address	Not Specified	::
domain	Wildcard domain name of the real server.	string	Maximum length: 255	
port	Port for communicating with the real server.	integer	Minimum value: 1 Maximum value: 65535	443
mappedport	Port for communicating with the real server.	user	Not Specified	
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-	active
type	TCP forwarding server type.	option	-	tcp-forwarding
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255	1
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63	
health-check	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	disable
health-check-proto	Protocol of the health check monitor to use when polling to determine server's connectivity status.	option	-	ping
holddown-interval	Enable/disable holddown timer. Server will be considered active and reachable once the holddown period has expired (30 seconds).	option	-	enable
translate-host	Enable/disable translation of hostname/IP from virtual server to real server.	option	-	enable

Parameter	Description	Type	Size	Default
ssh-client-cert	Set access-proxy SSH client certificate profile.	string	Maximum length: 79	
ssh-host-key-validation	Enable/disable SSH real server host key validation.	option	-	disable
ssh-host-key <name>	One or more server host key. Server host key name.	string	Maximum length: 79	

config ssl-cipher-suites

Parameter	Description	Type	Size	Default
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295	0
cipher	Cipher suite name.	option	-	
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	tls-1.0 tls-1.1 tls-1.2 tls-1.3

config firewall access-proxy6

Configure IPv6 access proxy.

```
config firewall access-proxy6
    Description: Configure IPv6 access proxy.
    edit <name>
        set vip {string}
    next
end
```

config firewall access-proxy6

Parameter	Description	Type	Size	Default
name	Access Proxy name.	string	Maximum length: 79	
vip	Virtual IP name.	string	Maximum length: 79	

config firewall address

Configure IPv4 addresses.

```
config firewall address
  Description: Configure IPv4 addresses.
  edit <name>
    set uuid {uuid}
    set subnet {ipv4-classnet-any}
    set type [ipmask|iprange|...]
    set sub-type [sdn|clearpass-spt|...]
    set clearpass-spt [unknown|healthy|...]
    set start-ip {ipv4-address-any}
    set end-ip {ipv4-address-any}
    set fqdn {string}
    set country {string}
    set wildcard-fqdn {string}
    set pattern-start {integer}
    set pattern-end {integer}
    set cache-ttl {integer}
    set wildcard {ipv4-classnet-any}
    set sdn {string}
    set fsso-group <name1>, <name2>, ...
    set interface {string}
    set tenant {string}
    set organization {string}
    set epq-name {string}
    set subnet-name {string}
    set sdn-tag {string}
    set policy-group {string}
    set obj-tag {string}
    set obj-type [ip|mac]
    set tag-detection-level {string}
    set tag-type {string}
    set comment {var-string}
    set associated-interface {string}
    set color {integer}
    set filter {var-string}
    set sdn-addr-type [private|public|...]
    set node-ip-only [enable|disable]
    set obj-id {var-string}
  config list
    Description: IP address list.
    edit <ip>
    next
  end
  config tagging
    Description: Config object tagging.
    edit <name>
      set category {string}
      set tags <name1>, <name2>, ...
    next
  end
  set allow-routing [enable|disable]
  set fabric-object [enable|disable]
```

```

    next
end

```

config firewall address

Parameter	Description	Type	Size	Default
name	Address name.	string	Maximum length: 79	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
subnet	IP address and subnet mask of address.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
type	Type of address.	option	-	ipmask
	OptionDescription			
	ipmask	Standard IPv4 address with subnet mask.		
	iprange	Range of IPv4 addresses between two specified addresses (inclusive).		
	fqdn	Fully Qualified Domain Name address.		
	fqdn-group	Fully Qualified Domain Name Group address.		
	geography	IP addresses from a specified country.		
	wildcard	Standard IPv4 using a wildcard subnet mask.		
	dynamic	Dynamic address object.		
	interface-subnet	IP and subnet of interface.		
sub-type	Sub-type of address.	option	-	sdn
	OptionDescription			
	sdn	SDN address.		
	clearpass-spt	ClearPass SPT (System Posture Token) address.		
	fsso	FSSO address.		
	ems-tag	FortiClient EMS tag.		
	fortivoice-tag	FortiVoice tag.		
	fortinac-tag	FortiNAC tag.		
	fortipolicy-tag	FortiPolicy tag.		
	swc-tag	Switch Controller NAC policy tag.		

Parameter	Description	Type	Size	Default														
clearpass-spt	SPT (System Posture Token) value.	option	-	unknown														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>unknown</i></td><td>UNKNOWN.</td></tr><tr><td><i>healthy</i></td><td>HEALTHY.</td></tr><tr><td><i>quarantine</i></td><td>QUARANTINE.</td></tr><tr><td><i>checkup</i></td><td>CHECKUP.</td></tr><tr><td><i>transient</i></td><td>TRANSIENT.</td></tr><tr><td><i>infected</i></td><td>INFECTED.</td></tr></table>	Option	Description	<i>unknown</i>	UNKNOWN.	<i>healthy</i>	HEALTHY.	<i>quarantine</i>	QUARANTINE.	<i>checkup</i>	CHECKUP.	<i>transient</i>	TRANSIENT.	<i>infected</i>	INFECTED.			
	Option	Description																
	<i>unknown</i>	UNKNOWN.																
	<i>healthy</i>	HEALTHY.																
	<i>quarantine</i>	QUARANTINE.																
	<i>checkup</i>	CHECKUP.																
	<i>transient</i>	TRANSIENT.																
<i>infected</i>	INFECTED.																	
start-ip	First IP address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0														
end-ip	Final IP address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0														
fqdn	Fully Qualified Domain Name address.	string	Maximum length: 255															
country	IP addresses associated to a specific country.	string	Maximum length: 2															
wildcard-fqdn	Fully Qualified Domain Name with wildcard characters.	string	Maximum length: 255															
pattern-start	Starting number of pattern for fqdn-group.	integer	Minimum value: 0 Maximum value: 65535	0														
pattern-end	Ending number of pattern for fqdn-group.	integer	Minimum value: 0 Maximum value: 65535	0														
cache-ttl	Defines the minimal TTL of individual IP addresses in FQDN cache measured in seconds.	integer	Minimum value: 0 Maximum value: 86400	0														

Parameter	Description	Type	Size	Default						
wildcard	IP address and wildcard netmask.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0						
sdn	SDN.	string	Maximum length: 35							
fsso-group <name>	FSSO group(s). FSSO group name.	string	Maximum length: 511							
interface	Name of interface whose IP address is to be used.	string	Maximum length: 35							
tenant	Tenant.	string	Maximum length: 35							
organization	Organization domain name (Syntax: organization/domain).	string	Maximum length: 35							
epg-name	Endpoint group name.	string	Maximum length: 255							
subnet-name	Subnet name.	string	Maximum length: 255							
sdn-tag	SDN Tag.	string	Maximum length: 15							
policy-group	Policy group name.	string	Maximum length: 15							
obj-tag	Tag of dynamic address object.	string	Maximum length: 255							
obj-type	Object type.	option	-	ip						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ip</i></td><td>IP address.</td></tr><tr><td><i>mac</i></td><td>MAC address</td></tr></table>				Option	Description	<i>ip</i>	IP address.	<i>mac</i>	MAC address
Option	Description									
<i>ip</i>	IP address.									
<i>mac</i>	MAC address									
tag-detection-level	Tag detection level of dynamic address object.	string	Maximum length: 15							
tag-type	Tag type of dynamic address object.	string	Maximum length: 63							
comment	Comment.	var-string	Maximum length: 255							
associated-interface	Network interface associated with address.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
filter	Match criteria filter.	var-string	Maximum length: 2047	
sdn-addr-type	Type of addresses to collect.	option	-	private
	Option	Description		
	<i>private</i>	Collect private addresses only.		
	<i>public</i>	Collect public addresses only.		
	<i>all</i>	Collect both public and private addresses.		
node-ip-only	Enable/disable collection of node addresses only in Kubernetes.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable collection of node addresses only in Kubernetes.		
	<i>disable</i>	Disable collection of node addresses only in Kubernetes.		
obj-id	Object ID for NSX.	var-string	Maximum length: 255	
allow-routing	Enable/disable use of this address in the static route configuration.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable use of this address in the static route configuration.		
	<i>disable</i>	Disable use of this address in the static route configuration.		
fabric-object	Security Fabric global object setting.	option	-	disable
	Option	Description		
	<i>enable</i>	Object is set as a security fabric-wide global object.		
	<i>disable</i>	Object is local to this security fabric member.		

config list

Parameter	Description	Type	Size	Default
ip	IP.	string	Maximum length: 35	

config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

config firewall address6-template

Configure IPv6 address templates.

```
config firewall address6-template
  Description: Configure IPv6 address templates.
  edit <name>
    set ip6 {ipv6-network}
    set subnet-segment-count {integer}
    config subnet-segment
      Description: IPv6 subnet segments.
      edit <id>
        set name {string}
        set bits {integer}
        set exclusive [enable|disable]
        config values
          Description: Subnet segment values.
          edit <name>
            set value {string}
          next
        end
      next
    end
  set fabric-object [enable|disable]
next
end
```

config firewall address6-template

Parameter	Description	Type	Size	Default
name	IPv6 address template name.	string	Maximum length: 63	
ip6	IPv6 address prefix.	ipv6-network	Not Specified	::/0

Parameter	Description	Type	Size	Default						
subnet-segment-count	Number of IPv6 subnet segments.	integer	Minimum value: 1 Maximum value: 6	0						
fabric-object	Security Fabric global object setting.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Object is set as a security fabric-wide global object.</td></tr><tr><td><i>disable</i></td><td>Object is local to this security fabric member.</td></tr></table>				Option	Description	<i>enable</i>	Object is set as a security fabric-wide global object.	<i>disable</i>	Object is local to this security fabric member.
Option	Description									
<i>enable</i>	Object is set as a security fabric-wide global object.									
<i>disable</i>	Object is local to this security fabric member.									

config subnet-segment

Parameter	Description	Type	Size	Default						
id	Subnet segment ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
name	Subnet segment name.	string	Maximum length: 63							
bits	Number of bits.	integer	Minimum value: 1 Maximum value: 16	0						
exclusive	Enable/disable exclusive value.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable exclusive value.</td></tr><tr><td><i>disable</i></td><td>Disable exclusive value.</td></tr></table>				Option	Description	<i>enable</i>	Enable exclusive value.	<i>disable</i>	Disable exclusive value.
Option	Description									
<i>enable</i>	Enable exclusive value.									
<i>disable</i>	Disable exclusive value.									

config values

Parameter	Description	Type	Size	Default
name	Subnet segment value name.	string	Maximum length: 63	
value	Subnet segment value.	string	Maximum length: 35	

config firewall address6

Configure IPv6 firewall addresses.

```
config firewall address6
  Description: Configure IPv6 firewall addresses.
  edit <name>
    set uuid {uuid}
    set type [ipprefix|iprange|...]
    set sdn {string}
    set ip6 {ipv6-network}
    set start-ip {ipv6-address}
    set end-ip {ipv6-address}
    set fqdn {string}
    set country {string}
    set cache-ttl {integer}
    set color {integer}
    set obj-id {var-string}
    config list
      Description: IP address list.
      edit <ip>
        next
      end
    config tagging
      Description: Config object tagging.
      edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
      next
    end
    set comment {var-string}
    set template {string}
    config subnet-segment
      Description: IPv6 subnet segments.
      edit <name>
        set type [any|specific]
        set value {string}
      next
    end
    set host-type [any|specific]
    set host {ipv6-address}
    set tenant {string}
    set epg-name {string}
    set sdn-tag {string}
    set fabric-object [enable|disable]
  next
end
```

config firewall address6

Parameter	Description	Type	Size	Default														
name	Address name.	string	Maximum length: 79															
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000														
type	Type of IPv6 address object.	option	-	ipprefix														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ipprefix</i></td><td>Uses the IP prefix to define a range of IPv6 addresses.</td></tr><tr><td><i>iprange</i></td><td>Range of IPv6 addresses between two specified addresses (inclusive).</td></tr><tr><td><i>fqdn</i></td><td>Fully qualified domain name.</td></tr><tr><td><i>geography</i></td><td>IPv6 addresses from a specified country.</td></tr><tr><td><i>dynamic</i></td><td>Dynamic address object for SDN.</td></tr><tr><td><i>template</i></td><td>Template.</td></tr></table>				Option	Description	<i>ipprefix</i>	Uses the IP prefix to define a range of IPv6 addresses.	<i>iprange</i>	Range of IPv6 addresses between two specified addresses (inclusive).	<i>fqdn</i>	Fully qualified domain name.	<i>geography</i>	IPv6 addresses from a specified country.	<i>dynamic</i>	Dynamic address object for SDN.	<i>template</i>	Template.
Option	Description																	
<i>ipprefix</i>	Uses the IP prefix to define a range of IPv6 addresses.																	
<i>iprange</i>	Range of IPv6 addresses between two specified addresses (inclusive).																	
<i>fqdn</i>	Fully qualified domain name.																	
<i>geography</i>	IPv6 addresses from a specified country.																	
<i>dynamic</i>	Dynamic address object for SDN.																	
<i>template</i>	Template.																	
sdn	SDN.	string	Maximum length: 35															
ip6	IPv6 address prefix (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxx/xxx).	ipv6-network	Not Specified	::/0														
start-ip	First IP address (inclusive) in the range for the address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::														
end-ip	Final IP address (inclusive) in the range for the address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::														
fqdn	Fully qualified domain name.	string	Maximum length: 255															
country	IPv6 addresses associated to a specific country.	string	Maximum length: 2															
cache-ttl	Minimal TTL of individual IPv6 addresses in FQDN cache.	integer	Minimum value: 0 Maximum value: 86400	0														

Parameter	Description	Type	Size	Default						
color	Integer value to determine the color of the icon in the GUI.	integer	Minimum value: 0 Maximum value: 32	0						
obj-id	Object ID for NSX.	var-string	Maximum length: 255							
comment	Comment.	var-string	Maximum length: 255							
template	IPv6 address template.	string	Maximum length: 63							
host-type	Host type.	option	-	any						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Wildcard.</td></tr><tr><td><i>specific</i></td><td>Specific host address.</td></tr></table>				Option	Description	<i>any</i>	Wildcard.	<i>specific</i>	Specific host address.
	Option	Description								
	<i>any</i>	Wildcard.								
<i>specific</i>	Specific host address.									
host	Host Address.	ipv6-address	Not Specified	::						
tenant	Tenant.	string	Maximum length: 35							
epg-name	Endpoint group name.	string	Maximum length: 255							
sdn-tag	SDN Tag.	string	Maximum length: 15							
fabric-object	Security Fabric global object setting.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Object is set as a security fabric-wide global object.</td></tr><tr><td><i>disable</i></td><td>Object is local to this security fabric member.</td></tr></table>				Option	Description	<i>enable</i>	Object is set as a security fabric-wide global object.	<i>disable</i>	Object is local to this security fabric member.
	Option	Description								
	<i>enable</i>	Object is set as a security fabric-wide global object.								
<i>disable</i>	Object is local to this security fabric member.									

config list

Parameter	Description	Type	Size	Default
ip	IP.	string	Maximum length: 89	

config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

config subnet-segment

Parameter	Description	Type	Size	Default						
name	Name.	string	Maximum length: 63							
type	Subnet segment type.	option	-	any						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Wildcard.</td></tr><tr><td><i>specific</i></td><td>Specific subnet segment address.</td></tr></table>				Option	Description	<i>any</i>	Wildcard.	<i>specific</i>	Specific subnet segment address.
	Option	Description								
	<i>any</i>	Wildcard.								
<i>specific</i>	Specific subnet segment address.									
value	Subnet segment value.	string	Maximum length: 35							

config firewall addrgrp

Configure IPv4 address groups.

```
config firewall addrgrp
  Description: Configure IPv4 address groups.
  edit <name>
    set type [default|folder]
    set category [default|ztna-ems-tag]
    set uuid {uuid}
    set member <name1>, <name2>, ...
    set comment {var-string}
    set exclude [enable|disable]
    set exclude-member <name1>, <name2>, ...
    set color {integer}
    config tagging
      Description: Config object tagging.
      edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
```



```

        next
    end
    set allow-routing [enable|disable]
    set fabric-object [enable|disable]
next
end

```

config firewall addrgrp

Parameter	Description	Type	Size	Default
name	Address group name.	string	Maximum length: 79	
type	Address group type.	option	-	default
	Option	Description		
	default	Default address group type (address may belong to multiple groups).		
	folder	Address folder group (members may not belong to any other group).		
category	Address group category.	option	-	default
	Option	Description		
	default	Default address group category (cannot be used as ztna-ems-tag in policy).		
	ztna-ems-tag	Members must be ztna-ems-tag group or ems-tag address, can be used as ztna-ems-tag in policy.		
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
member <name>	Address objects contained within the group. Address name.	string	Maximum length: 79	
comment	Comment.	var-string	Maximum length: 255	
exclude	Enable/disable address exclusion.	option	-	disable
	Option	Description		
	enable	Enable address exclusion.		
	disable	Disable address exclusion.		
exclude-member <name>	Address exclusion member. Address name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
allow-routing	Enable/disable use of this group in the static route configuration.	option	-	disable
	Option	Description		
	enable	Enable use of this group in the static route configuration.		
	disable	Disable use of this group in the static route configuration.		
fabric-object	Security Fabric global object setting.	option	-	disable
	Option	Description		
	enable	Object is set as a security fabric-wide global object.		
	disable	Object is local to this security fabric member.		

config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

config firewall addrgrp6

Configure IPv6 address groups.

```
config firewall addrgrp6
  Description: Configure IPv6 address groups.
  edit <name>
    set uuid {uuid}
    set color {integer}
    set comment {var-string}
    set member <name1>, <name2>, ...
  config tagging
    Description: Config object tagging.
    edit <name>
```

```

        set category {string}
        set tags <name1>, <name2>, ...
    next
end
    set fabric-object [enable|disable]
next
end

```

config firewall addrgrp6

Parameter	Description	Type	Size	Default
name	IPv6 address group name.	string	Maximum length: 79	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
color	Integer value to determine the color of the icon in the GUI.	integer	Minimum value: 0 Maximum value: 32	0
comment	Comment.	var-string	Maximum length: 255	
member <name>	Address objects contained within the group. Address6/addrgrp6 name.	string	Maximum length: 79	
fabric-object	Security Fabric global object setting.	option	-	disable
		Option	Description	
		<i>enable</i>	Object is set as a security fabric-wide global object.	
		<i>disable</i>	Object is local to this security fabric member.	

config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

config firewall auth-portal

Configure firewall authentication portals.

```
config firewall auth-portal
  Description: Configure firewall authentication portals.
  set groups <name1>, <name2>, ...
  set portal-addr {string}
  set portal-addr6 {string}
  set identity-based-route {string}
  set proxy-auth [enable|disable]
end
```

config firewall auth-portal

Parameter	Description	Type	Size	Default
groups <name>	Firewall user groups permitted to authenticate through this portal. Separate group names with spaces. Group name.	string	Maximum length: 79	
portal-addr	Address (or FQDN) of the authentication portal.	string	Maximum length: 63	
portal-addr6	IPv6 address (or FQDN) of authentication portal.	string	Maximum length: 63	
identity-based-route	Name of the identity-based route that applies to this portal.	string	Maximum length: 35	
proxy-auth	Enable/disable authentication by proxy daemon.	option	-	disable
		Option	Description	
		<i>enable</i>	Users are authenticated by proxy daemon.	
		<i>disable</i>	Users are not authenticated by proxy daemon.	

config firewall central-snat-map

Configure central SNAT policies.

```
config firewall central-snat-map
  Description: Configure central SNAT policies.
  edit <policyid>
    set status [enable|disable]
    set action [bypass|masquerade|...]
    set ipv6 [enable|disable]
    set srcintf {string}
    set dstintf {string}
```

```

    set src-addr <name1>, <name2>, ...
    set src-addr6 <name1>, <name2>, ...
    set dst-addr <name1>, <name2>, ...
    set dst-addr6 <name1>, <name2>, ...
    set nat-ippool <name1>, <name2>, ...
    set nat-ippool6 <name1>, <name2>, ...
  next
end

```

config firewall central-snat-map

Parameter	Description	Type	Size	Default								
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
status	Enable/disable the active status of this policy.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this policy.</td></tr><tr><td><i>disable</i></td><td>Disable this policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable this policy.	<i>disable</i>	Disable this policy.					
Option	Description											
<i>enable</i>	Enable this policy.											
<i>disable</i>	Disable this policy.											
action	central SNAT action.	option	-	masquerade								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass and do not perform NAT.</td></tr><tr><td><i>masquerade</i></td><td>NAT using the primary IP of destination interface.</td></tr><tr><td><i>ippool</i></td><td>NAT using ip pool.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass and do not perform NAT.	<i>masquerade</i>	NAT using the primary IP of destination interface.	<i>ippool</i>	NAT using ip pool.			
Option	Description											
<i>bypass</i>	Bypass and do not perform NAT.											
<i>masquerade</i>	NAT using the primary IP of destination interface.											
<i>ippool</i>	NAT using ip pool.											
ipv6	Enable/disable IPv6.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ipv6.</td></tr><tr><td><i>disable</i></td><td>Disable ipv6.</td></tr></table>	Option	Description	<i>enable</i>	Enable ipv6.	<i>disable</i>	Disable ipv6.					
Option	Description											
<i>enable</i>	Enable ipv6.											
<i>disable</i>	Disable ipv6.											
srcintf	Source interface name from available interfaces.	string	Maximum length: 35									
dstintf	Destination interface name from available interfaces.	string	Maximum length: 35									
src-addr <name>	IPv4 Original address. Address name.	string	Maximum length: 79									

Parameter	Description	Type	Size	Default
src-addr6 <name>	IPv6 Original address. Address name.	string	Maximum length: 79	
dst-addr <name>	IPv4 Destination address. Address name.	string	Maximum length: 79	
dst-addr6 <name>	IPv6 Destination address. Address name.	string	Maximum length: 79	
nat-ippool <name>	Name of the IP pools to be used to translate addresses from available IP Pools. IP pool name.	string	Maximum length: 79	
nat-ippool6 <name>	IPv6 pools to be used for source NAT. IP pool name.	string	Maximum length: 79	

config firewall city

Define city table.

```
config firewall city
    Description: Define city table.
    edit <id>
        set name {string}
    next
end
```

config firewall city

Parameter	Description	Type	Size	Default
id	City ID.	integer	Minimum value: 0 Maximum value: 65535	0
name	City name.	string	Maximum length: 63	

config firewall country

Define country table.

```

config firewall country
    Description: Define country table.
    edit <id>
        set name {string}
        set region <id1>, <id2>, ...
    next
end

```

config firewall country

Parameter	Description	Type	Size	Default
id	Country ID.	integer	Minimum value: 0 Maximum value: 65535	0
name	Country name.	string	Maximum length: 63	
region <id>	Region ID list. Region ID.	integer	Minimum value: 0 Maximum value: 65535	

config firewall decrypted-traffic-mirror

Configure decrypted traffic mirror.

```

config firewall decrypted-traffic-mirror
    Description: Configure decrypted traffic mirror.
    edit <name>
        set dstmac {mac-address}
        set traffic-type {option1},{option2}, ...
        set traffic-source [client|server|...]
        set interface <name1>, <name2>, ...
    next
end

```

config firewall decrypted-traffic-mirror

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default								
dstmac	Set destination MAC address for mirrored traffic.	mac-address	Not Specified	ff:ff:ff:ff:ff:ff								
traffic-type	Types of decrypted traffic to be mirrored.	option	-	ssl								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ssl</td><td>Mirror decrypted SSL traffic.</td></tr><tr><td>ssh</td><td>Mirror decrypted SSH traffic.</td></tr></table>				Option	Description	ssl	Mirror decrypted SSL traffic.	ssh	Mirror decrypted SSH traffic.		
	Option	Description										
	ssl	Mirror decrypted SSL traffic.										
	ssh	Mirror decrypted SSH traffic.										
traffic-source	Source of decrypted traffic to be mirrored.	option	-	client								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>client</td><td>Mirror client side decrypted traffic.</td></tr><tr><td>server</td><td>Mirror server side decrypted traffic.</td></tr><tr><td>both</td><td>Mirror both client and server side decrypted traffic.</td></tr></table>				Option	Description	client	Mirror client side decrypted traffic.	server	Mirror server side decrypted traffic.	both	Mirror both client and server side decrypted traffic.
	Option	Description										
	client	Mirror client side decrypted traffic.										
	server	Mirror server side decrypted traffic.										
both	Mirror both client and server side decrypted traffic.											
interface <name>	Decrypted traffic mirror interface. Decrypted traffic mirror interface.	string	Maximum length: 79									

config firewall global

Global firewall settings.

```
config firewall global
    Description: Global firewall settings.
    set banned-ip-persistency [disabled|permanent-only|...]
end
```

config firewall global

Parameter	Description	Type	Size	Default								
banned-ip-persistency	Persistency of banned IPs across power cycling.	option	-	disabled								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disabled</i></td><td>No entries are kept across power cycling.</td></tr><tr><td><i>permanent-only</i></td><td>Only permanent IP bans are kept across power cycling.</td></tr><tr><td><i>all</i></td><td>All IP bans are kept across power cycling.</td></tr></table>	Option	Description	<i>disabled</i>	No entries are kept across power cycling.	<i>permanent-only</i>	Only permanent IP bans are kept across power cycling.	<i>all</i>	All IP bans are kept across power cycling.			
Option	Description											
<i>disabled</i>	No entries are kept across power cycling.											
<i>permanent-only</i>	Only permanent IP bans are kept across power cycling.											
<i>all</i>	All IP bans are kept across power cycling.											

config firewall identity-based-route

Configure identity based routing.

```
config firewall identity-based-route
  Description: Configure identity based routing.
  edit <name>
    set comments {string}
    config rule
      Description: Rule.
      edit <id>
        set gateway {ipv4-address}
        set device {string}
        set groups <name1>, <name2>, ...
      next
    end
  next
end
```

config firewall identity-based-route

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
comments	Comments.	string	Maximum length: 127	

config rule

Parameter	Description	Type	Size	Default
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
gateway	IPv4 address of the gateway (Format: xxx.xxx.xxx.xxx , Default: 0.0.0.0).	ipv4-address	Not Specified	0.0.0.0
device	Outgoing interface for the rule.	string	Maximum length: 35	
groups <name>	Select one or more group(s) from available groups that are allowed to use this route. Separate group names with a space. Group name.	string	Maximum length: 79	

config firewall internet-service-addition

Configure Internet Services Addition.

```
config firewall internet-service-addition
  Description: Configure Internet Services Addition.
  edit <id>
    set comment {var-string}
    config entry
      Description: Entries added to the Internet Service addition database.
      edit <id>
        set addr-mode [ipv4|ipv6]
        set protocol {integer}
        config port-range
          Description: Port ranges in the custom entry.
          edit <id>
            set start-port {integer}
            set end-port {integer}
          next
        end
      next
    end
  next
end
```

config firewall internet-service-addition

Parameter	Description	Type	Size	Default
id	Internet Service ID in the Internet Service database.	integer	Minimum value: 0 Maximum value: 4294967295	0
comment	Comment.	var-string	Maximum length: 255	

config entry

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ipv4</i>	IPv4 mode.		
	<i>ipv6</i>	IPv6 mode.		
protocol	Integer value for the protocol type as defined by IANA (only TCP is supported).	integer	Minimum value: 6 Maximum value: 6	6

config port-range

Parameter	Description	Type	Size	Default
id	Custom entry port range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-port	Integer value for starting TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	1
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	65535

config firewall internet-service-append

Configure additional port mappings for Internet Services.

```
config firewall internet-service-append
    Description: Configure additional port mappings for Internet Services.
    set addr-mode [ipv4|ipv6|...]
    set match-port {integer}
    set append-port {integer}
end
```

config firewall internet-service-append

Parameter	Description	Type	Size	Default
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4
	Option	Description		
	<i>ipv4</i>	IPv4 mode.		
	<i>ipv6</i>	IPv6 mode.		
	<i>both</i>	Both IPv4 and IPv6 mode.		
match-port	Matching TCP/UDP/SCTP destination port (0 to 65535, 0 means any port).	integer	Minimum value: 0 Maximum value: 65535	0
append-port	Appending TCP/UDP/SCTP destination port (1 to 65535).	integer	Minimum value: 0 Maximum value: 65535	0

config firewall internet-service-botnet

Show Internet Service botnet.

```
config firewall internet-service-botnet
    Description: Show Internet Service botnet.
    edit <id>
        set name {string}
    next
end
```

config firewall internet-service-botnet

Parameter	Description	Type	Size	Default
id	Internet Service Botnet ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Internet Service Botnet name.	string	Maximum length: 63	

config firewall internet-service-custom-group

Configure custom Internet Service group.

```
config firewall internet-service-custom-group
  Description: Configure custom Internet Service group.
  edit <name>
    set comment {var-string}
    set member <name1>, <name2>, ...
  next
end
```

config firewall internet-service-custom-group

Parameter	Description	Type	Size	Default
name	Custom Internet Service group name.	string	Maximum length: 63	
comment	Comment.	var-string	Maximum length: 255	
member <name>	Custom Internet Service group members. Group member name.	string	Maximum length: 79	

config firewall internet-service-custom

Configure custom Internet Services.

```
config firewall internet-service-custom
  Description: Configure custom Internet Services.
  edit <name>
    set reputation {integer}
    set comment {var-string}
    config entry
      Description: Entries added to the Internet Service database and custom database.
      edit <id>
        set addr-mode [ipv4|ipv6]
        set protocol {integer}
        config port-range
          Description: Port ranges in the custom entry.
          edit <id>
            set start-port {integer}
            set end-port {integer}
          next
        end
        set dst <name1>, <name2>, ...
        set dst6 <name1>, <name2>, ...
      next
    end
  end
```

```

    next
end

```

config firewall internet-service-custom

Parameter	Description	Type	Size	Default
name	Internet Service name.	string	Maximum length: 63	
reputation	Reputation level of the custom Internet Service.	integer	Minimum value: 0 Maximum value: 4294967295	3
comment	Comment.	var-string	Maximum length: 255	

config entry

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4
	Option	Description		
	ipv4	IPv4 mode.		
	ipv6	IPv6 mode.		
protocol	Integer value for the protocol type as defined by IANA (only TCP is supported).	integer	Minimum value: 6 Maximum value: 6	6
dst <name>	Destination address or address group name. Select the destination address or address group object from available options.	string	Maximum length: 79	
dst6 <name>	Destination address6 or address6 group name. Select the destination address6 or address group object from available options.	string	Maximum length: 79	

config port-range

Parameter	Description	Type	Size	Default
id	Custom entry port range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-port	Integer value for starting TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	1
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	65535

config firewall internet-service-definition

Configure Internet Service definition.

```

config firewall internet-service-definition
  Description: Configure Internet Service definition.
  edit <id>
    config entry
      Description: Protocol and port information in an Internet Service entry.
      edit <seq-num>
        set category-id {integer}
        set name {string}
        set protocol {integer}
        config port-range
          Description: Port ranges in the definition entry.
          edit <id>
            set start-port {integer}
            set end-port {integer}
          next
        end
      next
    end
  next
end

```

config firewall internet-service-definition

Parameter	Description	Type	Size	Default
id	Internet Service application list ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config entry

Parameter	Description	Type	Size	Default
seq-num	Entry sequence number.	integer	Minimum value: 0 Maximum value: 4294967295	0
category-id	Internet Service category ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Internet Service name.	string	Maximum length: 63	
protocol	Integer value for the protocol type as defined by IANA.	integer	Minimum value: 0 Maximum value: 255	0

config port-range

Parameter	Description	Type	Size	Default
id	Custom entry port range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-port	Starting TCP/UDP/SCTP destination port (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535	1

Parameter	Description	Type	Size	Default
end-port	Ending TCP/UDP/SCTP destination port (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535	65535

config firewall internet-service-extension

Configure Internet Services Extension.

```
config firewall internet-service-extension
    Description: Configure Internet Services Extension.
    edit <id>
        set comment {var-string}
        config entry
            Description: Entries added to the Internet Service extension database.
            edit <id>
                set addr-mode [ipv4|ipv6]
                set protocol {integer}
                config port-range
                    Description: Port ranges in the custom entry.
                    edit <id>
                        set start-port {integer}
                        set end-port {integer}
                    next
                end
                set dst <name1>, <name2>, ...
                set dst6 <name1>, <name2>, ...
            next
        end
    config disable-entry
        Description: Disable entries in the Internet Service database.
        edit <id>
            set addr-mode [ipv4|ipv6]
            set protocol {integer}
            config port-range
                Description: Port ranges in the disable entry.
                edit <id>
                    set start-port {integer}
                    set end-port {integer}
                next
            end
            config ip-range
                Description: IPv4 ranges in the disable entry.
                edit <id>
                    set start-ip {ipv4-address-any}
                    set end-ip {ipv4-address-any}
                next
            end
            config ip6-range
                Description: IPv6 ranges in the disable entry.
```

```

        edit <id>
            set start-ip6 {ipv6-address}
            set end-ip6 {ipv6-address}
        next
    end
next
end
next
end
end

```

config firewall internet-service-extension

Parameter	Description	Type	Size	Default
id	Internet Service ID in the Internet Service database.	integer	Minimum value: 0 Maximum value: 4294967295	0
comment	Comment.	var-string	Maximum length: 255	

config entry

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4
	Option	Description		
	ipv4	IPv4 mode.		
	ipv6	IPv6 mode.		
protocol	Integer value for the protocol type as defined by IANA (only TCP is supported).	integer	Minimum value: 6 Maximum value: 6	6
dst <name>	Destination address or address group name. Select the destination address or address group object from available options.	string	Maximum length: 79	
dst6 <name>	Destination address6 or address6 group name. Select the destination address6 or address group object from available options.	string	Maximum length: 79	

config port-range

Parameter	Description	Type	Size	Default
id	Custom entry port range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-port	Starting TCP/UDP/SCTP destination port (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	1
end-port	Ending TCP/UDP/SCTP destination port (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	65535

config disable-entry

Parameter	Description	Type	Size	Default
id	Disable entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4
	Option Description			
	ipv4	IPv4 mode.		
	ipv6	IPv6 mode.		
protocol	Integer value for the protocol type as defined by IANA.	integer	Minimum value: 0 Maximum value: 255	0

config port-range

Parameter	Description	Type	Size	Default
id	Custom entry port range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-port	Starting TCP/UDP/SCTP destination port (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	1
end-port	Ending TCP/UDP/SCTP destination port (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	65535

config ip-range

Parameter	Description	Type	Size	Default
id	Disable entry range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-ip	Start IPv4 address.	ipv4-address-any	Not Specified	0.0.0.0
end-ip	End IPv4 address.	ipv4-address-any	Not Specified	0.0.0.0

config ip6-range

Parameter	Description	Type	Size	Default
id	Disable entry range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-ip6	Start IPv6 address.	ipv6-address	Not Specified	::
end-ip6	End IPv6 address.	ipv6-address	Not Specified	::

config firewall internet-service-group

Configure group of Internet Service.

```
config firewall internet-service-group
  Description: Configure group of Internet Service.
  edit <name>
    set comment {var-string}
    set direction [source|destination|...]
    set member <name1>, <name2>, ...
  next
end
```

config firewall internet-service-group

Parameter	Description	Type	Size	Default								
name	Internet Service group name.	string	Maximum length: 63									
comment	Comment.	var-string	Maximum length: 255									
direction	How this service may be used (source, destination or both).	option	-	both								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>source</i></td><td>As source when applied.</td></tr><tr><td><i>destination</i></td><td>As destination when applied.</td></tr><tr><td><i>both</i></td><td>Both directions when applied.</td></tr></table>				Option	Description	<i>source</i>	As source when applied.	<i>destination</i>	As destination when applied.	<i>both</i>	Both directions when applied.
Option	Description											
<i>source</i>	As source when applied.											
<i>destination</i>	As destination when applied.											
<i>both</i>	Both directions when applied.											
member <name>	Internet Service group member. Internet Service name.	string	Maximum length: 79									

config firewall internet-service-ipbl-reason

IP block list reason.

```
config firewall internet-service-ipbl-reason
  Description: IP block list reason.
  edit <id>
    set name {string}
  next
end
```

config firewall internet-service-ipbl-reason

Parameter	Description	Type	Size	Default
id	IP block list reason ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	IP block list reason name.	string	Maximum length: 63	

config firewall internet-service-ipbl-vendor

IP block list vendor.

```
config firewall internet-service-ipbl-vendor
  Description: IP block list vendor.
  edit <id>
    set name {string}
  next
end
```

config firewall internet-service-ipbl-vendor

Parameter	Description	Type	Size	Default
id	IP block list vendor ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	IP block list vendor name.	string	Maximum length: 63	

config firewall internet-service-list

Internet Service list.

```
config firewall internet-service-list
  Description: Internet Service list.
  edit <id>
    set name {string}
```

```

    next
end

```

config firewall internet-service-list

Parameter	Description	Type	Size	Default
id	Internet Service category ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Internet Service category name.	string	Maximum length: 63	

config firewall internet-service-name

Define internet service names.

```

config firewall internet-service-name
    Description: Define internet service names.
    edit <name>
        set type [default|location]
        set internet-service-id {integer}
        set country-id {integer}
        set region-id {integer}
        set city-id {integer}
    next
end

```

config firewall internet-service-name

Parameter	Description	Type	Size	Default						
name	Internet Service name.	string	Maximum length: 63							
type	Internet Service name type.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Automatically generated Internet Service.</td></tr><tr><td><i>location</i></td><td>Geography location based Internet Service.</td></tr></table>				Option	Description	<i>default</i>	Automatically generated Internet Service.	<i>location</i>	Geography location based Internet Service.
	Option	Description								
	<i>default</i>	Automatically generated Internet Service.								
<i>location</i>	Geography location based Internet Service.									

Parameter	Description	Type	Size	Default
internet-service-id	Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
country-id	Country or Area ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
region-id	Region ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
city-id	City ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config firewall internet-service-owner

Internet Service owner.

```
config firewall internet-service-owner
    Description: Internet Service owner.
    edit <id>
        set name {string}
    next
end
```

config firewall internet-service-owner

Parameter	Description	Type	Size	Default
id	Internet Service owner ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Internet Service owner name.	string	Maximum length: 63	

config firewall internet-service-reputation

Show Internet Service reputation.

```
config firewall internet-service-reputation
  Description: Show Internet Service reputation.
  edit <id>
    set description {string}
  next
end
```

config firewall internet-service-reputation

Parameter	Description	Type	Size	Default
id	Internet Service Reputation ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
description	Description.	string	Maximum length: 127	

config firewall internet-service-sld

Internet Service Second Level Domain.

```
config firewall internet-service-sld
  Description: Internet Service Second Level Domain.
  edit <id>
    set name {string}
  next
end
```

config firewall internet-service-sld

Parameter	Description	Type	Size	Default
id	Second Level Domain ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Second Level Domain name.	string	Maximum length: 63	

config firewall internet-service-subapp

Show Internet Service sub app ID.

```
config firewall internet-service-subapp
    Description: Show Internet Service sub app ID.
    edit <id>
        set sub-app <id1>, <id2>, ...
    next
end
```

config firewall internet-service-subapp

Parameter	Description	Type	Size	Default
id	Internet Service main ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
sub-app <id>	Subapp number list. Subapp ID.	integer	Minimum value: 0 Maximum value: 4294967295	

config firewall internet-service

Show Internet Service application.

```
config firewall internet-service
    Description: Show Internet Service application.
    edit <id>
        set name {string}
        set icon-id {integer}
        set direction [src|dst|...]
        set database [isdb|irdb]
        set ip-range-number {integer}
        set extra-ip-range-number {integer}
        set ip-number {integer}
        set ip6-range-number {integer}
        set extra-ip6-range-number {integer}
        set singularity {integer}
        set obsolete {integer}
    next
end
```

config firewall internet-service

Parameter	Description	Type	Size	Default
id	Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Internet Service name.	string	Maximum length: 63	
icon-id	Icon ID of Internet Service.	integer	Minimum value: 0 Maximum value: 4294967295	0
direction	How this service may be used in a firewall policy (source, destination or both).	option	-	both
	Option Description			
	src	As source in the firewall policy.		
	dst	As destination in the firewall policy.		
	both	Both directions in the firewall policy.		
database	Database name this Internet Service belongs to.	option	-	isdb
	Option Description			
	isdb	Internet Service Database.		
	irdb	Internet RRR Database.		
ip-range-number	Number of IPv4 ranges.	integer	Minimum value: 0 Maximum value: 4294967295	0
extra-ip-range-number	Extra number of IPv4 ranges.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
ip-number	Total number of IPv4 addresses.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip6-range-number	Number of IPv6 ranges.	integer	Minimum value: 0 Maximum value: 4294967295	0
extra-ip6-range-number	Extra number of IPv6 ranges.	integer	Minimum value: 0 Maximum value: 4294967295	0
singularity	Singular level of the Internet Service.	integer	Minimum value: 0 Maximum value: 65535	0
obsolete	Indicates whether the Internet Service can be used.	integer	Minimum value: 0 Maximum value: 255	0

config firewall ippool

Configure IPv4 IP pools.

```
config firewall ippool
    Description: Configure IPv4 IP pools.
    edit <name>
        set startip {ipv4-address-any}
        set endip {ipv4-address-any}
        set comments {var-string}
    next
end
```

config firewall ippool

Parameter	Description	Type	Size	Default
name	IP pool name.	string	Maximum length: 79	
startip	First IPv4 address (inclusive) in the range for the address pool (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).	ipv4-address-any	Not Specified	0.0.0.0
endip	Final IPv4 address (inclusive) in the range for the address pool (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).	ipv4-address-any	Not Specified	0.0.0.0
comments	Comment.	var-string	Maximum length: 255	

config firewall ippool6

Configure IPv6 IP pools.

```
config firewall ippool6
    Description: Configure IPv6 IP pools.
    edit <name>
        set startip {ipv6-address}
        set endip {ipv6-address}
        set comments {var-string}
        set nat46 [disable|enable]
        set add-nat46-route [disable|enable]
    next
end
```

config firewall ippool6

Parameter	Description	Type	Size	Default
name	IPv6 IP pool name.	string	Maximum length: 79	
startip	First IPv6 address.	ipv6-address	Not Specified	::
endip	Final IPv6 address.	ipv6-address	Not Specified	::
comments	Comment.	var-string	Maximum length: 255	
nat46	Enable/disable NAT46.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable NAT46.		
	<i>enable</i>	Enable NAT46.		
add-nat46-route	Enable/disable adding NAT46 route.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable adding NAT46 route.		
	<i>enable</i>	Enable adding NAT46 route.		

config firewall network-service-dynamic

Configure Dynamic Network Services.

```
config firewall network-service-dynamic
    Description: Configure Dynamic Network Services.
    edit <name>
        set sdn {string}
        set comment {var-string}
        set filter {var-string}
    next
end
```

config firewall network-service-dynamic

Parameter	Description	Type	Size	Default
name	Dynamic Network Service name.	string	Maximum length: 63	
sdn	SDN connector name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
filter	Match criteria filter.	var-string	Maximum length: 2047	

config firewall policy

Configure firewall policies.

```
config firewall policy
  Description: Configure firewall policies.
  edit <policyid>
    set type [explicit-web|transparent|...]
    set status [enable|disable]
    set name {string}
    set uuid {uuid}
    set force-proxy [enable|disable]
    set implicit-proxy-detection [enable|disable]
    set dynamic-bypass [enable|disable]
    set srcintf <name1>, <name2>, ...
    set dstintf <name1>, <name2>, ...
    set ztna-device-ownership [enable|disable]
    set srcaddr <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
    set srcaddr6 <name1>, <name2>, ...
    set dstaddr6 <name1>, <name2>, ...
    set action [accept|deny|...]
    set schedule {string}
    set policy-expiry [enable|disable]
    set policy-expiry-date {datetime}
    set service <name1>, <name2>, ...
    set explicit-web-proxy {string}
    set transparent [enable|disable]
    set access-proxy <name1>, <name2>, ...
    set ztna-ems-tag <name1>, <name2>, ...
    set ztna-tags-match-logic [or|and]
    set device-ownership [enable|disable]
    set pass-through [enable|disable]
    set url-category <id1>, <id2>, ...
    set url-risk <name1>, <name2>, ...
    set internet-service [enable|disable]
    set internet-service-name <name1>, <name2>, ...
    set internet-service-group <name1>, <name2>, ...
    set internet-service-custom <name1>, <name2>, ...
    set internet-service6 [enable|disable]
    set internet-service6-name <name1>, <name2>, ...
    set internet-service6-group <name1>, <name2>, ...
    set internet-service6-custom <name1>, <name2>, ...
    set internet-service6-custom-group <name1>, <name2>, ...
    set internet-service-custom-group <name1>, <name2>, ...
    set utm-status [enable|disable]
    set ztna-policy-redirect [enable|disable]
    set webproxy-profile {string}
    set logtraffic [all|utm|...]
    set logtraffic-start [enable|disable]
    set log-http-transaction [disable|enable]
    set extended-log [enable|disable]
    set wanopt [enable|disable]
    set wanopt-detection [active|passive|...]
    set wanopt-passive-opt [default|transparent|...]
```

```
set wanopt-profile {string}
set wanopt-peer {string}
set webcache [enable|disable]
set webcache-https [disable|enable]
set reverse-cache [disable|enable]
set http-tunnel-auth [enable|disable]
set ssh-policy-check [enable|disable]
set webproxy-forward-server {string}
set isolator-server {string}
set poolname <name1>, <name2>, ...
set groups <name1>, <name2>, ...
set users <name1>, <name2>, ...
set disclaimer [disable|domain|...]
set comments {var-string}
set redirect-url {var-string}
set custom-log-fields <field-id1>, <field-id2>, ...
set replacemsg-override-group {string}
set srcaddr-negate [enable|disable]
set dstaddr-negate [enable|disable]
set service-negate [enable|disable]
set internet-service-negate [enable|disable]
set internet-service6-negate [enable|disable]
set application <id1>, <id2>, ...
set app-category <id1>, <id2>, ...
set app-group <name1>, <name2>, ...
set decrypted-traffic-mirror {string}
set max-session-per-user {integer}
set profile-type [single|group]
set profile-group {string}
set profile-protocol-options {string}
set ssl-ssh-profile {string}
set av-profile {string}
set ia-profile {string}
set webfilter-profile {string}
set dnsfilter-profile {string}
set emailfilter-profile {string}
set dlp-profile {string}
set file-filter-profile {string}
set ips-sensor {string}
set application-list {string}
set icap-profile {string}
set cifs-profile {string}
set videofilter-profile {string}
set isolator-profile {string}
set redirect-profile {string}
set ssh-filter-profile {string}
set casb-profile {string}
set detect-https-in-http-request [enable|disable]
next
end
```


config firewall policy

Parameter	Description	Type	Size	Default																
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967294	0																
type	Type of policy.	option	-	transparent																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>explicit-web</i></td><td>Explicit Web Proxy policy</td></tr><tr><td><i>transparent</i></td><td>Transparent firewall policy</td></tr><tr><td><i>explicit-ftp</i></td><td>Explicit FTP Proxy policy</td></tr><tr><td><i>ssh-tunnel</i></td><td>SSH Tunnel policy</td></tr><tr><td><i>ssh</i></td><td>SSH policy</td></tr><tr><td><i>access-proxy</i></td><td>Access Proxy</td></tr><tr><td><i>wanopt</i></td><td>WANopt Tunnel</td></tr></table>	Option	Description	<i>explicit-web</i>	Explicit Web Proxy policy	<i>transparent</i>	Transparent firewall policy	<i>explicit-ftp</i>	Explicit FTP Proxy policy	<i>ssh-tunnel</i>	SSH Tunnel policy	<i>ssh</i>	SSH policy	<i>access-proxy</i>	Access Proxy	<i>wanopt</i>	WANopt Tunnel			
	Option	Description																		
	<i>explicit-web</i>	Explicit Web Proxy policy																		
	<i>transparent</i>	Transparent firewall policy																		
	<i>explicit-ftp</i>	Explicit FTP Proxy policy																		
	<i>ssh-tunnel</i>	SSH Tunnel policy																		
	<i>ssh</i>	SSH policy																		
	<i>access-proxy</i>	Access Proxy																		
<i>wanopt</i>	WANopt Tunnel																			
status	Enable or disable this policy.	option	-	enable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.													
	Option	Description																		
	<i>enable</i>	Enable setting.																		
<i>disable</i>	Disable setting.																			
name	Policy name.	string	Maximum length: 35																	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000																
force-proxy	Force proxy.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Force all TCP transparent traffic to proxy.</td></tr><tr><td><i>disable</i></td><td>Do not force TCP transparent traffic to proxy.</td></tr></table>	Option	Description	<i>enable</i>	Force all TCP transparent traffic to proxy.	<i>disable</i>	Do not force TCP transparent traffic to proxy.													
	Option	Description																		
	<i>enable</i>	Force all TCP transparent traffic to proxy.																		
<i>disable</i>	Do not force TCP transparent traffic to proxy.																			
implicit-proxy-detection	Implicit proxy detection.	option	-	disable																

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable implicit proxy detection.</td></tr><tr><td><i>disable</i></td><td>Disable implicit proxy detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable implicit proxy detection.	<i>disable</i>	Disable implicit proxy detection.			
	Option	Description								
	<i>enable</i>	Enable implicit proxy detection.								
<i>disable</i>	Disable implicit proxy detection.									
dynamic-bypass	Dynamic bypass.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable dynamic bypass to all HTTP traffic in this policy.</td></tr><tr><td><i>disable</i></td><td>Disable dynamic bypass to all HTTP traffic in this policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable dynamic bypass to all HTTP traffic in this policy.	<i>disable</i>	Disable dynamic bypass to all HTTP traffic in this policy.			
	Option	Description								
	<i>enable</i>	Enable dynamic bypass to all HTTP traffic in this policy.								
<i>disable</i>	Disable dynamic bypass to all HTTP traffic in this policy.									
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79							
dstintf <name>	Outgoing (egress) interface. Interface name.	string	Maximum length: 79							
ztna-device-ownership	Enable/disable zero trust device ownership.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ZTNA device ownership check.</td></tr><tr><td><i>disable</i></td><td>Disable ZTNA device ownership check.</td></tr></table>	Option	Description	<i>enable</i>	Enable ZTNA device ownership check.	<i>disable</i>	Disable ZTNA device ownership check.			
	Option	Description								
	<i>enable</i>	Enable ZTNA device ownership check.								
<i>disable</i>	Disable ZTNA device ownership check.									
srcaddr <name>	Source address and address group names. Address name.	string	Maximum length: 79							
dstaddr <name>	Destination address and address group names. Address name.	string	Maximum length: 79							
srcaddr6 <name>	IPv6 source address (web proxy and ftp proxy only). Address name.	string	Maximum length: 79							
dstaddr6 <name>	IPv6 destination address (web proxy and ftp proxy only). Address name.	string	Maximum length: 79							
action	Policy action (allow/deny).	option	-	deny						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accept</i></td><td>Allows session that match the firewall policy.</td></tr><tr><td><i>deny</i></td><td>Blocks sessions that match the firewall policy.</td></tr></table>	Option	Description	<i>accept</i>	Allows session that match the firewall policy.	<i>deny</i>	Blocks sessions that match the firewall policy.			
	Option	Description								
	<i>accept</i>	Allows session that match the firewall policy.								
<i>deny</i>	Blocks sessions that match the firewall policy.									

Parameter	Description	Type	Size	Default
	Option Description			
	<i>redirect</i>	Redirect sessions that match the firewall policy to a url.		
	<i>isolate</i>	Isolate sessions that match the firewall policy with isolator.		
schedule	Schedule name.	string	Maximum length: 35	
policy-expiry	Enable/disable policy expiry.	option	-	disable
	Option Description			
	<i>enable</i>	Enable policy expiry.		
	<i>disable</i>	Disable polcy expiry.		
policy-expiry-date	Policy expiry date (YYYY-MM-DD HH:MM:SS).	datetime	Not Specified	0000-00-00 00:00:00
service <name>	Service and service group names. Service and service group names.	string	Maximum length: 79	
explicit-web-proxy	Explicit web proxy.	string	Maximum length: 35	
transparent	set webproxy to use original client address.	option	-	disable
	Option Description			
	<i>enable</i>	Enable using original client address for webproxy.		
	<i>disable</i>	Disable using original client address for webproxy.		
access-proxy <name>	Access Proxy. Access Proxy name.	string	Maximum length: 79	
ztna-ems-tag <name>	Source ztna-ems-tag names. Address name.	string	Maximum length: 79	
ztna-tags-match-logic	ZTNA tag matching logic.	option	-	or
	Option Description			
	<i>or</i>	Match ZTNA tags using a logical OR operator.		
	<i>and</i>	Match ZTNA tags using a logical AND operator.		
device-ownership	When enabled, the ownership enforcement will be done at policy level.	option	-	disable

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable device ownership.</td></tr><tr><td><i>disable</i></td><td>Disable device ownership.</td></tr></table>	Option	Description	<i>enable</i>	Enable device ownership.	<i>disable</i>	Disable device ownership.			
	Option	Description								
	<i>enable</i>	Enable device ownership.								
<i>disable</i>	Disable device ownership.									
pass-through	Enable/disable policy matching pass through	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable policy matching pass through.</td></tr><tr><td><i>disable</i></td><td>Disable policy matching pass through.</td></tr></table>	Option	Description	<i>enable</i>	Enable policy matching pass through.	<i>disable</i>	Disable policy matching pass through.			
	Option	Description								
	<i>enable</i>	Enable policy matching pass through.								
<i>disable</i>	Disable policy matching pass through.									
url-category <id>	URL category ID list. URL category ID.	integer	Minimum value: 0 Maximum value: 4294967295							
url-risk <name>	URL risk level name. Risk level name.	string	Maximum length: 79							
internet- service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of Internet Services in policy.</td></tr><tr><td><i>disable</i></td><td>Disable use of Internet Services in policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of Internet Services in policy.	<i>disable</i>	Disable use of Internet Services in policy.			
	Option	Description								
	<i>enable</i>	Enable use of Internet Services in policy.								
<i>disable</i>	Disable use of Internet Services in policy.									
internet- service-name <name>	Internet Service name. Internet Service name.	string	Maximum length: 79							
internet- service-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79							
internet- service- custom <name>	Custom Internet Service Name. Custom Internet Service name.	string	Maximum length: 79							
internet- service6	Enable/disable use of IPv6 Internet Services for this policy. If enabled, destination address and service are not used.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of IPv6 Internet Services in policy.</td></tr><tr><td><i>disable</i></td><td>Disable use of IPv6 Internet Services in policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of IPv6 Internet Services in policy.	<i>disable</i>	Disable use of IPv6 Internet Services in policy.			
	Option	Description								
	<i>enable</i>	Enable use of IPv6 Internet Services in policy.								
<i>disable</i>	Disable use of IPv6 Internet Services in policy.									
internet-service6-name <name>	IPv6 Internet Service name. IPv6 Internet Service name.	string	Maximum length: 79							
internet-service6-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79							
internet-service6-custom <name>	Custom IPv6 Internet Service name. Custom Internet Service name.	string	Maximum length: 79							
internet-service6-custom-group <name>	Custom Internet Service6 group name. Custom Internet Service6 group name.	string	Maximum length: 79							
internet-service-custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79							
utm-status	Enable to add one or more security profiles (AV, IPS, etc.) to the firewall policy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
ztna-policy-redirect	Redirect ZTNA traffic to matching Access-Proxy proxy-policy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ZTNA proxy-policy redirect.</td></tr><tr><td><i>disable</i></td><td>Disable ZTNA proxy-policy redirect.</td></tr></table>	Option	Description	<i>enable</i>	Enable ZTNA proxy-policy redirect.	<i>disable</i>	Disable ZTNA proxy-policy redirect.			
	Option	Description								
	<i>enable</i>	Enable ZTNA proxy-policy redirect.								
<i>disable</i>	Disable ZTNA proxy-policy redirect.									
webproxy-profile	Web proxy profile using when none matched policy.	string	Maximum length: 63							
logtraffic	Enable or disable logging. Log all sessions or security profile sessions.	option	-	utm						

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Log all sessions accepted or denied by this policy.</td></tr><tr><td><i>utm</i></td><td>Log traffic that has a security profile applied to it.</td></tr><tr><td><i>disable</i></td><td>Disable all logging for this policy.</td></tr></table>	Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.			
	Option	Description										
	<i>all</i>	Log all sessions accepted or denied by this policy.										
	<i>utm</i>	Log traffic that has a security profile applied to it.										
<i>disable</i>	Disable all logging for this policy.											
logtraffic-start	Record logs when a session starts and ends.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
log-http-transaction	Enable/disable http transaction log.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable HTTP transaction log.</td></tr><tr><td><i>enable</i></td><td>Enable HTTP transaction log.</td></tr></table>	Option	Description	<i>disable</i>	Disable HTTP transaction log.	<i>enable</i>	Enable HTTP transaction log.					
	Option	Description										
	<i>disable</i>	Disable HTTP transaction log.										
<i>enable</i>	Enable HTTP transaction log.											
extended-log	Enable/disable extended log for http transaction.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
wanopt	Enable/disable WAN optimization.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
wanopt-detection	WAN optimization auto-detection mode.	option	-	active								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>active</i></td><td>Active WAN optimization peer auto-detection.</td></tr><tr><td><i>passive</i></td><td>Passive WAN optimization peer auto-detection.</td></tr><tr><td><i>off</i></td><td>Turn off WAN optimization peer auto-detection.</td></tr></table>	Option	Description	<i>active</i>	Active WAN optimization peer auto-detection.	<i>passive</i>	Passive WAN optimization peer auto-detection.	<i>off</i>	Turn off WAN optimization peer auto-detection.			
	Option	Description										
	<i>active</i>	Active WAN optimization peer auto-detection.										
	<i>passive</i>	Passive WAN optimization peer auto-detection.										
<i>off</i>	Turn off WAN optimization peer auto-detection.											

Parameter	Description	Type	Size	Default								
wanopt-passive-opt	WAN optimization passive mode options. This option decides what IP address will be used to connect server.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Allow client side WAN opt peer to decide.</td></tr><tr><td>transparent</td><td>Use address of client to connect to server.</td></tr><tr><td>non-transparent</td><td>Use local FortiProxy address to connect to server.</td></tr></table>	Option	Description	default	Allow client side WAN opt peer to decide.	transparent	Use address of client to connect to server.	non-transparent	Use local FortiProxy address to connect to server.			
Option	Description											
default	Allow client side WAN opt peer to decide.											
transparent	Use address of client to connect to server.											
non-transparent	Use local FortiProxy address to connect to server.											
wanopt-profile	WAN optimization profile.	string	Maximum length: 35									
wanopt-peer	WAN optimization peer.	string	Maximum length: 35									
webcache	Enable/disable web cache.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.					
Option	Description											
enable	Enable setting.											
disable	Disable setting.											
webcache-https	Enable/disable web cache for HTTPS.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable web cache for HTTPS.</td></tr><tr><td>enable</td><td>Enable web cache for HTTPS.</td></tr></table>	Option	Description	disable	Disable web cache for HTTPS.	enable	Enable web cache for HTTPS.					
Option	Description											
disable	Disable web cache for HTTPS.											
enable	Enable web cache for HTTPS.											
reverse-cache	Enable/disable reverse cache servers.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable reverse cache.</td></tr><tr><td>enable</td><td>Enable reverse cache servers.</td></tr></table>	Option	Description	disable	Disable reverse cache.	enable	Enable reverse cache servers.					
Option	Description											
disable	Disable reverse cache.											
enable	Enable reverse cache servers.											
http-tunnel-auth	Enable/disable HTTP tunnel authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.					
Option	Description											
enable	Enable setting.											
disable	Disable setting.											

Parameter	Description	Type	Size	Default										
ssh-policy-check	Enable/disable SSH policy check.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSH policy check.</td></tr><tr><td><i>disable</i></td><td>Disable SSH policy check.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSH policy check.	<i>disable</i>	Disable SSH policy check.							
Option	Description													
<i>enable</i>	Enable SSH policy check.													
<i>disable</i>	Disable SSH policy check.													
webproxy-forward-server	Webproxy forward server name.	string	Maximum length: 63											
isolator-server	isolator server name.	string	Maximum length: 63											
poolname <name>	Name of IP pool object. IP pool name.	string	Maximum length: 79											
groups <name>	Names of user groups that can authenticate with this policy. Group name.	string	Maximum length: 79											
users <name>	Names of individual users that can authenticate with this policy. Names of individual users that can authenticate with this policy.	string	Maximum length: 79											
disclaimer	Web proxy disclaimer setting: by domain, policy, or user.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable disclaimer.</td></tr><tr><td><i>domain</i></td><td>Display disclaimer for domain</td></tr><tr><td><i>policy</i></td><td>Display disclaimer for policy</td></tr><tr><td><i>user</i></td><td>Display disclaimer for current user</td></tr></table>	Option	Description	<i>disable</i>	Disable disclaimer.	<i>domain</i>	Display disclaimer for domain	<i>policy</i>	Display disclaimer for policy	<i>user</i>	Display disclaimer for current user			
Option	Description													
<i>disable</i>	Disable disclaimer.													
<i>domain</i>	Display disclaimer for domain													
<i>policy</i>	Display disclaimer for policy													
<i>user</i>	Display disclaimer for current user													
comments	Comment.	var-string	Maximum length: 1023											
redirect-url	Redirect URL for further web proxy processing.	var-string	Maximum length: 1023											
custom-log-fields <field-id>	Custom fields to append to log messages for this policy. Custom log field.	string	Maximum length: 35											
replacemsg-override-group	Override the default replacement message group for this policy.	string	Maximum length: 35											

Parameter	Description	Type	Size	Default
srcaddr-negate	When enabled srcaddr specifies what the source address must NOT be.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable source address negate.		
	<i>disable</i>	Disable source address negate.		
dstaddr-negate	When enabled dstaddr specifies what the destination address must NOT be.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable destination address negate.		
	<i>disable</i>	Disable destination address negate.		
service-negate	When enabled service specifies what the service must NOT be.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable negated service match.		
	<i>disable</i>	Disable negated service match.		
internet-service-negate	When enabled internet-service specifies what the service must NOT be.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable negated Internet Service match.		
	<i>disable</i>	Disable negated Internet Service match.		
internet-service6-negate	When enabled internet-service6 specifies what the service must not be.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable negated IPv6 Internet Service match.		
	<i>disable</i>	Disable negated IPv6 Internet Service match.		
application <id>	Application ID list. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default						
app-category <id>	Application category ID list. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295							
app-group <name>	One or more application group names. Application group name.	string	Maximum length: 79							
decrypted-traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35							
max-session-per-user	Max UTM sessions per user.	integer	Minimum value: 0 Maximum value: 4294967295	0						
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-	single						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>single</td><td>Do not allow security profile groups.</td></tr><tr><td>group</td><td>Allow security profile groups.</td></tr></table>				Option	Description	single	Do not allow security profile groups.	group	Allow security profile groups.
Option	Description									
single	Do not allow security profile groups.									
group	Allow security profile groups.									
profile-group	Name of profile group.	string	Maximum length: 35							
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35	default						
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35	no-inspection						
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35							
ia-profile	Image analyzer profile.	string	Maximum length: 35							
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35							
dnsfilter-profile	Name of an existing DNS filter profile.	string	Maximum length: 35							
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default
dlp-profile	Name of an existing DLP profile.	string	Maximum length: 35	
file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 35	
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35	
application-list	Name of an existing Application list.	string	Maximum length: 35	
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35	
cifs-profile	Name of an existing CIFS profile.	string	Maximum length: 35	
videofilter-profile	Name of an existing VideoFilter profile.	string	Maximum length: 35	
isolator-profile	Name of an existing isolator profile.	string	Maximum length: 35	
redirect-profile	Name of an existing URL Redirect profile.	string	Maximum length: 35	
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35	
casb-profile	Name of an existing CASB profile.	string	Maximum length: 35	
detect-https-in-http-request	Enable/disable detection of HTTPS in HTTP request.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable detection of HTTPS in HTTP request.	
		<i>disable</i>	Disable detection of HTTPS in HTTP request.	

config firewall profile-group

Configure profile groups.

```
config firewall profile-group
  Description: Configure profile groups.
  edit <name>
    set profile-protocol-options {string}
    set ssl-ssh-profile {string}
    set av-profile {string}
```

```

        set ia-profile {string}
        set webfilter-profile {string}
        set dnsfilter-profile {string}
        set emailfilter-profile {string}
        set dlp-profile {string}
        set file-filter-profile {string}
        set ips-sensor {string}
        set application-list {string}
        set icap-profile {string}
        set cifs-profile {string}
        set videofilter-profile {string}
        set isolator-profile {string}
        set redirect-profile {string}
        set ssh-filter-profile {string}
        set casb-profile {string}
    next
end

```

config firewall profile-group

Parameter	Description	Type	Size	Default
name	Profile group name.	string	Maximum length: 35	
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35	default
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35	certificate-inspection
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35	
ia-profile	Image analyzer profile.	string	Maximum length: 35	
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35	
dnsfilter-profile	Name of an existing DNS filter profile.	string	Maximum length: 35	
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35	
dlp-profile	Name of an existing DLP profile.	string	Maximum length: 35	
file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 35	
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
application-list	Name of an existing Application list.	string	Maximum length: 35	
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35	
cifs-profile	Name of an existing CIFS profile.	string	Maximum length: 35	
videofilter-profile	Name of an existing VideoFilter profile.	string	Maximum length: 35	
isolator-profile	Name of an existing isolator profile.	string	Maximum length: 35	
redirect-profile	Name of an existing URL Redirect profile.	string	Maximum length: 35	
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35	
casb-profile	Name of an existing CASB profile.	string	Maximum length: 35	

config firewall profile-protocol-options

Configure protocol options.

```
config firewall profile-protocol-options
  Description: Configure protocol options.
  edit <name>
    set comment {var-string}
    set replacemsg-group {string}
    set oversize-log [disable|enable]
    set switching-protocols-log [disable|enable]
    config proxy-redirect
      Description: Configure proxy redirection protocol options.
      set ports {integer}
      set status [enable|disable]
    end
    config http
      Description: Configure HTTP protocol options.
      set ports {integer}
      set status [enable|disable]
      set options {option1}, {option2}, ...
      set comfort-interval {integer}
      set comfort-amount {integer}
      set range-block [disable|enable]
      set strip-x-forwarded-for [disable|enable]
      set post-lang {option1}, {option2}, ...
      set streaming-content-bypass [enable|disable]
      set dns-protection [enable|disable]
```

```
set switching-protocols [bypass|block]
set unknown-http-version [reject|tunnel|...]
set tunnel-non-http [enable|disable]
set h2c [enable|disable]
set unknown-content-encoding [block|inspect|...]
set oversize-limit {integer}
set uncompressed-oversize-limit {integer}
set uncompressed-nest-limit {integer}
set stream-based-uncompressed-limit {integer}
set scan-bzip2 [enable|disable]
set verify-dns-for-policy-matching [enable|disable]
set block-page-status-code {integer}
set retry-count {integer}
set domain-fronting [allow|block|...]
set tcp-window-type [auto-tuning|system|...]
set tcp-window-minimum {integer}
set tcp-window-maximum {integer}
set tcp-window-size {integer}
set ssl-offloaded [no|yes]
set address-ip-rating [enable|disable]
set encrypted-file [pass|inspect|...]
set encrypted-file-log [enable|disable]
end
config ftp
    Description: Configure FTP protocol options.
    set ports {integer}
    set status [enable|disable]
    set options {option1}, {option2}, ...
    set comfort-interval {integer}
    set comfort-amount {integer}
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set stream-based-uncompressed-limit {integer}
    set scan-bzip2 [enable|disable]
    set tcp-window-type [auto-tuning|system|...]
    set tcp-window-minimum {integer}
    set tcp-window-maximum {integer}
    set tcp-window-size {integer}
    set ssl-offloaded [no|yes]
    set explicit-ftp-tls [enable|disable]
end
config imap
    Description: Configure IMAP protocol options.
    set ports {integer}
    set status [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set scan-bzip2 [enable|disable]
    set ssl-offloaded [no|yes]
    set address-ip-rating [enable|disable]
end
config mapi
    Description: Configure MAPI protocol options.
```

```
    set ports {integer}
    set status [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set scan-bzip2 [enable|disable]
end
config pop3
    Description: Configure POP3 protocol options.
    set ports {integer}
    set status [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set scan-bzip2 [enable|disable]
    set ssl-offloaded [no|yes]
end
config smtp
    Description: Configure SMTP protocol options.
    set ports {integer}
    set status [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set scan-bzip2 [enable|disable]
    set server-busy [enable|disable]
    set ssl-offloaded [no|yes]
end
config nntp
    Description: Configure NNTP protocol options.
    set ports {integer}
    set status [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set scan-bzip2 [enable|disable]
end
config ssh
    Description: Configure SFTP and SCP protocol options.
    set options {option1}, {option2}, ...
    set comfort-interval {integer}
    set comfort-amount {integer}
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set stream-based-uncompressed-limit {integer}
    set scan-bzip2 [enable|disable]
    set tcp-window-type [auto-tuning|system|...]
    set tcp-window-minimum {integer}
    set tcp-window-maximum {integer}
    set tcp-window-size {integer}
    set ssl-offloaded [no|yes]
```

```

end
config dns
    Description: Configure DNS protocol options.
    set ports {integer}
    set status [enable|disable]
end
config cifs
    Description: Configure CIFS protocol options.
    set ports {integer}
    set status [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set scan-bzip2 [enable|disable]
    set tcp-window-type [auto-tuning|system|...]
    set tcp-window-minimum {integer}
    set tcp-window-maximum {integer}
    set tcp-window-size {integer}
    set server-credential-type [none|credential-replication|...]
    set domain-controller {string}
    config server-keytab
        Description: Server keytab.
        edit <principal>
            set keytab {string}
        next
    end
end
config mail-signature
    Description: Configure Mail signature.
    set status [disable|enable]
    set signature {string}
end
set rpc-over-http [enable|disable]
next
end

```

config firewall profile-protocol-options

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
comment	Optional comments.	var-string	Maximum length: 255	
replacemsg-group	Name of the replacement message group to be used.	string	Maximum length: 35	
oversize-log	Enable/disable logging for antivirus oversize file blocking.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable logging for antivirus oversize file blocking.		
	<i>enable</i>	Enable logging for antivirus oversize file blocking.		
switching-protocols-log	Enable/disable logging for HTTP/HTTPS switching protocols.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable logging for HTTP/HTTPS switching protocols.		
	<i>enable</i>	Enable logging for HTTP/HTTPS switching protocols.		
rpc-over-http	Enable/disable inspection of RPC over HTTP.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable inspection of RPC over HTTP.		
	<i>disable</i>	Disable inspection of RPC over HTTP.		

config proxy-redirect

Parameter	Description	Type	Size	Default
ports	Ports to inspect all for content.	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config http

Parameter	Description	Type	Size	Default
ports	Ports to scan for content.	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
options	One or more options that can be applied to the session.	option	-	
	Option	Description		
	<i>clientcomfort</i>	Prevent client timeout.		
	<i>servercomfort</i>	Prevent server timeout.		
	<i>oversize</i>	Block oversized file.		
	<i>chunkedbypass</i>	Bypass chunked transfer encoded sites.		
comfort-interval	Interval between successive transmissions of data for client comforting (seconds).	integer	Minimum value: 1 Maximum value: 900	10
comfort-amount	Number of bytes to send in each transmission for client comforting (bytes).	integer	Minimum value: 1 Maximum value: 65535	1
range-block	Enable/disable blocking of partial downloads.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable range header blocking (allow partial file downloads)		
	<i>enable</i>	Enable range header blocking (treat all partial file downloads as full file download)		
strip-x-forwarded-for	Enable/disable stripping of HTTP X-Forwarded-For header.	option	-	disable

Parameter	Description	Type	Size	Default																																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable changing of HTTP X-Forwarded-For header.</td></tr><tr><td><i>enable</i></td><td>Enable replacement of X-Forwarded-For value with 1.1.1.1.</td></tr></table>	Option	Description	<i>disable</i>	Disable changing of HTTP X-Forwarded-For header.	<i>enable</i>	Enable replacement of X-Forwarded-For value with 1.1.1.1.																																									
	Option	Description																																														
	<i>disable</i>	Disable changing of HTTP X-Forwarded-For header.																																														
<i>enable</i>	Enable replacement of X-Forwarded-For value with 1.1.1.1.																																															
post-lang	ID codes for character sets to be used to convert to UTF-8 for banned words and DLP on HTTP posts (maximum of 5 character sets).	option	-																																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>jisx0201</i></td><td>Japanese Industrial Standard 0201.</td></tr><tr><td><i>jisx0208</i></td><td>Japanese Industrial Standard 0208.</td></tr><tr><td><i>jisx0212</i></td><td>Japanese Industrial Standard 0212.</td></tr><tr><td><i>gb2312</i></td><td>Guojia Biaozhun 2312 (simplified Chinese).</td></tr><tr><td><i>ksc5601-ex</i></td><td>Wansung Korean standard 5601.</td></tr><tr><td><i>euc-jp</i></td><td>Extended Unicode Japanese.</td></tr><tr><td><i>sjis</i></td><td>Shift Japanese Industrial Standard.</td></tr><tr><td><i>iso2022-jp</i></td><td>ISO 2022 Japanese.</td></tr><tr><td><i>iso2022-jp-1</i></td><td>ISO 2022-1 Japanese.</td></tr><tr><td><i>iso2022-jp-2</i></td><td>ISO 2022-2 Japanese.</td></tr><tr><td><i>euc-cn</i></td><td>Extended Unicode Chinese.</td></tr><tr><td><i>ces-gbk</i></td><td>Extended GB2312 (simplified Chinese).</td></tr><tr><td><i>hz</i></td><td>Hanzi simplified Chinese.</td></tr><tr><td><i>ces-big5</i></td><td>Big-5 traditional Chinese.</td></tr><tr><td><i>euc-kr</i></td><td>Extended Unicode Korean.</td></tr><tr><td><i>iso2022-jp-3</i></td><td>ISO 2022-3 Japanese.</td></tr><tr><td><i>iso8859-1</i></td><td>ISO 8859 Part 1 (Western European).</td></tr><tr><td><i>tis620</i></td><td>Thai Industrial Standard 620.</td></tr><tr><td><i>cp874</i></td><td>Code Page 874 (Thai).</td></tr><tr><td><i>cp1252</i></td><td>Code Page 1252 (Western European Latin).</td></tr><tr><td><i>cp1251</i></td><td>Code Page 1251 (Cyrillic).</td></tr></table>	Option	Description	<i>jisx0201</i>	Japanese Industrial Standard 0201.	<i>jisx0208</i>	Japanese Industrial Standard 0208.	<i>jisx0212</i>	Japanese Industrial Standard 0212.	<i>gb2312</i>	Guojia Biaozhun 2312 (simplified Chinese).	<i>ksc5601-ex</i>	Wansung Korean standard 5601.	<i>euc-jp</i>	Extended Unicode Japanese.	<i>sjis</i>	Shift Japanese Industrial Standard.	<i>iso2022-jp</i>	ISO 2022 Japanese.	<i>iso2022-jp-1</i>	ISO 2022-1 Japanese.	<i>iso2022-jp-2</i>	ISO 2022-2 Japanese.	<i>euc-cn</i>	Extended Unicode Chinese.	<i>ces-gbk</i>	Extended GB2312 (simplified Chinese).	<i>hz</i>	Hanzi simplified Chinese.	<i>ces-big5</i>	Big-5 traditional Chinese.	<i>euc-kr</i>	Extended Unicode Korean.	<i>iso2022-jp-3</i>	ISO 2022-3 Japanese.	<i>iso8859-1</i>	ISO 8859 Part 1 (Western European).	<i>tis620</i>	Thai Industrial Standard 620.	<i>cp874</i>	Code Page 874 (Thai).	<i>cp1252</i>	Code Page 1252 (Western European Latin).	<i>cp1251</i>	Code Page 1251 (Cyrillic).			
	Option	Description																																														
	<i>jisx0201</i>	Japanese Industrial Standard 0201.																																														
	<i>jisx0208</i>	Japanese Industrial Standard 0208.																																														
	<i>jisx0212</i>	Japanese Industrial Standard 0212.																																														
	<i>gb2312</i>	Guojia Biaozhun 2312 (simplified Chinese).																																														
	<i>ksc5601-ex</i>	Wansung Korean standard 5601.																																														
	<i>euc-jp</i>	Extended Unicode Japanese.																																														
	<i>sjis</i>	Shift Japanese Industrial Standard.																																														
	<i>iso2022-jp</i>	ISO 2022 Japanese.																																														
	<i>iso2022-jp-1</i>	ISO 2022-1 Japanese.																																														
	<i>iso2022-jp-2</i>	ISO 2022-2 Japanese.																																														
	<i>euc-cn</i>	Extended Unicode Chinese.																																														
	<i>ces-gbk</i>	Extended GB2312 (simplified Chinese).																																														
	<i>hz</i>	Hanzi simplified Chinese.																																														
	<i>ces-big5</i>	Big-5 traditional Chinese.																																														
	<i>euc-kr</i>	Extended Unicode Korean.																																														
	<i>iso2022-jp-3</i>	ISO 2022-3 Japanese.																																														
	<i>iso8859-1</i>	ISO 8859 Part 1 (Western European).																																														
	<i>tis620</i>	Thai Industrial Standard 620.																																														
<i>cp874</i>	Code Page 874 (Thai).																																															
<i>cp1252</i>	Code Page 1252 (Western European Latin).																																															
<i>cp1251</i>	Code Page 1251 (Cyrillic).																																															
streaming-content-bypass	Enable/disable bypassing of streaming content from buffering.	option	-	enable																																												

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable bypassing of streaming content from buffering		
	<i>disable</i>	Disable bypassing of streaming content from buffering		
dns-protection	Enable/disable DNS protection for HTTP/HTTPS traffic.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
switching-protocols	Bypass from scanning, or block a connection that attempts to switch protocol.	option	-	bypass
	Option	Description		
	<i>bypass</i>	Bypass connections when switching protocols.		
	<i>block</i>	Block connections when switching protocols.		
unknown-http-version	How to handle HTTP sessions that do not comply with HTTP 0.9, 1.0, or 1.1.	option	-	reject
	Option	Description		
	<i>reject</i>	Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.		
	<i>tunnel</i>	Pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.		
	<i>best-effort</i>	Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.		
tunnel-non-http	Configure how to process non-HTTP traffic when a profile configured for HTTP traffic accepts a non-HTTP session. Can occur if an application sends non-HTTP traffic using an HTTP destination port.	option	-	enable
	Option	Description		
	<i>enable</i>	Pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.		
	<i>disable</i>	Drop or tear down non-HTTP sessions accepted by the profile.		

Parameter	Description	Type	Size	Default								
h2c	Enable/disable h2c HTTP connection upgrade.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow h2c HTTP connection upgrades. h2c tunnels do not support content scan.</td></tr><tr><td><i>disable</i></td><td>Do not allow h2c HTTP connection upgrades.</td></tr></table>				Option	Description	<i>enable</i>	Allow h2c HTTP connection upgrades. h2c tunnels do not support content scan.	<i>disable</i>	Do not allow h2c HTTP connection upgrades.		
	Option	Description										
	<i>enable</i>	Allow h2c HTTP connection upgrades. h2c tunnels do not support content scan.										
<i>disable</i>	Do not allow h2c HTTP connection upgrades.											
unknown-content-encoding	Configure the action the FortiGate unit will take on unknown content-encoding.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Block HTTP session when unknown content-encoding is detected.</td></tr><tr><td><i>inspect</i></td><td>Scan HTTP traffic as plain-text when unknown content-encoding is detected.</td></tr><tr><td><i>bypass</i></td><td>Bypass scan when unknown content-encoding is detected.</td></tr></table>				Option	Description	<i>block</i>	Block HTTP session when unknown content-encoding is detected.	<i>inspect</i>	Scan HTTP traffic as plain-text when unknown content-encoding is detected.	<i>bypass</i>	Bypass scan when unknown content-encoding is detected.
	Option	Description										
	<i>block</i>	Block HTTP session when unknown content-encoding is detected.										
	<i>inspect</i>	Scan HTTP traffic as plain-text when unknown content-encoding is detected.										
<i>bypass</i>	Bypass scan when unknown content-encoding is detected.											
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 26214**	10								
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 1 Maximum value: 26214**	10								
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12								
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned in megabytes. Stream-based uncompression used only under certain conditions.	integer	Minimum value: 0 Maximum value: 4294967295	0								
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											

Parameter	Description	Type	Size	Default										
verify-dns-for-policy-matching	Enable/disable verify DNS for policy matching.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
	Option	Description												
	<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.													
block-page-status-code	Code number returned for blocked HTTP pages.	integer	Minimum value: 100 Maximum value: 599	403										
retry-count	Number of attempts to retry HTTP connection.	integer	Minimum value: 0 Maximum value: 100	0										
domain-fronting*	Configure HTTP domain fronting.	option	-	block										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow domain fronting.</td></tr><tr><td><i>block</i></td><td>Block and log domain fronting.</td></tr><tr><td><i>monitor</i></td><td>Allow and log domain fronting.</td></tr></table>	Option	Description	<i>allow</i>	Allow domain fronting.	<i>block</i>	Block and log domain fronting.	<i>monitor</i>	Allow and log domain fronting.					
	Option	Description												
	<i>allow</i>	Allow domain fronting.												
	<i>block</i>	Block and log domain fronting.												
<i>monitor</i>	Allow and log domain fronting.													
tcp-window-type	TCP window type to use for this protocol.	option	-	auto-tuning										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto-tuning</i></td><td>Allow system to auto-tune TCP window size (default).</td></tr><tr><td><i>system</i></td><td>Use system default TCP window size for this protocol.</td></tr><tr><td><i>static</i></td><td>Manually specify TCP window size.</td></tr><tr><td><i>dynamic</i></td><td>Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.</td></tr></table>	Option	Description	<i>auto-tuning</i>	Allow system to auto-tune TCP window size (default).	<i>system</i>	Use system default TCP window size for this protocol.	<i>static</i>	Manually specify TCP window size.	<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.			
	Option	Description												
	<i>auto-tuning</i>	Allow system to auto-tune TCP window size (default).												
	<i>system</i>	Use system default TCP window size for this protocol.												
	<i>static</i>	Manually specify TCP window size.												
<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.													
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072										

Parameter	Description	Type	Size	Default								
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 33554432	8388608								
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	262144								
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>no</td><td>SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled.</td></tr><tr><td>yes</td><td>SSL decryption and encryption performed by an external device.</td></tr></table>				Option	Description	no	SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled.	yes	SSL decryption and encryption performed by an external device.		
	Option	Description										
	no	SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled.										
yes	SSL decryption and encryption performed by an external device.											
address-ip-rating	Enable/disable IP based URL rating.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.		
	Option	Description										
	enable	Enable setting.										
disable	Disable setting.											
encrypted-file	Encrypted file action.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>pass</td><td>Pass encrypted files without content scan.</td></tr><tr><td>inspect</td><td>Request password to decrypt and scan encrypted file. Files failed to decrypt will be blocked.</td></tr><tr><td>block</td><td>Block encrypted files.</td></tr></table>				Option	Description	pass	Pass encrypted files without content scan.	inspect	Request password to decrypt and scan encrypted file. Files failed to decrypt will be blocked.	block	Block encrypted files.
	Option	Description										
	pass	Pass encrypted files without content scan.										
	inspect	Request password to decrypt and scan encrypted file. Files failed to decrypt will be blocked.										
block	Block encrypted files.											
encrypted-file-log	Enable/disable Log encrypted file.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.		
	Option	Description										
	enable	Enable setting.										
disable	Disable setting.											

* This parameter may not exist in some models.

** Values may differ between models.

config ftp

Parameter	Description	Type	Size	Default												
ports	Ports to scan for content.	integer	Minimum value: 1 Maximum value: 65535													
status	Enable/disable the active status of scanning for this protocol.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.						
	Option	Description														
	<i>enable</i>	Enable setting.														
<i>disable</i>	Disable setting.															
options	One or more options that can be applied to the session.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>clientcomfort</i></td><td>Prevent client timeout.</td></tr><tr><td><i>oversize</i></td><td>Block oversized file.</td></tr><tr><td><i>splice</i></td><td>Enable splice mode.</td></tr><tr><td><i>bypass-rest-command</i></td><td>Bypass REST command.</td></tr><tr><td><i>bypass-mode-command</i></td><td>Bypass MODE command.</td></tr></table>				Option	Description	<i>clientcomfort</i>	Prevent client timeout.	<i>oversize</i>	Block oversized file.	<i>splice</i>	Enable splice mode.	<i>bypass-rest-command</i>	Bypass REST command.	<i>bypass-mode-command</i>	Bypass MODE command.
	Option	Description														
	<i>clientcomfort</i>	Prevent client timeout.														
	<i>oversize</i>	Block oversized file.														
	<i>splice</i>	Enable splice mode.														
	<i>bypass-rest-command</i>	Bypass REST command.														
<i>bypass-mode-command</i>	Bypass MODE command.															
comfort-interval	Interval between successive transmissions of data for client comforting (seconds).	integer	Minimum value: 1 Maximum value: 900	10												
comfort-amount	Number of bytes to send in each transmission for client comforting (bytes).	integer	Minimum value: 1 Maximum value: 65535	1												
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 26214**	10												
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 1 Maximum value: 26214**	10												

Parameter	Description	Type	Size	Default										
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12										
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned in megabytes. Stream-based uncompression used only under certain conditions.	integer	Minimum value: 0 Maximum value: 4294967295	0										
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
	Option	Description												
	<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.													
tcp-window-type	TCP window type to use for this protocol.	option	-	auto-tuning										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto-tuning</i></td><td>Allow system to auto-tune TCP window size (default).</td></tr><tr><td><i>system</i></td><td>Use system default TCP window size for this protocol.</td></tr><tr><td><i>static</i></td><td>Manually specify TCP window size.</td></tr><tr><td><i>dynamic</i></td><td>Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.</td></tr></table>				Option	Description	<i>auto-tuning</i>	Allow system to auto-tune TCP window size (default).	<i>system</i>	Use system default TCP window size for this protocol.	<i>static</i>	Manually specify TCP window size.	<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.
	Option	Description												
	<i>auto-tuning</i>	Allow system to auto-tune TCP window size (default).												
	<i>system</i>	Use system default TCP window size for this protocol.												
	<i>static</i>	Manually specify TCP window size.												
<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.													
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072										
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 33554432	8388608										
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	262144										

Parameter	Description	Type	Size	Default
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no
	Option	Description		
	no	SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled.		
	yes	SSL decryption and encryption performed by an external device.		
explicit-ftp-tls	Enable/disable deep inspection of FTP control session over STARTTLS.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		

** Values may differ between models.

config imap

Parameter	Description	Type	Size	Default						
ports	Ports to scan for content.	integer	Minimum value: 1 Maximum value: 65535							
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
options	One or more options that can be applied to the session.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fragmail</i></td><td>Pass fragmented email.</td></tr><tr><td><i>oversize</i></td><td>Block oversized email.</td></tr></table>				Option	Description	<i>fragmail</i>	Pass fragmented email.	<i>oversize</i>	Block oversized email.
	Option	Description								
	<i>fragmail</i>	Pass fragmented email.								
<i>oversize</i>	Block oversized email.									

Parameter	Description	Type	Size	Default						
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 26214**	10						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 1 Maximum value: 26214**	10						
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>no</i></td><td>SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled.</td></tr><tr><td><i>yes</i></td><td>SSL decryption and encryption performed by an external device.</td></tr></table>				Option	Description	<i>no</i>	SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled.	<i>yes</i>	SSL decryption and encryption performed by an external device.
Option	Description									
<i>no</i>	SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled.									
<i>yes</i>	SSL decryption and encryption performed by an external device.									
address-ip-rating	Enable/disable IP based URL rating.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

** Values may differ between models.

config mapi

Parameter	Description	Type	Size	Default						
ports	Ports to scan for content.	integer	Minimum value: 1 Maximum value: 65535							
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
options	One or more options that can be applied to the session.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fragmail</i></td><td>Pass fragmented email.</td></tr><tr><td><i>oversize</i></td><td>Block oversized email.</td></tr></table>	Option	Description	<i>fragmail</i>	Pass fragmented email.	<i>oversize</i>	Block oversized email.			
Option	Description									
<i>fragmail</i>	Pass fragmented email.									
<i>oversize</i>	Block oversized email.									
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 26214**	10						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 1 Maximum value: 26214**	10						
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

** Values may differ between models.

config pop3

Parameter	Description	Type	Size	Default
ports	Ports to scan for content.	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	OptionDescription			
	enable	Enable setting.		
	disable	Disable setting.		
options	One or more options that can be applied to the session.	option	-	
	OptionDescription			
	fragmail	Pass fragmented email.		
	oversize	Block oversized email.		
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 26214**	10
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 1 Maximum value: 26214**	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	OptionDescription			
	enable	Enable setting.		
	disable	Disable setting.		

Parameter	Description	Type	Size	Default
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no
	Option Description			
	<i>no</i>	SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled.		
	<i>yes</i>	SSL decryption and encryption performed by an external device.		

** Values may differ between models.

config smtp

Parameter	Description	Type	Size	Default
ports	Ports to scan for content.	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
options	One or more options that can be applied to the session.	option	-	
	Option Description			
	<i>fragmail</i>	Pass fragmented email.		
	<i>oversize</i>	Block oversized email.		
	<i>splice</i>	Enable splice mode.		
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 26214**	10

Parameter	Description	Type	Size	Default						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 1 Maximum value: 26214**	10						
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
server-busy	Enable/disable SMTP server busy when server not available.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>no</td><td>SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled.</td></tr><tr><td>yes</td><td>SSL decryption and encryption performed by an external device.</td></tr></table>	Option	Description	no	SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled.	yes	SSL decryption and encryption performed by an external device.			
Option	Description									
no	SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled.									
yes	SSL decryption and encryption performed by an external device.									

** Values may differ between models.

config nntp

Parameter	Description	Type	Size	Default
ports	Ports to scan for content.	integer	Minimum value: 1 Maximum value: 65535	

Parameter	Description	Type	Size	Default
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
options	One or more options that can be applied to the session.	option	-	
	Option Description			
	<i>oversize</i>	Block oversized file.		
	<i>splice</i>	Enable splice mode.		
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 26214**	10
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 1 Maximum value: 26214**	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

** Values may differ between models.

config ssh

Parameter	Description	Type	Size	Default
options	One or more options that can be applied to the session.	option	-	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>oversize</i>	Block oversized file.		
	<i>clientcomfort</i>	Prevent client timeout.		
	<i>servercomfort</i>	Prevent server timeout.		
comfort-interval	Interval between successive transmissions of data for client comforting (seconds).	integer	Minimum value: 1 Maximum value: 900	10
comfort-amount	Number of bytes to send in each transmission for client comforting (bytes).	integer	Minimum value: 1 Maximum value: 65535	1
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 26214**	10
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 1 Maximum value: 26214**	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned in megabytes. Stream-based uncompression used only under certain conditions.	integer	Minimum value: 0 Maximum value: 4294967295	0
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
tcp-window-type	TCP window type to use for this protocol.	option	-	auto-tuning

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>auto-tuning</i>	Allow system to auto-tune TCP window size (default).		
	<i>system</i>	Use system default TCP window size for this protocol.		
	<i>static</i>	Manually specify TCP window size.		
	<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.		
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 33554432	8388608
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	262144
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no
	Option	Description		
	<i>no</i>	SSL decryption and encryption performed by FortiProxy when deep-inspection is enabled.		
	<i>yes</i>	SSL decryption and encryption performed by an external device.		

** Values may differ between models.

config dns

Parameter	Description	Type	Size	Default
ports	Ports to scan for content.	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		

config cifs

Parameter	Description	Type	Size	Default						
ports	Ports to scan for content.	integer	Minimum value: 1 Maximum value: 65535							
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
options	One or more options that can be applied to the session.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>oversize</i></td><td>Block oversized file.</td></tr></table>	Option	Description	<i>oversize</i>	Block oversized file.					
Option	Description									
<i>oversize</i>	Block oversized file.									
oversize-limit	Maximum in-memory file size that can be scanned (MB).	integer	Minimum value: 1 Maximum value: 26214**	10						

Parameter	Description	Type	Size	Default										
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 1 Maximum value: 26214**	10										
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12										
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
tcp-window-type	TCP window type to use for this protocol.	option	-	auto-tuning										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto-tuning</i></td><td>Allow system to auto-tune TCP window size (default).</td></tr><tr><td><i>system</i></td><td>Use system default TCP window size for this protocol.</td></tr><tr><td><i>static</i></td><td>Manually specify TCP window size.</td></tr><tr><td><i>dynamic</i></td><td>Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.</td></tr></table>	Option	Description	<i>auto-tuning</i>	Allow system to auto-tune TCP window size (default).	<i>system</i>	Use system default TCP window size for this protocol.	<i>static</i>	Manually specify TCP window size.	<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.			
Option	Description													
<i>auto-tuning</i>	Allow system to auto-tune TCP window size (default).													
<i>system</i>	Use system default TCP window size for this protocol.													
<i>static</i>	Manually specify TCP window size.													
<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.													
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072										
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 33554432	8388608										

Parameter	Description	Type	Size	Default								
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	262144								
server-credential-type	CIFS server credential type.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Credential derivation not set.</td></tr><tr><td><i>credential-replication</i></td><td>Credential derived using Replication account on Domain Controller.</td></tr><tr><td><i>credential-keytab</i></td><td>Credential derived using server keytab.</td></tr></table>				Option	Description	<i>none</i>	Credential derivation not set.	<i>credential-replication</i>	Credential derived using Replication account on Domain Controller.	<i>credential-keytab</i>	Credential derived using server keytab.
	Option	Description										
	<i>none</i>	Credential derivation not set.										
	<i>credential-replication</i>	Credential derived using Replication account on Domain Controller.										
<i>credential-keytab</i>	Credential derived using server keytab.											
domain-controller	Domain for which to decrypt CIFS traffic.	string	Maximum length: 63									

** Values may differ between models.

config server-keytab

Parameter	Description	Type	Size	Default
principal	Service principal. For example, host/cifsserver.example.com@example.com.	string	Maximum length: 511	
keytab	Base64 encoded keytab file containing credential of the server.	string	Maximum length: 8191	

config mail-signature

Parameter	Description	Type	Size	Default						
status	Enable/disable adding an email signature to SMTP email messages as they pass through the FortiProxy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable mail signature.</td></tr><tr><td><i>enable</i></td><td>Enable mail signature.</td></tr></table>				Option	Description	<i>disable</i>	Disable mail signature.	<i>enable</i>	Enable mail signature.
	Option	Description								
	<i>disable</i>	Disable mail signature.								
<i>enable</i>	Enable mail signature.									
signature	Email signature to be added to outgoing email (if the signature contains spaces, enclose with quotation marks).	string	Maximum length: 1023							

config firewall proxy-address

Configure web proxy address.

```
config firewall proxy-address
  Description: Configure web proxy address.
  edit <name>
    set uuid {uuid}
    set type [host-regex|url|...]
    set host {string}
    set host-regex {string}
    set path {string}
    set query {string}
    set referrer [enable|disable]
    set post-arg [enable|disable]
    set category <id1>, <id2>, ...
    set url-list {string}
    set method {option1}, {option2}, ...
    set ua {option1}, {option2}, ...
    set ua-min-ver {string}
    set ua-max-ver {string}
    set header-name {string}
    set header {string}
    set case-sensitivity [disable|enable]
    config header-group
      Description: HTTP header group.
      edit <id>
        set header-name {string}
        set header {string}
        set case-sensitivity [disable|enable]
      next
    end
  set color {integer}
  config tagging
    Description: Config object tagging.
    edit <name>
      set category {string}
      set tags <name1>, <name2>, ...
    next
  end
  set comment {var-string}
  set application <name1>, <name2>, ...
next
end
```

config firewall proxy-address

Parameter	Description	Type	Size	Default
name	Address name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
type	Proxy address type.	option	-	url
	Option	Description		
	<i>host-regex</i>	Host regular expression.		
	<i>url</i>	HTTP URL.		
	<i>category</i>	FortiGuard URL category.		
	<i>url-list</i>	HTTP URL list from external resource or Web filter URL list.		
	<i>method</i>	HTTP request method.		
	<i>ua</i>	HTTP request user agent.		
	<i>header</i>	HTTP request header.		
	<i>src-advanced</i>	HTTP advanced source criteria.		
	<i>dst-advanced</i>	HTTP advanced destination criteria.		
	<i>saas</i>	SaaS application.		
host	Address object for the host.	string	Maximum length: 79	
host-regex	Host name as a regular expression.	string	Maximum length: 255	
path	URL path as a regular expression.	string	Maximum length: 255	
query	Match the query part of the URL as a regular expression.	string	Maximum length: 255	
referrer	Enable/disable use of referrer field in the HTTP header to match the address.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
post-arg	Enable/disable use of body in the HTTP POST to match the query.	option	-	disable

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.															
	Option	Description																				
	<i>enable</i>	Enable setting.																				
<i>disable</i>	Disable setting.																					
category <id>	FortiGuard category ID. FortiGuard category ID.	integer	Minimum value: 0 Maximum value: 4294967295																			
url-list	External or Web filter URL list.	string	Maximum length: 35																			
method	HTTP request methods to be used.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>get</i></td><td>GET method.</td></tr><tr><td><i>post</i></td><td>POST method.</td></tr><tr><td><i>put</i></td><td>PUT method.</td></tr><tr><td><i>head</i></td><td>HEAD method.</td></tr><tr><td><i>connect</i></td><td>CONNECT method.</td></tr><tr><td><i>trace</i></td><td>TRACE method.</td></tr><tr><td><i>options</i></td><td>OPTIONS method.</td></tr><tr><td><i>delete</i></td><td>DELETE method.</td></tr></table>	Option	Description	<i>get</i>	GET method.	<i>post</i>	POST method.	<i>put</i>	PUT method.	<i>head</i>	HEAD method.	<i>connect</i>	CONNECT method.	<i>trace</i>	TRACE method.	<i>options</i>	OPTIONS method.	<i>delete</i>	DELETE method.			
	Option	Description																				
	<i>get</i>	GET method.																				
	<i>post</i>	POST method.																				
	<i>put</i>	PUT method.																				
	<i>head</i>	HEAD method.																				
	<i>connect</i>	CONNECT method.																				
	<i>trace</i>	TRACE method.																				
	<i>options</i>	OPTIONS method.																				
<i>delete</i>	DELETE method.																					
ua	Names of browsers to be used as user agent.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>chrome</i></td><td>Google Chrome.</td></tr><tr><td><i>ms</i></td><td>Microsoft Internet Explorer or EDGE.</td></tr><tr><td><i>firefox</i></td><td>Mozilla Firefox.</td></tr><tr><td><i>safari</i></td><td>Apple Safari.</td></tr><tr><td><i>ie</i></td><td>Microsoft Internet Explorer.</td></tr><tr><td><i>edge</i></td><td>Microsoft Edge.</td></tr><tr><td><i>other</i></td><td>Other browsers.</td></tr></table>	Option	Description	<i>chrome</i>	Google Chrome.	<i>ms</i>	Microsoft Internet Explorer or EDGE.	<i>firefox</i>	Mozilla Firefox.	<i>safari</i>	Apple Safari.	<i>ie</i>	Microsoft Internet Explorer.	<i>edge</i>	Microsoft Edge.	<i>other</i>	Other browsers.					
	Option	Description																				
	<i>chrome</i>	Google Chrome.																				
	<i>ms</i>	Microsoft Internet Explorer or EDGE.																				
	<i>firefox</i>	Mozilla Firefox.																				
	<i>safari</i>	Apple Safari.																				
	<i>ie</i>	Microsoft Internet Explorer.																				
	<i>edge</i>	Microsoft Edge.																				
<i>other</i>	Other browsers.																					

Parameter	Description	Type	Size	Default						
ua-min-ver	Minimum version of the user agent specified in dotted notation. For example, use 90.0.1 with the ua field set to "chrome" to require Google Chrome's minimum version must be 90.0.1.	string	Maximum length: 63							
ua-max-ver	Maximum version of the user agent specified in dotted notation. For example, use 120 with the ua field set to "chrome" to require Google Chrome's maximum version must be 120.	string	Maximum length: 63							
header-name	Name of HTTP header.	string	Maximum length: 79							
header	HTTP header name as a regular expression.	string	Maximum length: 255							
case-sensitivity	Enable to make the pattern case sensitive.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Case insensitive in pattern.</td></tr><tr><td>enable</td><td>Case sensitive in pattern.</td></tr></table>				Option	Description	disable	Case insensitive in pattern.	enable	Case sensitive in pattern.
Option	Description									
disable	Case insensitive in pattern.									
enable	Case sensitive in pattern.									
color	Integer value to determine the color of the icon in the GUI.	integer	Minimum value: 0 Maximum value: 32	0						
comment	Optional comments.	var-string	Maximum length: 255							
application<name>	SaaS application. SaaS application name.	string	Maximum length: 79							

config header-group

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
header-name	HTTP header.	string	Maximum length: 79	
header	HTTP header regular expression.	string	Maximum length: 255	

Parameter	Description	Type	Size	Default
case-sensitivity	Case sensitivity in pattern.	option	-	disable
	Option	Description		
	disable	Case insensitive in pattern.		
	enable	Case sensitive in pattern.		

config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

config firewall proxy-address6

Configure web proxy address6.

```
config firewall proxy-address6
  Description: Configure web proxy address6.
  edit <name>
    set uuid {uuid}
    set type [host-regex|url|...]
    set host {string}
    set host-regex {string}
    set path {string}
    set query {string}
    set referrer [enable|disable]
    set post-arg [enable|disable]
    set category <id1>, <id2>, ...
    set url-list {string}
    set method {option1}, {option2}, ...
    set ua {option1}, {option2}, ...
    set ua-min-ver {string}
    set ua-max-ver {string}
    set header-name {string}
    set header {string}
    set case-sensitivity [disable|enable]
    config header-group
      Description: HTTP header group.
      edit <id>
```

```

        set header-name {string}
        set header {string}
        set case-sensitivity [disable|enable]
    next
end
set color {integer}
config tagging
    Description: Config object tagging.
    edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
    next
end
set comment {var-string}
set application <name1>, <name2>, ...
next
end

```

config firewall proxy-address6

Parameter	Description	Type	Size	Default
name	Address6 name.	string	Maximum length: 79	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
type	Proxy address6 type.	option	-	url
	Option		Description	
	<i>host-regex</i>		Host regular expression.	
	<i>url</i>		HTTP URL.	
	<i>category</i>		FortiGuard URL category.	
	<i>url-list</i>		HTTP URL list from external resource or Web filter URL list.	
	<i>method</i>		HTTP request method.	
	<i>ua</i>		HTTP request user agent.	
	<i>header</i>		HTTP request header.	
	<i>src-advanced</i>		HTTP advanced source criteria.	
	<i>dst-advanced</i>		HTTP advanced destination criteria.	
<i>saas</i>		SaaS application.		
host	Address6 object for the host.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default																		
host-regex	Host name as a regular expression.	string	Maximum length: 255																			
path	URL path as a regular expression.	string	Maximum length: 255																			
query	Match the query part of the URL as a regular expression.	string	Maximum length: 255																			
referrer	Enable/disable use of referrer field in the HTTP header to match the address.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.												
Option	Description																					
<i>enable</i>	Enable setting.																					
<i>disable</i>	Disable setting.																					
post-arg	Enable/disable use of body in the HTTP POST to match the query.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.												
Option	Description																					
<i>enable</i>	Enable setting.																					
<i>disable</i>	Disable setting.																					
category<id>	FortiGuard category ID. FortiGuard category ID.	integer	Minimum value: 0 Maximum value: 4294967295																			
url-list	External or Web filter URL list.	string	Maximum length: 35																			
method	HTTP request methods to be used.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>get</i></td><td>GET method.</td></tr><tr><td><i>post</i></td><td>POST method.</td></tr><tr><td><i>put</i></td><td>PUT method.</td></tr><tr><td><i>head</i></td><td>HEAD method.</td></tr><tr><td><i>connect</i></td><td>CONNECT method.</td></tr><tr><td><i>trace</i></td><td>TRACE method.</td></tr><tr><td><i>options</i></td><td>OPTIONS method.</td></tr><tr><td><i>delete</i></td><td>DELETE method.</td></tr></table>				Option	Description	<i>get</i>	GET method.	<i>post</i>	POST method.	<i>put</i>	PUT method.	<i>head</i>	HEAD method.	<i>connect</i>	CONNECT method.	<i>trace</i>	TRACE method.	<i>options</i>	OPTIONS method.	<i>delete</i>	DELETE method.
Option	Description																					
<i>get</i>	GET method.																					
<i>post</i>	POST method.																					
<i>put</i>	PUT method.																					
<i>head</i>	HEAD method.																					
<i>connect</i>	CONNECT method.																					
<i>trace</i>	TRACE method.																					
<i>options</i>	OPTIONS method.																					
<i>delete</i>	DELETE method.																					

Parameter	Description	Type	Size	Default																
ua	Names of browsers to be used as user agent.	option	-																	
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>chrome</td><td>Google Chrome.</td></tr><tr><td>ms</td><td>Microsoft Internet Explorer or EDGE.</td></tr><tr><td>firefox</td><td>Mozilla Firefox.</td></tr><tr><td>safari</td><td>Apple Safari.</td></tr><tr><td>ie</td><td>Microsoft Internet Explorer.</td></tr><tr><td>edge</td><td>Microsoft Edge.</td></tr><tr><td>other</td><td>Other browsers.</td></tr></table>	Option	Description	chrome	Google Chrome.	ms	Microsoft Internet Explorer or EDGE.	firefox	Mozilla Firefox.	safari	Apple Safari.	ie	Microsoft Internet Explorer.	edge	Microsoft Edge.	other	Other browsers.			
	Option	Description																		
	chrome	Google Chrome.																		
	ms	Microsoft Internet Explorer or EDGE.																		
	firefox	Mozilla Firefox.																		
	safari	Apple Safari.																		
	ie	Microsoft Internet Explorer.																		
	edge	Microsoft Edge.																		
other	Other browsers.																			
ua-min-ver	Minimum version of the user agent specified in dotted notation. For example, use 90.0.1 with the ua field set to "chrome" to require Google Chrome's minimum version must be 90.0.1.	string	Maximum length: 63																	
ua-max-ver	Maximum version of the user agent specified in dotted notation. For example, use 120 with the ua field set to "chrome" to require Google Chrome's maximum version must be 120.	string	Maximum length: 63																	
header-name	Name of HTTP header.	string	Maximum length: 79																	
header	HTTP header name as a regular expression.	string	Maximum length: 255																	
case-sensitivity	Enable to make the pattern case sensitive.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Case insensitive in pattern.</td></tr><tr><td>enable</td><td>Case sensitive in pattern.</td></tr></table>	Option	Description	disable	Case insensitive in pattern.	enable	Case sensitive in pattern.													
	Option	Description																		
	disable	Case insensitive in pattern.																		
enable	Case sensitive in pattern.																			
color	Integer value to determine the color of the icon in the GUI.	integer	Minimum value: 0 Maximum value: 32	0																
comment	Optional comments.	var-string	Maximum length: 255																	
application <name>	SaaS application. SaaS application name.	string	Maximum length: 79																	

config header-group

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
header-name	HTTP header.	string	Maximum length: 79	
header	HTTP header regular expression.	string	Maximum length: 255	
case-sensitivity	Case sensitivity in pattern.	option	-	disable
	Option	Description		
	disable	Case insensitive in pattern.		
	enable	Case sensitive in pattern.		

config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

config firewall proxy-addrgrp

Configure web proxy address group.

```
config firewall proxy-addrgrp
  Description: Configure web proxy address group.
  edit <name>
    set type [src|dst]
    set uuid {uuid}
    set member <name1>, <name2>, ...
    set color {integer}
    config tagging
```

```

        Description: Config object tagging.
        edit <name>
            set category {string}
            set tags <name1>, <name2>, ...
        next
    end
    set comment {var-string}
next
end

```

config firewall proxy-addrgrp

Parameter	Description	Type	Size	Default						
name	Address group name.	string	Maximum length: 79							
type	Source or destination address group type.	option	-	src						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>src</td><td>Source group.</td></tr><tr><td>dst</td><td>Destination group.</td></tr></table>				Option	Description	src	Source group.	dst	Destination group.
	Option	Description								
	src	Source group.								
dst	Destination group.									
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
member <name>	Members of address group. Address name.	string	Maximum length: 79							
color	Integer value to determine the color of the icon in the GUI.	integer	Minimum value: 0 Maximum value: 32	0						
comment	Optional comments.	var-string	Maximum length: 255							

config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

config firewall proxy-addrgrp6

Configure web proxy address group6.

```
config firewall proxy-addrgrp6
  Description: Configure web proxy address group6.
  edit <name>
    set type [src|dst]
    set uuid {uuid}
    set member <name1>, <name2>, ...
    set color {integer}
    config tagging
      Description: Config object tagging.
      edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
      next
    end
    set comment {var-string}
  next
end
```

config firewall proxy-addrgrp6

Parameter	Description	Type	Size	Default						
name	Address group6.	string	Maximum length: 79							
type	Source or destination address group6 type.	option	-	src						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>src</td><td>Source group.</td></tr><tr><td>dst</td><td>Destination group.</td></tr></table>				Option	Description	src	Source group.	dst	Destination group.
	Option	Description								
	src	Source group.								
dst	Destination group.									
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
member <name>	Members of address group6. Address name.	string	Maximum length: 79							
color	Integer value to determine the color of the icon in the GUI.	integer	Minimum value: 0 Maximum value: 32	0						
comment	Optional comments.	var-string	Maximum length: 255							

config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

config firewall region

Define region table.

```
config firewall region
    Description: Define region table.
    edit <id>
        set name {string}
        set city <id1>, <id2>, ...
    next
end
```

config firewall region

Parameter	Description	Type	Size	Default
id	Region ID.	integer	Minimum value: 0 Maximum value: 65535	0
name	Region name.	string	Maximum length: 63	
city <id>	City ID list. City ID.	integer	Minimum value: 0 Maximum value: 65535	

config firewall schedule group

Schedule group configuration.

```

config firewall schedule group
    Description: Schedule group configuration.
    edit <name>
        set member <name1>, <name2>, ...
        set color {integer}
        set fabric-object [enable|disable]
    next
end

```

config firewall schedule group

Parameter	Description	Type	Size	Default
name	Schedule group name.	string	Maximum length: 31	
member <name>	Schedules added to the schedule group. Schedule name.	string	Maximum length: 79	
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
fabric-object	Security Fabric global object setting.	option	-	disable
		Option	Description	
		<i>enable</i>	Object is set as a security fabric-wide global object.	
		<i>disable</i>	Object is local to this security fabric member.	

config firewall schedule onetime

Onetime schedule configuration.

```

config firewall schedule onetime
    Description: Onetime schedule configuration.
    edit <name>
        set start {user}
        set start-utc {user}
        set end {user}
        set end-utc {user}
        set color {integer}
        set expiration-days {integer}
        set fabric-object [enable|disable]
    next
end

```

config firewall schedule onetime

Parameter	Description	Type	Size	Default
name	Onetime schedule name.	string	Maximum length: 31	
start	Schedule start date and time, format hh:mm yyyy/mm/dd.	user	Not Specified	
start-utc	Schedule start date and time, in epoch format.	user	Not Specified	
end	Schedule end date and time, format hh:mm yyyy/mm/dd.	user	Not Specified	
end-utc	Schedule end date and time, in epoch format.	user	Not Specified	
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
expiration-days	Write an event log message this many days before the schedule expires.	integer	Minimum value: 0 Maximum value: 100	3
fabric-object	Security Fabric global object setting.	option	-	disable
	Option	Description		
	enable	Object is set as a security fabric-wide global object.		
	disable	Object is local to this security fabric member.		

config firewall schedule recurring

Recurring schedule configuration.

```

config firewall schedule recurring
  Description: Recurring schedule configuration.
  edit <name>
    set start {user}
    set end {user}
    set day {option1}, {option2}, ...
    set color {integer}
    set fabric-object [enable|disable]
  next
end

```

config firewall schedule recurring

Parameter	Description	Type	Size	Default
name	Recurring schedule name.	string	Maximum length: 31	
start	Time of day to start the schedule, format hh:mm.	user	Not Specified	
end	Time of day to end the schedule, format hh:mm.	user	Not Specified	
day	One or more days of the week on which the schedule is valid. Separate the names of the days with a space.	option	-	none
	OptionDescription			
	sunday	Sunday.		
	monday	Monday.		
	tuesday	Tuesday.		
	wednesday	Wednesday.		
	thursday	Thursday.		
	friday	Friday.		
	saturday	Saturday.		
	none	None.		
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
fabric-object	Security Fabric global object setting.	option	-	disable
	OptionDescription			
	enable	Object is set as a security fabric-wide global object.		
	disable	Object is local to this security fabric member.		

config firewall service category

Configure service categories.

```
config firewall service category
  Description: Configure service categories.
  edit <name>
```

```

        set comment {var-string}
        set fabric-object [enable|disable]
    next
end

```

config firewall service category

Parameter	Description	Type	Size	Default
name	Service category name.	string	Maximum length: 63	
comment	Comment.	var-string	Maximum length: 255	
fabric-object	Security Fabric global object setting.	option	-	disable
		Option	Description	
		<i>enable</i>	Object is set as a security fabric-wide global object.	
		<i>disable</i>	Object is local to this security fabric member.	

config firewall service custom

Configure custom services.

```

config firewall service custom
    Description: Configure custom services.
    edit <name>
        set proxy [enable|disable]
        set category {string}
        set protocol [TCP/UDP/SCTP|ICMP|...]
        set iprange {user}
        set fqdn {string}
        set protocol-number {integer}
        set icmptype {integer}
        set icmpcode {integer}
        set tcp-portrange {user}
        set udp-portrange {user}
        set sctp-portrange {user}
        set tcp-halfclose-timer {integer}
        set tcp-halfopen-timer {integer}
        set tcp-timewait-timer {integer}
        set tcp-rst-timer {integer}
        set udp-idle-timer {integer}
        set session-ttl {user}
        set check-reset-range [disable|strict|...]
        set comment {var-string}
        set color {integer}
        set app-service-type [disable|app-id|...]
        set app-category <id1>, <id2>, ...
    end
end

```

```

        set application <id1>, <id2>, ...
        set fabric-object [enable|disable]
    next
end

```

config firewall service custom

Parameter	Description	Type	Size	Default																						
name	Custom service name.	string	Maximum length: 79																							
proxy	Enable/disable web proxy service.	option	-	disable																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																
	Option	Description																								
	<i>enable</i>	Enable setting.																								
<i>disable</i>	Disable setting.																									
category	Service category.	string	Maximum length: 63																							
protocol	Protocol type based on IANA numbers.	option	-	TCP/UDP/SCTP																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TCP/UDP/SCTP</i></td><td>TCP, UDP and SCTP.</td></tr><tr><td><i>ICMP</i></td><td>ICMP.</td></tr><tr><td><i>ICMP6</i></td><td>ICMP6.</td></tr><tr><td><i>IP</i></td><td>IP.</td></tr><tr><td><i>HTTP</i></td><td>HTTP - for web proxy.</td></tr><tr><td><i>FTP</i></td><td>FTP - for web proxy.</td></tr><tr><td><i>CONNECT</i></td><td>Connect - for web proxy.</td></tr><tr><td><i>SOCKS-TCP</i></td><td>Socks TCP - for web proxy.</td></tr><tr><td><i>SOCKS-UDP</i></td><td>Socks UDP - for web proxy.</td></tr><tr><td><i>ALL</i></td><td>All - for web proxy.</td></tr></table>				Option	Description	<i>TCP/UDP/SCTP</i>	TCP, UDP and SCTP.	<i>ICMP</i>	ICMP.	<i>ICMP6</i>	ICMP6.	<i>IP</i>	IP.	<i>HTTP</i>	HTTP - for web proxy.	<i>FTP</i>	FTP - for web proxy.	<i>CONNECT</i>	Connect - for web proxy.	<i>SOCKS-TCP</i>	Socks TCP - for web proxy.	<i>SOCKS-UDP</i>	Socks UDP - for web proxy.	<i>ALL</i>	All - for web proxy.
	Option	Description																								
	<i>TCP/UDP/SCTP</i>	TCP, UDP and SCTP.																								
	<i>ICMP</i>	ICMP.																								
	<i>ICMP6</i>	ICMP6.																								
	<i>IP</i>	IP.																								
	<i>HTTP</i>	HTTP - for web proxy.																								
	<i>FTP</i>	FTP - for web proxy.																								
	<i>CONNECT</i>	Connect - for web proxy.																								
	<i>SOCKS-TCP</i>	Socks TCP - for web proxy.																								
	<i>SOCKS-UDP</i>	Socks UDP - for web proxy.																								
<i>ALL</i>	All - for web proxy.																									
iprange	Start and end of the IP range associated with service.	user	Not Specified																							
fqdn	Fully qualified domain name.	string	Maximum length: 255																							

Parameter	Description	Type	Size	Default
protocol-number	IP protocol number.	integer	Minimum value: 0 Maximum value: 254	0
icmptype	ICMP type.	integer	Minimum value: 0 Maximum value: 4294967295	
icmpcode	ICMP code.	integer	Minimum value: 0 Maximum value: 255	
tcp-portrange	Multiple TCP port ranges.	user	Not Specified	
udp-portrange	Multiple UDP port ranges.	user	Not Specified	
sctp-portrange	Multiple SCTP port ranges.	user	Not Specified	
tcp-halfclose-timer	Wait time to close a TCP session waiting for an unanswered FIN packet.	integer	Minimum value: 0 Maximum value: 86400	0
tcp-halfopen-timer	Wait time to close a TCP session waiting for an unanswered open session packet.	integer	Minimum value: 0 Maximum value: 86400	0
tcp-timewait-timer	Set the length of the TCP TIME-WAIT state in seconds.	integer	Minimum value: 0 Maximum value: 300	0
tcp-rst-timer	Set the length of the TCP CLOSE state in seconds.	integer	Minimum value: 5 Maximum value: 300	0
udp-idle-timer	Number of seconds before an idle UDP connection times out.	integer	Minimum value: 0 Maximum value: 86400	0
session-ttl	Session TTL.	user	Not Specified	
check-reset-range	Configure the type of ICMP error message verification.	option	-	default

Parameter	Description	Type	Size	Default
	Option Description			
	<i>disable</i>	Disable RST range check.		
	<i>strict</i>	Check RST range strictly.		
	<i>default</i>	Using system default setting.		
comment	Comment.	var-string	Maximum length: 255	
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
app-service-type	Application service type.	option	-	disable
	Option Description			
	<i>disable</i>	Disable application type.		
	<i>app-id</i>	Application ID.		
	<i>app-category</i>	Applicatin category.		
app-category <id>	Application category ID. Application category id.	integer	Minimum value: 0 Maximum value: 4294967295	
application <id>	Application ID. Application id.	integer	Minimum value: 0 Maximum value: 4294967295	
fabric-object	Security Fabric global object setting.	option	-	disable
	Option Description			
	<i>enable</i>	Object is set as a security fabric-wide global object.		
	<i>disable</i>	Object is local to this security fabric member.		

config firewall service group

Configure service groups.


```

config firewall service group
    Description: Configure service groups.
    edit <name>
        set proxy [enable|disable]
        set member <name1>, <name2>, ...
        set comment {var-string}
        set color {integer}
        set fabric-object [enable|disable]
    next
end

```

config firewall service group

Parameter	Description	Type	Size	Default
name	Service group name.	string	Maximum length: 79	
proxy	Enable/disable web proxy service group.	option	-	disable
	Option Description			
	enable Enable setting.			
	disable Disable setting.			
member <name>	Service objects contained within the group. Service or service group name.	string	Maximum length: 79	
comment	Comment.	var-string	Maximum length: 255	
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
fabric-object	Security Fabric global object setting.	option	-	disable
	Option Description			
	enable Object is set as a security fabric-wide global object.			
	disable Object is local to this security fabric member.			

config firewall shaper per-ip-shaper

Configure per-IP traffic shaper.

```

config firewall shaper per-ip-shaper
    Description: Configure per-IP traffic shaper.
    edit <name>

```

```

    set max-bandwidth {integer}
    set bandwidth-unit [kbps|mbps|...]
    set max-concurrent-session {integer}
    set max-concurrent-tcp-session {integer}
    set max-concurrent-udp-session {integer}
    set diffserv-forward [enable|disable]
    set diffserv-reverse [enable|disable]
    set diffservcode-forward {user}
    set diffservcode-rev {user}
next
end

```

config firewall shaper per-ip-shaper

Parameter	Description	Type	Size	Default								
name	Traffic shaper name.	string	Maximum length: 35									
max-bandwidth	Upper bandwidth limit enforced by this shaper. 0 means no limit. Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 80000000	0								
bandwidth-unit	Unit of measurement for maximum bandwidth for this shaper (Kbps, Mbps or Gbps).	option	-	kbps								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>kbps</td><td>Kilobits per second.</td></tr><tr><td>mbps</td><td>Megabits per second.</td></tr><tr><td>gbps</td><td>Gigabits per second.</td></tr></table>				Option	Description	kbps	Kilobits per second.	mbps	Megabits per second.	gbps	Gigabits per second.
Option	Description											
kbps	Kilobits per second.											
mbps	Megabits per second.											
gbps	Gigabits per second.											
max-concurrent-session	Maximum number of concurrent sessions allowed by this shaper. 0 means no limit.	integer	Minimum value: 0 Maximum value: 2097000	0								
max-concurrent-tcp-session	Maximum number of concurrent TCP sessions allowed by this shaper. 0 means no limit.	integer	Minimum value: 0 Maximum value: 2097000	0								
max-concurrent-udp-session	Maximum number of concurrent UDP sessions allowed by this shaper. 0 means no limit.	integer	Minimum value: 0 Maximum value: 2097000	0								

Parameter	Description	Type	Size	Default						
diffserv-forward	Enable/disable changing the Forward (original) DiffServ setting applied to traffic accepted by this shaper.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting forward (original) traffic DiffServ.</td></tr><tr><td><i>disable</i></td><td>Disable setting forward (original) traffic DiffServ.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting forward (original) traffic DiffServ.	<i>disable</i>	Disable setting forward (original) traffic DiffServ.			
Option	Description									
<i>enable</i>	Enable setting forward (original) traffic DiffServ.									
<i>disable</i>	Disable setting forward (original) traffic DiffServ.									
diffserv-reverse	Enable/disable changing the Reverse (reply) DiffServ setting applied to traffic accepted by this shaper.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting reverse (reply) traffic DiffServ.</td></tr><tr><td><i>disable</i></td><td>Disable setting reverse (reply) traffic DiffServ.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.	<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.			
Option	Description									
<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.									
<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.									
diffservcode-forward	Forward (original) DiffServ setting to be applied to traffic accepted by this shaper.	user	Not Specified							
diffservcode-rev	Reverse (reply) DiffServ setting to be applied to traffic accepted by this shaper.	user	Not Specified							

config firewall shaper traffic-shaper

Configure shared traffic shaper.

```
config firewall shaper traffic-shaper
  Description: Configure shared traffic shaper.
  edit <name>
    set guaranteed-bandwidth {integer}
    set maximum-bandwidth {integer}
    set bandwidth-unit [kbps|mbps|...]
    set priority [low|medium|...]
    set per-policy [disable|enable]
    set diffserv [enable|disable]
    set diffservcode {user}
    set dscp-marking-method [multi-stage|static]
    set exceed-bandwidth {integer}
    set exceed-dscp {user}
    set maximum-dscp {user}
    set overhead {integer}
  next
end
```

config firewall shaper traffic-shaper

Parameter	Description	Type	Size	Default								
name	Traffic shaper name.	string	Maximum length: 35									
guaranteed-bandwidth	Amount of bandwidth guaranteed for this shaper. Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 80000000	0								
maximum-bandwidth	Upper bandwidth limit enforced by this shaper. 0 means no limit. Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 80000000	0								
bandwidth-unit	Unit of measurement for guaranteed and maximum bandwidth for this shaper (Kbps, Mbps or Gbps).	option	-	kbps								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>kbps</i></td><td>Kilobits per second.</td></tr><tr><td><i>mbps</i></td><td>Megabits per second.</td></tr><tr><td><i>gbps</i></td><td>Gigabits per second.</td></tr></table>				Option	Description	<i>kbps</i>	Kilobits per second.	<i>mbps</i>	Megabits per second.	<i>gbps</i>	Gigabits per second.
Option	Description											
<i>kbps</i>	Kilobits per second.											
<i>mbps</i>	Megabits per second.											
<i>gbps</i>	Gigabits per second.											
priority	Higher priority traffic is more likely to be forwarded without delays and without compromising the guaranteed bandwidth.	option	-	high								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>low</i></td><td>Low priority.</td></tr><tr><td><i>medium</i></td><td>Medium priority.</td></tr><tr><td><i>high</i></td><td>High priority.</td></tr></table>				Option	Description	<i>low</i>	Low priority.	<i>medium</i>	Medium priority.	<i>high</i>	High priority.
Option	Description											
<i>low</i>	Low priority.											
<i>medium</i>	Medium priority.											
<i>high</i>	High priority.											
per-policy	Enable/disable applying a separate shaper for each policy. For example, if enabled the guaranteed bandwidth is applied separately for each policy.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>All referring policies share one traffic shaper.</td></tr><tr><td><i>enable</i></td><td>Each referring policy has its own traffic shaper.</td></tr></table>				Option	Description	<i>disable</i>	All referring policies share one traffic shaper.	<i>enable</i>	Each referring policy has its own traffic shaper.		
Option	Description											
<i>disable</i>	All referring policies share one traffic shaper.											
<i>enable</i>	Each referring policy has its own traffic shaper.											
diffserv	Enable/disable changing the DiffServ setting applied to traffic accepted by this shaper.	option	-	disable								

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting traffic DiffServ.</td></tr><tr><td><i>disable</i></td><td>Disable setting traffic DiffServ.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting traffic DiffServ.	<i>disable</i>	Disable setting traffic DiffServ.			
	Option	Description								
	<i>enable</i>	Enable setting traffic DiffServ.								
<i>disable</i>	Disable setting traffic DiffServ.									
diffservcode	DiffServ setting to be applied to traffic accepted by this shaper.	user	Not Specified							
dscp-marking-method	Select DSCP marking method.	option	-	static						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>multi-stage</i></td><td>Multistage marking.</td></tr><tr><td><i>static</i></td><td>Static marking.</td></tr></table>	Option	Description	<i>multi-stage</i>	Multistage marking.	<i>static</i>	Static marking.			
	Option	Description								
	<i>multi-stage</i>	Multistage marking.								
<i>static</i>	Static marking.									
exceed-bandwidth	Exceed bandwidth used for DSCP multi-stage marking. Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 80000000	0						
exceed-dscp	DSCP mark for traffic in guaranteed-bandwidth and exceed-bandwidth.	user	Not Specified							
maximum-dscp	DSCP mark for traffic in exceed-bandwidth and maximum-bandwidth.	user	Not Specified							
overhead	Per-packet size overhead used in rate computations.	integer	Minimum value: 0 Maximum value: 100	0						

config firewall shaping-policy

Configure shaping policies.

```
config firewall shaping-policy
  Description: Configure shaping policies.
  edit <id>
    set uuid {uuid}
    set name {string}
    set comment {var-string}
    set status [enable|disable]
    set ip-version [4|6]
    set service-type [service|internet-service]
    set srcaddr <name1>, <name2>, ...
    set dstaddr <name1>, <name2>, ...
    set srcaddr6 <name1>, <name2>, ...
```

```

set dstaddr6 <name1>, <name2>, ...
set service <name1>, <name2>, ...
set internet-service-name <name1>, <name2>, ...
set internet-service-group <name1>, <name2>, ...
set internet-service-custom <name1>, <name2>, ...
set internet-service-custom-group <name1>, <name2>, ...
set schedule {string}
set users <name1>, <name2>, ...
set groups <name1>, <name2>, ...
set application <id1>, <id2>, ...
set app-category <id1>, <id2>, ...
set app-group <name1>, <name2>, ...
set dstintf <name1>, <name2>, ...
set traffic-shaper {string}
set traffic-shaper-reverse {string}
set per-ip-shaper {string}
set class-id {integer}
set class-id-reverse {integer}
set diffserv-forward [enable|disable]
set diffservcode-forward {user}
set diffserv-reverse [enable|disable]
set diffservcode-rev {user}
next
end

```

config firewall shaping-policy

Parameter	Description	Type	Size	Default
id	Shaping policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
name	Shaping policy name.	string	Maximum length: 35	
comment	Comments.	var-string	Maximum length: 255	
status	Enable/disable traffic shaping policy.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable traffic shaping policy.		
	<i>disable</i>	Disable traffic shaping policy.		
ip-version	IP version.	option	-	4

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>4</td><td>Use IPv4 addressing for Configuration Method.</td></tr><tr><td>6</td><td>Use IPv6 addressing for Configuration Method.</td></tr></table>	Option	Description	4	Use IPv4 addressing for Configuration Method.	6	Use IPv6 addressing for Configuration Method.			
	Option	Description								
	4	Use IPv4 addressing for Configuration Method.								
6	Use IPv6 addressing for Configuration Method.									
service-type	Select service-type: service / internet-service.	option	-	service						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>service</td><td>Firewall services.</td></tr><tr><td>internet-service</td><td>Internet-services.</td></tr></table>	Option	Description	service	Firewall services.	internet-service	Internet-services.			
	Option	Description								
	service	Firewall services.								
internet-service	Internet-services.									
srcaddr <name>	Source address. Address name.	string	Maximum length: 79							
dstaddr <name>	Destination address. Address name.	string	Maximum length: 79							
srcaddr6 <name>	IPv6 source address. Address name.	string	Maximum length: 79							
dstaddr6 <name>	IPv6 destination address. Address name.	string	Maximum length: 79							
service <name>	Service name. Service name.	string	Maximum length: 79							
internet- service-name <name>	Internet Service ID. Internet Service name.	string	Maximum length: 79							
internet- service-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79							
internet- service-custom <name>	Custom Internet Service name. Custom Internet Service name.	string	Maximum length: 79							
internet- service- custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79							
schedule	Schedule name.	string	Maximum length: 35	always						
users <name>	User name. User name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default
groups <name>	User authentication groups. Group name.	string	Maximum length: 79	
application <id>	IDs of one or more applications that this shaper applies application control traffic shaping to. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
app-category <id>	IDs of one or more application categories that this shaper applies application control traffic shaping to. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
app-group <name>	One or more application group names. Application group name.	string	Maximum length: 79	
dstintf <name>	Destination interface list. Interface name.	string	Maximum length: 79	
traffic-shaper	Forward traffic shaper.	string	Maximum length: 35	
traffic-shaper- reverse	Reverse traffic shaper.	string	Maximum length: 35	
per-ip-shaper	Per IP shaper.	string	Maximum length: 35	
class-id	Forward class id.	integer	Minimum value: 2 Maximum value: 31	0
class-id- reverse	Reverse class id.	integer	Minimum value: 2 Maximum value: 31	0
diffserv- forward	Enable/disable forward (original) traffic DiffServ.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
diffservcode- forward	Forward (original) traffic DiffServ code point value.	user	Not Specified	

Parameter	Description	Type	Size	Default						
diffserv-reverse	Enable/disable reverse (reply) traffic DiffServ.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
diffservcode-rev	Reverse (reply) traffic DiffServ code point value.	user	Not Specified							

config firewall shaping-profile

Configure shaping profiles.

```
config firewall shaping-profile
  Description: Configure shaping profiles.
  edit <profile-name>
    set comment {var-string}
    set default-class {integer}
    config classes
      Description: Define shaping classes of this shaping profile
      edit <name>
        set class-id {integer}
        set priority [top|critical|...]
        set guaranteed-bandwidth {integer}
        set maximum-bandwidth {integer}
      next
    end
  next
end
```

config firewall shaping-profile

Parameter	Description	Type	Size	Default
profile-name	Shaping profile name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 1023	
default-class	Default class ID to handle unclassified packets.	integer	Minimum value: 2 Maximum value: 32	2

config classes

Parameter	Description	Type	Size	Default
name	Class Name.	string	Maximum length: 35	
class-id	Class ID.	integer	Minimum value: 2 Maximum value: 32	0
priority	Priority.	option	-	top
	Option	Description		
	<i>top</i>	Top priority.		
	<i>critical</i>	Critical priority.		
	<i>high</i>	High priority.		
	<i>medium</i>	Medium priority.		
	<i>low</i>	Low priority.		
guaranteed-bandwidth	Guaranteed bandwidth in percentage.	integer	Minimum value: 0 Maximum value: 100	0
maximum-bandwidth	Maximum bandwidth in percentage.	integer	Minimum value: 1 Maximum value: 100	1

config firewall sniffer

Configure sniffer.

```
config firewall sniffer
  Description: Configure sniffer.
  edit <id>
    set uuid {uuid}
    set status [enable|disable]
    set logtraffic [all|utm|...]
    set non-ip [enable|disable]
    set interface {string}
    set host {string}
    set port {string}
    set protocol {string}
    set vlan {string}
```

```

next
end

```

config firewall sniffer

Parameter	Description	Type	Size	Default								
id	Sniffer ID.	integer	Minimum value: 0 Maximum value: 9999	0								
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000								
status	Enable/disable the active status of the sniffer.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer status.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer status.</td></tr></table>				Option	Description	<i>enable</i>	Enable sniffer status.	<i>disable</i>	Disable sniffer status.		
	Option	Description										
	<i>enable</i>	Enable sniffer status.										
<i>disable</i>	Disable sniffer status.											
logtraffic	Either log all sessions, only sessions that have a security profile applied, or disable all logging for this policy.	option	-	utm								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Log all sessions accepted or denied by this policy.</td></tr><tr><td><i>utm</i></td><td>Log traffic that has a security profile applied to it.</td></tr><tr><td><i>disable</i></td><td>Disable all logging for this policy.</td></tr></table>				Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.
	Option	Description										
	<i>all</i>	Log all sessions accepted or denied by this policy.										
	<i>utm</i>	Log traffic that has a security profile applied to it.										
<i>disable</i>	Disable all logging for this policy.											
non-ip	Enable/disable sniffing non-IP packets.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer for non-IP packets.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer for non-IP packets.</td></tr></table>				Option	Description	<i>enable</i>	Enable sniffer for non-IP packets.	<i>disable</i>	Disable sniffer for non-IP packets.		
	Option	Description										
	<i>enable</i>	Enable sniffer for non-IP packets.										
<i>disable</i>	Disable sniffer for non-IP packets.											
interface	Interface name that traffic sniffing will take place on.	string	Maximum length: 35									
host	Hosts to filter for in sniffer traffic.	string	Maximum length: 63									
port	Ports to sniff.	string	Maximum length: 63									

Parameter	Description	Type	Size	Default
protocol	Integer value for the protocol type as defined by IANA.	string	Maximum length: 63	
vlan	List of VLANs to sniff.	string	Maximum length: 63	

config firewall ssh host-key

SSH proxy host public keys.

```
config firewall ssh host-key
  Description: SSH proxy host public keys.
  edit <name>
    set status [trusted|revoked]
    set type [RSA|DSA|...]
    set nid [256|384|...]
    set usage [transparent-proxy|access-proxy]
    set ip {ipv4-address-any}
    set port {integer}
    set hostname {string}
    set public-key {var-string}
  next
end
```

config firewall ssh host-key

Parameter	Description	Type	Size	Default								
name	SSH public key name.	string	Maximum length: 35									
status	Set the trust status of the public key.	option	-	trusted								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>trusted</i></td><td>The public key is trusted.</td></tr><tr><td><i>revoked</i></td><td>The public key is revoked.</td></tr></table>				Option	Description	<i>trusted</i>	The public key is trusted.	<i>revoked</i>	The public key is revoked.		
	Option	Description										
	<i>trusted</i>	The public key is trusted.										
<i>revoked</i>	The public key is revoked.											
type	Set the type of the public key.	option	-	RSA								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>RSA</i></td><td>The type of the public key is RSA.</td></tr><tr><td><i>DSA</i></td><td>The type of the public key is DSA.</td></tr><tr><td><i>ECDSA</i></td><td>The type of the public key is ECDSA.</td></tr></table>				Option	Description	<i>RSA</i>	The type of the public key is RSA.	<i>DSA</i>	The type of the public key is DSA.	<i>ECDSA</i>	The type of the public key is ECDSA.
	Option	Description										
	<i>RSA</i>	The type of the public key is RSA.										
	<i>DSA</i>	The type of the public key is DSA.										
<i>ECDSA</i>	The type of the public key is ECDSA.											

Parameter	Description	Type	Size	Default													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ED25519</i></td><td>The type of the public key is ED25519.</td></tr><tr><td><i>RSA-CA</i></td><td>The type of the public key is from RSA CA.</td></tr><tr><td><i>DSA-CA</i></td><td>The type of the public key is from DSA CA.</td></tr><tr><td><i>ECDSA-CA</i></td><td>The type of the public key is from ECDSA CA.</td></tr><tr><td><i>ED25519-CA</i></td><td>The type of the public key is from ED25519 CA.</td></tr></table>		Option	Description	<i>ED25519</i>	The type of the public key is ED25519.	<i>RSA-CA</i>	The type of the public key is from RSA CA.	<i>DSA-CA</i>	The type of the public key is from DSA CA.	<i>ECDSA-CA</i>	The type of the public key is from ECDSA CA.	<i>ED25519-CA</i>	The type of the public key is from ED25519 CA.			
	Option	Description															
	<i>ED25519</i>	The type of the public key is ED25519.															
	<i>RSA-CA</i>	The type of the public key is from RSA CA.															
	<i>DSA-CA</i>	The type of the public key is from DSA CA.															
	<i>ECDSA-CA</i>	The type of the public key is from ECDSA CA.															
	<i>ED25519-CA</i>	The type of the public key is from ED25519 CA.															
nid	Set the nid of the ECDSA key.	option	-	256													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>256</i></td><td>The NID is ecdsa-sha2-nistp256.</td></tr><tr><td><i>384</i></td><td>The NID is ecdsa-sha2-nistp384.</td></tr><tr><td><i>521</i></td><td>The NID is ecdsa-sha2-nistp521.</td></tr></table>		Option	Description	<i>256</i>	The NID is ecdsa-sha2-nistp256.	<i>384</i>	The NID is ecdsa-sha2-nistp384.	<i>521</i>	The NID is ecdsa-sha2-nistp521.							
	Option	Description															
	<i>256</i>	The NID is ecdsa-sha2-nistp256.															
	<i>384</i>	The NID is ecdsa-sha2-nistp384.															
	<i>521</i>	The NID is ecdsa-sha2-nistp521.															
usage	Usage for this public key.	option	-	transparent-proxy													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>transparent-proxy</i></td><td>Transparent proxy uses this public key to validate server.</td></tr><tr><td><i>access-proxy</i></td><td>Access proxy uses this public key to validate server.</td></tr></table>		Option	Description	<i>transparent-proxy</i>	Transparent proxy uses this public key to validate server.	<i>access-proxy</i>	Access proxy uses this public key to validate server.									
	Option	Description															
	<i>transparent-proxy</i>	Transparent proxy uses this public key to validate server.															
<i>access-proxy</i>	Access proxy uses this public key to validate server.																
ip	IP address of the SSH server.	ipv4-address-any	Not Specified	0.0.0.0													
port	Port of the SSH server.	integer	Minimum value: 0 Maximum value: 4294967295	22													
hostname	Hostname of the SSH server to match SSH certificate principals.	string	Maximum length: 255														
public-key	SSH public key.	var-string	Maximum length: 32768														

config firewall ssh local-ca

SSH proxy local CA.

```

config firewall ssh local-ca
  Description: SSH proxy local CA.
  edit <name>
    set password {password}
    set private-key {user}
    set public-key {user}
    set source [built-in|user]
  next
end

```

config firewall ssh local-ca

Parameter	Description	Type	Size	Default
name	SSH proxy local CA name.	string	Maximum length: 35	
password	Password for SSH private key.	password	Not Specified	
private-key	SSH proxy private key, encrypted with a password.	user	Not Specified	
public-key	SSH proxy public key.	user	Not Specified	
source	SSH proxy local CA source type.	option	-	user
	Option	Description		
	<i>built-in</i>	Built-in SSH proxy local keys.		
	<i>user</i>	User imported SSH proxy local keys.		

config firewall ssh local-key

SSH proxy local keys.

```

config firewall ssh local-key
  Description: SSH proxy local keys.
  edit <name>
    set password {password}
    set private-key {user}
    set public-key {user}
    set source [built-in|user]
  next
end

```

config firewall ssh local-key

Parameter	Description	Type	Size	Default
name	SSH proxy local key name.	string	Maximum length: 35	
password	Password for SSH private key.	password	Not Specified	
private-key	SSH proxy private key, encrypted with a password.	user	Not Specified	
public-key	SSH proxy public key.	user	Not Specified	
source	SSH proxy local key source type.	option	-	user
	Option	Description		
	<i>built-in</i>	Built-in SSH proxy local keys.		
	<i>user</i>	User imported SSH proxy local keys.		

config firewall ssh setting

SSH proxy settings.

```
config firewall ssh setting
  Description: SSH proxy settings.
  set caname {string}
  set untrusted-caname {string}
  set hostkey-rsa2048 {string}
  set hostkey-dsa1024 {string}
  set hostkey-ecdsa256 {string}
  set hostkey-ecdsa384 {string}
  set hostkey-ecdsa521 {string}
  set hostkey-ed25519 {string}
  set host-trusted-checking [enable|disable]
end
```

config firewall ssh setting

Parameter	Description	Type	Size	Default
caname	CA certificate used by SSH Inspection.	string	Maximum length: 35	
untrusted-caname	Untrusted CA certificate used by SSH Inspection.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default						
hostkey-rsa2048	RSA certificate used by SSH proxy.	string	Maximum length: 35							
hostkey-dsa1024	DSA certificate used by SSH proxy.	string	Maximum length: 35							
hostkey-ecdsa256	ECDSA nid256 certificate used by SSH proxy.	string	Maximum length: 35							
hostkey-ecdsa384	ECDSA nid384 certificate used by SSH proxy.	string	Maximum length: 35							
hostkey-ecdsa521	ECDSA nid384 certificate used by SSH proxy.	string	Maximum length: 35							
hostkey-ed25519	ED25519 hostkey used by SSH proxy.	string	Maximum length: 35							
host-trusted-checking	Enable/disable host trusted checking.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable host key trusted checking.</td></tr><tr><td><i>disable</i></td><td>Disable host key trusted checking.</td></tr></table>				Option	Description	<i>enable</i>	Enable host key trusted checking.	<i>disable</i>	Disable host key trusted checking.
Option	Description									
<i>enable</i>	Enable host key trusted checking.									
<i>disable</i>	Disable host key trusted checking.									

config firewall ssl-server

Configure SSL servers.

```
config firewall ssl-server
    Description: Configure SSL servers.
    edit <name>
        set ip {ipv4-address-any}
        set port {integer}
        set ssl-mode [half|full]
        set add-header-x-forwarded-proto [enable|disable]
        set mapped-port {integer}
        set ssl-cert <name1>, <name2>, ...
        set ssl-dh-bits [768|1024|...]
        set ssl-algorithm [high|medium|...]
        set ssl-client-renegotiation [allow|deny|...]
        set ssl-min-version [tls-1.0|tls-1.1|...]
        set ssl-max-version [tls-1.0|tls-1.1|...]
        set ssl-send-empty-frags [enable|disable]
        set url-rewrite [enable|disable]
    next
end
```


config firewall ssl-server

Parameter	Description	Type	Size	Default								
name	Server name.	string	Maximum length: 35									
ip	IPv4 address of the SSL server.	ipv4-address-any	Not Specified	0.0.0.0								
port	Server service port.	integer	Minimum value: 1 Maximum value: 65535	443								
ssl-mode	SSL/TLS mode for encryption and decryption of traffic.	option	-	full								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>half</td><td>Client to FortiProxy SSL.</td></tr><tr><td>full</td><td>Client to FortiProxy and FortiProxy to Server SSL.</td></tr></table>				Option	Description	half	Client to FortiProxy SSL.	full	Client to FortiProxy and FortiProxy to Server SSL.		
Option	Description											
half	Client to FortiProxy SSL.											
full	Client to FortiProxy and FortiProxy to Server SSL.											
add-header-x-forwarded-proto	Enable/disable adding an X-Forwarded-Proto header to forwarded requests.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Add X-Forwarded-Proto header.</td></tr><tr><td>disable</td><td>Do not add X-Forwarded-Proto header.</td></tr></table>				Option	Description	enable	Add X-Forwarded-Proto header.	disable	Do not add X-Forwarded-Proto header.		
Option	Description											
enable	Add X-Forwarded-Proto header.											
disable	Do not add X-Forwarded-Proto header.											
mapped-port	Mapped server service port.	integer	Minimum value: 1 Maximum value: 65535	80								
ssl-cert <name>	List of certificate names to use for SSL connections to this server. (default = "Fortinet_SSL"). Certificate list.	string	Maximum length: 79									
ssl-dh-bits	Bit-size of Diffie-Hellman.	option	-	2048								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>768</td><td>768-bit Diffie-Hellman prime.</td></tr><tr><td>1024</td><td>1024-bit Diffie-Hellman prime.</td></tr><tr><td>1536</td><td>1536-bit Diffie-Hellman prime.</td></tr></table>				Option	Description	768	768-bit Diffie-Hellman prime.	1024	1024-bit Diffie-Hellman prime.	1536	1536-bit Diffie-Hellman prime.
Option	Description											
768	768-bit Diffie-Hellman prime.											
1024	1024-bit Diffie-Hellman prime.											
1536	1536-bit Diffie-Hellman prime.											

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>2048</td><td>2048-bit Diffie-Hellman prime.</td></tr></table>	Option	Description	2048	2048-bit Diffie-Hellman prime.									
	Option	Description												
2048	2048-bit Diffie-Hellman prime.													
ssl-algorithm	Relative strength of encryption algorithms accepted in negotiation.	option	-	high										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high</td><td>High encryption. Allow only AES and ChaCha</td></tr><tr><td>medium</td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td>low</td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr></table>	Option	Description	high	High encryption. Allow only AES and ChaCha	medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.					
	Option	Description												
	high	High encryption. Allow only AES and ChaCha												
	medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.												
low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.													
ssl-client-renegotiation	Allow or block client renegotiation by server.	option	-	allow										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow a SSL client to renegotiate.</td></tr><tr><td>deny</td><td>Abort any SSL connection that attempts to renegotiate.</td></tr><tr><td>secure</td><td>Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.</td></tr></table>	Option	Description	allow	Allow a SSL client to renegotiate.	deny	Abort any SSL connection that attempts to renegotiate.	secure	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.					
	Option	Description												
	allow	Allow a SSL client to renegotiate.												
	deny	Abort any SSL connection that attempts to renegotiate.												
secure	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.													
ssl-min-version	Lowest SSL/TLS version to negotiate.	option	-	tls-1.1										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tls-1.0</td><td>TLS 1.0.</td></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr><tr><td>tls-1.2</td><td>TLS 1.2.</td></tr><tr><td>tls-1.3</td><td>TLS 1.3.</td></tr></table>	Option	Description	tls-1.0	TLS 1.0.	tls-1.1	TLS 1.1.	tls-1.2	TLS 1.2.	tls-1.3	TLS 1.3.			
	Option	Description												
	tls-1.0	TLS 1.0.												
	tls-1.1	TLS 1.1.												
	tls-1.2	TLS 1.2.												
tls-1.3	TLS 1.3.													
ssl-max-version	Highest SSL/TLS version to negotiate.	option	-	tls-1.3										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tls-1.0</td><td>TLS 1.0.</td></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr><tr><td>tls-1.2</td><td>TLS 1.2.</td></tr><tr><td>tls-1.3</td><td>TLS 1.3.</td></tr></table>	Option	Description	tls-1.0	TLS 1.0.	tls-1.1	TLS 1.1.	tls-1.2	TLS 1.2.	tls-1.3	TLS 1.3.			
	Option	Description												
	tls-1.0	TLS 1.0.												
	tls-1.1	TLS 1.1.												
	tls-1.2	TLS 1.2.												
tls-1.3	TLS 1.3.													
ssl-send-empty-frags	Enable/disable sending empty fragments to avoid attack on CBC IV.	option	-	enable										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Send empty fragments.		
	<i>disable</i>	Do not send empty fragments.		
url-rewrite	Enable/disable rewriting the URL.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config firewall ssl-ssh-profile

Configure SSL/SSH protocol options.

```
config firewall ssl-ssh-profile
  Description: Configure SSL/SSH protocol options.
  edit <name>
    set comment {var-string}
    config ssl
      Description: Configure SSL options.
      set inspect-all [disable|certificate-inspection|...]
      set client-certificate [bypass|inspect|...]
      set unsupported-ssl-version [allow|block]
      set unsupported-ssl-cipher [allow|block]
      set unsupported-ssl-negotiation [allow|block]
      set expired-server-cert [allow|block|...]
      set revoked-server-cert [allow|block|...]
      set untrusted-server-cert [allow|block|...]
      set cert-validation-timeout [allow|block|...]
      set cert-validation-failure [allow|block|...]
      set sni-server-cert-check [enable|strict|...]
      set cert-probe-failure [allow|block]
      set encrypted-client-hello [allow|block]
      set min-allowed-ssl-version [ssl-3.0|tls-1.0|...]
    end
    config https
      Description: Configure HTTPS options.
      set ports {integer}
      set status [disable|certificate-inspection|...]
      set quic [inspect|bypass|...]
      set proxy-after-tcp-handshake [enable|disable]
      set client-certificate [bypass|inspect|...]
      set unsupported-ssl-version [allow|block]
      set unsupported-ssl-cipher [allow|block]
      set unsupported-ssl-negotiation [allow|block]
      set expired-server-cert [allow|block|...]
      set revoked-server-cert [allow|block|...]
```

```
    set untrusted-server-cert [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set cert-validation-failure [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
    set cert-probe-failure [allow|block]
    set encrypted-client-hello [allow|block]
    set min-allowed-ssl-version [ssl-3.0|tls-1.0|...]
end
config ftps
    Description: Configure FTPS options.
    set ports {integer}
    set status [disable|deep-inspection]
    set client-certificate [bypass|inspect|...]
    set unsupported-ssl-version [allow|block]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set expired-server-cert [allow|block|...]
    set revoked-server-cert [allow|block|...]
    set untrusted-server-cert [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set cert-validation-failure [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
    set min-allowed-ssl-version [ssl-3.0|tls-1.0|...]
end
config imaps
    Description: Configure IMAPS options.
    set ports {integer}
    set status [disable|deep-inspection]
    set proxy-after-tcp-handshake [enable|disable]
    set client-certificate [bypass|inspect|...]
    set unsupported-ssl-version [allow|block]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set expired-server-cert [allow|block|...]
    set revoked-server-cert [allow|block|...]
    set untrusted-server-cert [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set cert-validation-failure [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
end
config pop3s
    Description: Configure POP3S options.
    set ports {integer}
    set status [disable|deep-inspection]
    set proxy-after-tcp-handshake [enable|disable]
    set client-certificate [bypass|inspect|...]
    set unsupported-ssl-version [allow|block]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set expired-server-cert [allow|block|...]
    set revoked-server-cert [allow|block|...]
    set untrusted-server-cert [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set cert-validation-failure [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
end
```

```
config smtps
    Description: Configure SMTPS options.
    set ports {integer}
    set status [disable|deep-inspection]
    set proxy-after-tcp-handshake [enable|disable]
    set client-certificate [bypass|inspect|...]
    set unsupported-ssl-version [allow|block]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set expired-server-cert [allow|block|...]
    set revoked-server-cert [allow|block|...]
    set untrusted-server-cert [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set cert-validation-failure [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
end
config ssh
    Description: Configure SSH options.
    set ports {integer}
    set status [disable|deep-inspection]
    set proxy-after-tcp-handshake [enable|disable]
    set unsupported-version [bypass|block]
    set ssh-tun-policy-check [disable|enable]
    set ssh-algorithm [compatible|high-encryption]
end
config dot
    Description: Configure DNS over TLS options.
    set status [disable|deep-inspection]
    set quic [inspect|bypass|...]
    set proxy-after-tcp-handshake [enable|disable]
    set client-certificate [bypass|inspect|...]
    set unsupported-ssl-version [allow|block]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set expired-server-cert [allow|block|...]
    set revoked-server-cert [allow|block|...]
    set untrusted-server-cert [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set cert-validation-failure [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
end
config ssl-client-certificate
    Description: Configure SSL client certificate setting.
    set status [do-not-offer|keyring-list|...]
    set keyring-list {string}
    set caname {string}
    set cert {string}
end
config ssl-exempt
    Description: Servers to exempt from SSL inspection.
    edit <id>
        set type [fortiguard-category|address|...]
        set fortiguard-category {integer}
        set address {string}
        set address6 {string}
        set wildcard-fqdn {string}
```

```

        set regex {string}
        set finger-print-category [unknown|firefox|...]
    next
end
config ech-outer-sni
    Description: ClientHelloOuter SNIs to be blocked.
    edit <name>
        set sni {string}
    next
end
set allowlist [enable|disable]
set block-blocklisted-certificates [disable|enable]
set server-cert-mode [re-sign|replace]
set use-ssl-server [disable|enable]
set caname {string}
set untrusted-caname {string}
set server-cert <name1>, <name2>, ...
config ssl-server
    Description: SSL server settings used for client certificate request.
    edit <id>
        set ip {ipv4-address-any}
        set https-client-certificate [bypass|inspect|...]
        set smtps-client-certificate [bypass|inspect|...]
        set pop3s-client-certificate [bypass|inspect|...]
        set imaps-client-certificate [bypass|inspect|...]
        set ftps-client-certificate [bypass|inspect|...]
        set ssl-other-client-certificate [bypass|inspect|...]
    next
end
set ssl-exemption-ip-rating [enable|disable]
set ssl-exemption-log [disable|enable]
set ssl-anomaly-log [disable|enable]
set ssl-negotiation-log [disable|enable]
set ssl-server-cert-log [disable|enable]
set ssl-handshake-log [disable|enable]
set rpc-over-https [enable|disable]
set mapi-over-https [enable|disable]
set supported-alpn [http1-1|http2|...]
next
end

```

config firewall ssl-ssh-profile

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
comment	Optional comments.	var-string	Maximum length: 255	
allowlist	Enable/disable exempting servers by FortiGuard allowlist.	option	-	disable

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
block-blocklisted-certificates	Enable/disable blocking SSL-based botnet communication by FortiGuard certificate blacklist.	option	-	enable
	Option Description			
	<i>disable</i>	Disable FortiGuard certificate blacklist.		
	<i>enable</i>	Enable FortiGuard certificate blacklist.		
server-cert-mode	Re-sign or replace the server's certificate.	option	-	re-sign
	Option Description			
	<i>re-sign</i>	Multiple clients connecting to multiple servers.		
	<i>replace</i>	Protect an SSL server.		
use-ssl-server	Enable/disable the use of SSL server table for SSL offloading.	option	-	disable
	Option Description			
	<i>disable</i>	Don't use SSL server configuration.		
	<i>enable</i>	Use SSL server configuration.		
caname	CA certificate used by SSL Inspection.	string	Maximum length: 35	default-ca
untrusted-caname	Untrusted CA certificate used by SSL Inspection.	string	Maximum length: 35	default-untrusted-ca
server-cert <name>	Certificate used by SSL Inspection to replace server certificate. Certificate list.	string	Maximum length: 79	
ssl-exemption-ip-rating	Enable/disable IP based URL rating.	option	-	enable
	Option Description			
	<i>enable</i>	Enable IP based URL rating.		
	<i>disable</i>	Disable IP based URL rating.		

Parameter	Description	Type	Size	Default						
ssl-exemption-log	Enable/disable logging SSL exemptions.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging SSL exemptions.</td></tr><tr><td><i>enable</i></td><td>Enable logging SSL exemptions.</td></tr></table>	Option	Description	<i>disable</i>	Disable logging SSL exemptions.	<i>enable</i>	Enable logging SSL exemptions.			
Option	Description									
<i>disable</i>	Disable logging SSL exemptions.									
<i>enable</i>	Enable logging SSL exemptions.									
ssl-anomaly-log	Enable/disable logging of SSL anomalies.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging of SSL anomalies.</td></tr><tr><td><i>enable</i></td><td>Enable logging of SSL anomalies.</td></tr></table>	Option	Description	<i>disable</i>	Disable logging of SSL anomalies.	<i>enable</i>	Enable logging of SSL anomalies.			
Option	Description									
<i>disable</i>	Disable logging of SSL anomalies.									
<i>enable</i>	Enable logging of SSL anomalies.									
ssl-negotiation-log	Enable/disable logging SSL negotiation.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging SSL negotiation.</td></tr><tr><td><i>enable</i></td><td>Enable logging SSL negotiation.</td></tr></table>	Option	Description	<i>disable</i>	Disable logging SSL negotiation.	<i>enable</i>	Enable logging SSL negotiation.			
Option	Description									
<i>disable</i>	Disable logging SSL negotiation.									
<i>enable</i>	Enable logging SSL negotiation.									
ssl-server-cert-log	Enable/disable logging of server certificate information.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging server certificate.</td></tr><tr><td><i>enable</i></td><td>Enable logging server certificate.</td></tr></table>	Option	Description	<i>disable</i>	Disable logging server certificate.	<i>enable</i>	Enable logging server certificate.			
Option	Description									
<i>disable</i>	Disable logging server certificate.									
<i>enable</i>	Enable logging server certificate.									
ssl-handshake-log	Enable/disable logging of TLS handshakes.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging TLS handshakes.</td></tr><tr><td><i>enable</i></td><td>Enable logging TLS handshakes.</td></tr></table>	Option	Description	<i>disable</i>	Disable logging TLS handshakes.	<i>enable</i>	Enable logging TLS handshakes.			
Option	Description									
<i>disable</i>	Disable logging TLS handshakes.									
<i>enable</i>	Enable logging TLS handshakes.									
rpc-over-https	Enable/disable inspection of RPC over HTTPS.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable inspection of RPC over HTTPS.</td></tr></table>	Option	Description	<i>enable</i>	Enable inspection of RPC over HTTPS.					
Option	Description									
<i>enable</i>	Enable inspection of RPC over HTTPS.									

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable inspection of RPC over HTTPS.</td></tr></table>	Option	Description	<i>disable</i>	Disable inspection of RPC over HTTPS.									
	Option	Description												
<i>disable</i>	Disable inspection of RPC over HTTPS.													
mapi-over-https	Enable/disable inspection of MAPI over HTTPS.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable inspection of MAPI over HTTPS.</td></tr><tr><td><i>disable</i></td><td>Disable inspection of MAPI over HTTPS.</td></tr></table>	Option	Description	<i>enable</i>	Enable inspection of MAPI over HTTPS.	<i>disable</i>	Disable inspection of MAPI over HTTPS.							
	Option	Description												
	<i>enable</i>	Enable inspection of MAPI over HTTPS.												
<i>disable</i>	Disable inspection of MAPI over HTTPS.													
supported-alpn	Configure ALPN option.	option	-	all										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http1-1</i></td><td>Enable all ALPN including HTTP1.1 except HTTP2 and SPDY.</td></tr><tr><td><i>http2</i></td><td>Enable all ALPN including HTTP2 except HTTP1.1 and SPDY.</td></tr><tr><td><i>all</i></td><td>Allow all ALPN extensions except SPDY.</td></tr><tr><td><i>none</i></td><td>Do not use ALPN.</td></tr></table>	Option	Description	<i>http1-1</i>	Enable all ALPN including HTTP1.1 except HTTP2 and SPDY.	<i>http2</i>	Enable all ALPN including HTTP2 except HTTP1.1 and SPDY.	<i>all</i>	Allow all ALPN extensions except SPDY.	<i>none</i>	Do not use ALPN.			
	Option	Description												
	<i>http1-1</i>	Enable all ALPN including HTTP1.1 except HTTP2 and SPDY.												
	<i>http2</i>	Enable all ALPN including HTTP2 except HTTP1.1 and SPDY.												
	<i>all</i>	Allow all ALPN extensions except SPDY.												
<i>none</i>	Do not use ALPN.													

config ssl

Parameter	Description	Type	Size	Default
inspect-all	Level of SSL inspection.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>certificate-inspection</i>	Inspect SSL handshake only.		
	<i>deep-inspection</i>	Full SSL inspection.		
client-certificate	Action based on received client certificate.	option	-	bypass
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
	<i>bypass-on-cert-req</i>	Bypass on certificate request.		

Parameter	Description	Type	Size	Default								
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the version is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the version is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the version is not supported.	<i>block</i>	Block the session when the version is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the version is not supported.											
<i>block</i>	Block the session when the version is not supported.											
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the cipher is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the cipher is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the cipher is not supported.											
<i>block</i>	Block the session when the cipher is not supported.											
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the negotiation is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the negotiation is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the negotiation is not supported.											
<i>block</i>	Block the session when the negotiation is not supported.											
expired-server-cert	Action based on server certificate is expired.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
cert-validation-failure	Action based on certificate validation failure.	option	-	block
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable
	Option	Description		
	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.		
	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.		
	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.		
cert-probe-failure	Action based on certificate probe failure.	option	-	block
	Option	Description		
	<i>allow</i>	Bypass the session when unable to retrieve server's certificate for inspection.		
	<i>block</i>	Block the session when unable to retrieve server's certificate for inspection.		

Parameter	Description	Type	Size	Default												
encrypted-client-hello	Block/allow session based on existence of encrypted-client-hello.	option	-	block												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Pass the session when encrypted-client-hello exists.</td></tr><tr><td><i>block</i></td><td>Block the session when encrypted-client-hello exists.</td></tr></table>	Option	Description	<i>allow</i>	Pass the session when encrypted-client-hello exists.	<i>block</i>	Block the session when encrypted-client-hello exists.									
Option	Description															
<i>allow</i>	Pass the session when encrypted-client-hello exists.															
<i>block</i>	Block the session when encrypted-client-hello exists.															
min-allowed-ssl-version	Minimum SSL version to be allowed.	option	-	tls-1.1												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
Option	Description															
<i>ssl-3.0</i>	SSL 3.0.															
<i>tls-1.0</i>	TLS 1.0.															
<i>tls-1.1</i>	TLS 1.1.															
<i>tls-1.2</i>	TLS 1.2.															
<i>tls-1.3</i>	TLS 1.3.															

config https

Parameter	Description	Type	Size	Default								
ports	Ports to use for scanning.	integer	Minimum value: 1 Maximum value: 65535									
status	Configure protocol inspection status.	option	-	deep-inspection								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>certificate-inspection</i></td><td>Inspect SSL handshake only.</td></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>certificate-inspection</i>	Inspect SSL handshake only.	<i>deep-inspection</i>	Full SSL inspection.			
Option	Description											
<i>disable</i>	Disable.											
<i>certificate-inspection</i>	Inspect SSL handshake only.											
<i>deep-inspection</i>	Full SSL inspection.											
quic	QUIC inspection status.	option	-	inspect								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>inspect</i></td><td>Inspect QUIC traffic.</td></tr></table>	Option	Description	<i>inspect</i>	Inspect QUIC traffic.							
Option	Description											
<i>inspect</i>	Inspect QUIC traffic.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>bypass</i>	Bypass QUIC traffic.		
	<i>block</i>	Block QUIC traffic.		
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
client-certificate	Action based on received client certificate.	option	-	bypass
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
	<i>bypass-on-cert-req</i>	Bypass on certificate request.		
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block
	Option	Description		
	<i>allow</i>	Bypass the session when the version is not supported.		
	<i>block</i>	Block the session when the version is not supported.		
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow
	Option	Description		
	<i>allow</i>	Bypass the session when the cipher is not supported.		
	<i>block</i>	Block the session when the cipher is not supported.		
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow
	Option	Description		
	<i>allow</i>	Bypass the session when the negotiation is not supported.		
	<i>block</i>	Block the session when the negotiation is not supported.		

Parameter	Description	Type	Size	Default								
expired-server-cert	Action based on server certificate is expired.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-failure	Action based on certificate validation failure.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											

Parameter	Description	Type	Size	Default												
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td></tr><tr><td><i>strict</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td></tr><tr><td><i>disable</i></td><td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td></tr></table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.							
Option	Description															
<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.															
<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.															
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.															
cert-probe-failure	Action based on certificate probe failure.	option	-	block												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when unable to retrieve server's certificate for inspection.</td></tr><tr><td><i>block</i></td><td>Block the session when unable to retrieve server's certificate for inspection.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when unable to retrieve server's certificate for inspection.	<i>block</i>	Block the session when unable to retrieve server's certificate for inspection.									
Option	Description															
<i>allow</i>	Bypass the session when unable to retrieve server's certificate for inspection.															
<i>block</i>	Block the session when unable to retrieve server's certificate for inspection.															
encrypted-client-hello	Block/allow session based on existence of encrypted-client-hello.	option	-	block												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Pass the session when encrypted-client-hello exists.</td></tr><tr><td><i>block</i></td><td>Block the session when encrypted-client-hello exists.</td></tr></table>	Option	Description	<i>allow</i>	Pass the session when encrypted-client-hello exists.	<i>block</i>	Block the session when encrypted-client-hello exists.									
Option	Description															
<i>allow</i>	Pass the session when encrypted-client-hello exists.															
<i>block</i>	Block the session when encrypted-client-hello exists.															
min-allowed-ssl-version	Minimum SSL version to be allowed.	option	-	tls-1.1												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
Option	Description															
<i>ssl-3.0</i>	SSL 3.0.															
<i>tls-1.0</i>	TLS 1.0.															
<i>tls-1.1</i>	TLS 1.1.															
<i>tls-1.2</i>	TLS 1.2.															
<i>tls-1.3</i>	TLS 1.3.															

config ftps

Parameter	Description	Type	Size	Default										
ports	Ports to use for scanning.	integer	Minimum value: 1 Maximum value: 65535											
status	Configure protocol inspection status.	option	-	deep-inspection										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.							
Option	Description													
<i>disable</i>	Disable.													
<i>deep-inspection</i>	Full SSL inspection.													
client-certificate	Action based on received client certificate.	option	-	bypass										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass the session.</td></tr><tr><td><i>inspect</i></td><td>Inspect the session.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>bypass-on-cert-req</i></td><td>Bypass on certificate request.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.	<i>bypass-on-cert-req</i>	Bypass on certificate request.			
Option	Description													
<i>bypass</i>	Bypass the session.													
<i>inspect</i>	Inspect the session.													
<i>block</i>	Block the session.													
<i>bypass-on-cert-req</i>	Bypass on certificate request.													
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the version is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the version is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the version is not supported.	<i>block</i>	Block the session when the version is not supported.							
Option	Description													
<i>allow</i>	Bypass the session when the version is not supported.													
<i>block</i>	Block the session when the version is not supported.													
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the cipher is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the cipher is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.							
Option	Description													
<i>allow</i>	Bypass the session when the cipher is not supported.													
<i>block</i>	Block the session when the cipher is not supported.													
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow										

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the negotiation is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the negotiation is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
	Option	Description										
	<i>allow</i>	Bypass the session when the negotiation is not supported.										
<i>block</i>	Block the session when the negotiation is not supported.											
expired-server-cert	Action based on server certificate is expired.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
	Option	Description										
	<i>allow</i>	Allow the server certificate.										
	<i>block</i>	Block the session.										
<i>ignore</i>	Re-sign the server certificate as trusted.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
	Option	Description										
	<i>allow</i>	Allow the server certificate.										
	<i>block</i>	Block the session.										
<i>ignore</i>	Re-sign the server certificate as trusted.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
	Option	Description										
	<i>allow</i>	Allow the server certificate.										
	<i>block</i>	Block the session.										
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
	Option	Description										
	<i>allow</i>	Allow the server certificate.										
	<i>block</i>	Block the session.										
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-failure	Action based on certificate validation failure.	option	-	block								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable
	Option	Description		
	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.		
	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.		
	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.		
min-allowed-ssl-version	Minimum SSL version to be allowed.	option	-	tls-1.1
	Option	Description		
	<i>ssl-3.0</i>	SSL 3.0.		
	<i>tls-1.0</i>	TLS 1.0.		
	<i>tls-1.1</i>	TLS 1.1.		
	<i>tls-1.2</i>	TLS 1.2.		
	<i>tls-1.3</i>	TLS 1.3.		

config imaps

Parameter	Description	Type	Size	Default
ports	Ports to use for scanning.	integer	Minimum value: 1 Maximum value: 65535	
status	Configure protocol inspection status.	option	-	deep-inspection

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.							
	Option	Description												
	<i>disable</i>	Disable.												
<i>deep-inspection</i>	Full SSL inspection.													
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
	Option	Description												
	<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.													
client-certificate	Action based on received client certificate.	option	-	inspect										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass the session.</td></tr><tr><td><i>inspect</i></td><td>Inspect the session.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>bypass-on-cert-req</i></td><td>Bypass on certificate request.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.	<i>bypass-on-cert-req</i>	Bypass on certificate request.			
	Option	Description												
	<i>bypass</i>	Bypass the session.												
	<i>inspect</i>	Inspect the session.												
	<i>block</i>	Block the session.												
<i>bypass-on-cert-req</i>	Bypass on certificate request.													
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the version is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the version is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the version is not supported.	<i>block</i>	Block the session when the version is not supported.							
	Option	Description												
	<i>allow</i>	Bypass the session when the version is not supported.												
<i>block</i>	Block the session when the version is not supported.													
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the cipher is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the cipher is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.							
	Option	Description												
	<i>allow</i>	Bypass the session when the cipher is not supported.												
<i>block</i>	Block the session when the cipher is not supported.													
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the negotiation is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the negotiation is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.							
	Option	Description												
	<i>allow</i>	Bypass the session when the negotiation is not supported.												
<i>block</i>	Block the session when the negotiation is not supported.													

Parameter	Description	Type	Size	Default								
expired-server-cert	Action based on server certificate is expired.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow the server certificate.</td></tr><tr><td>block</td><td>Block the session.</td></tr><tr><td>ignore</td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	allow	Allow the server certificate.	block	Block the session.	ignore	Re-sign the server certificate as trusted.			
Option	Description											
allow	Allow the server certificate.											
block	Block the session.											
ignore	Re-sign the server certificate as trusted.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow the server certificate.</td></tr><tr><td>block</td><td>Block the session.</td></tr><tr><td>ignore</td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	allow	Allow the server certificate.	block	Block the session.	ignore	Re-sign the server certificate as trusted.			
Option	Description											
allow	Allow the server certificate.											
block	Block the session.											
ignore	Re-sign the server certificate as trusted.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow the server certificate.</td></tr><tr><td>block</td><td>Block the session.</td></tr><tr><td>ignore</td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	allow	Allow the server certificate.	block	Block the session.	ignore	Re-sign the server certificate as trusted.			
Option	Description											
allow	Allow the server certificate.											
block	Block the session.											
ignore	Re-sign the server certificate as trusted.											
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow the server certificate.</td></tr><tr><td>block</td><td>Block the session.</td></tr><tr><td>ignore</td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	allow	Allow the server certificate.	block	Block the session.	ignore	Re-sign the server certificate as trusted.			
Option	Description											
allow	Allow the server certificate.											
block	Block the session.											
ignore	Re-sign the server certificate as trusted.											
cert-validation-failure	Action based on certificate validation failure.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow the server certificate.</td></tr><tr><td>block</td><td>Block the session.</td></tr><tr><td>ignore</td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	allow	Allow the server certificate.	block	Block the session.	ignore	Re-sign the server certificate as trusted.			
Option	Description											
allow	Allow the server certificate.											
block	Block the session.											
ignore	Re-sign the server certificate as trusted.											

Parameter	Description	Type	Size	Default								
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td></tr><tr><td><i>strict</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td></tr><tr><td><i>disable</i></td><td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td></tr></table>				Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.
Option	Description											
<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.											
<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.											
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											

config pop3s

Parameter	Description	Type	Size	Default						
ports	Ports to use for scanning.	integer	Minimum value: 1 Maximum value: 65535							
status	Configure protocol inspection status.	option	-	deep-inspection						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.			
Option	Description									
<i>disable</i>	Disable.									
<i>deep-inspection</i>	Full SSL inspection.									
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
client-certificate	Action based on received client certificate.	option	-	inspect						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass the session.</td></tr><tr><td><i>inspect</i></td><td>Inspect the session.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.			
Option	Description									
<i>bypass</i>	Bypass the session.									
<i>inspect</i>	Inspect the session.									

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>bypass-on-cert-req</i></td><td>Bypass on certificate request.</td></tr></table>	Option	Description	<i>block</i>	Block the session.	<i>bypass-on-cert-req</i>	Bypass on certificate request.					
	Option	Description										
	<i>block</i>	Block the session.										
<i>bypass-on-cert-req</i>	Bypass on certificate request.											
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the version is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the version is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the version is not supported.	<i>block</i>	Block the session when the version is not supported.					
	Option	Description										
	<i>allow</i>	Bypass the session when the version is not supported.										
<i>block</i>	Block the session when the version is not supported.											
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the cipher is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the cipher is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.					
	Option	Description										
	<i>allow</i>	Bypass the session when the cipher is not supported.										
<i>block</i>	Block the session when the cipher is not supported.											
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the negotiation is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the negotiation is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
	Option	Description										
	<i>allow</i>	Bypass the session when the negotiation is not supported.										
<i>block</i>	Block the session when the negotiation is not supported.											
expired-server-cert	Action based on server certificate is expired.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
	Option	Description										
	<i>allow</i>	Allow the server certificate.										
	<i>block</i>	Block the session.										
<i>ignore</i>	Re-sign the server certificate as trusted.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.							
	Option	Description										
<i>allow</i>	Allow the server certificate.											

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.					
	Option	Description										
	<i>block</i>	Block the session.										
<i>ignore</i>	Re-sign the server certificate as trusted.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
	Option	Description										
	<i>allow</i>	Allow the server certificate.										
	<i>block</i>	Block the session.										
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
	Option	Description										
	<i>allow</i>	Allow the server certificate.										
	<i>block</i>	Block the session.										
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-failure	Action based on certificate validation failure.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
	Option	Description										
	<i>allow</i>	Allow the server certificate.										
	<i>block</i>	Block the session.										
<i>ignore</i>	Re-sign the server certificate as trusted.											
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td></tr><tr><td><i>strict</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td></tr><tr><td><i>disable</i></td><td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td></tr></table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
	Option	Description										
	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.										
<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.											
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											

config smtps

Parameter	Description	Type	Size	Default										
ports	Ports to use for scanning.	integer	Minimum value: 1 Maximum value: 65535											
status	Configure protocol inspection status.	option	-	deep-inspection										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.							
Option	Description													
<i>disable</i>	Disable.													
<i>deep-inspection</i>	Full SSL inspection.													
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
client-certificate	Action based on received client certificate.	option	-	inspect										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass the session.</td></tr><tr><td><i>inspect</i></td><td>Inspect the session.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>bypass-on-cert-req</i></td><td>Bypass on certificate request.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.	<i>bypass-on-cert-req</i>	Bypass on certificate request.			
Option	Description													
<i>bypass</i>	Bypass the session.													
<i>inspect</i>	Inspect the session.													
<i>block</i>	Block the session.													
<i>bypass-on-cert-req</i>	Bypass on certificate request.													
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the version is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the version is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the version is not supported.	<i>block</i>	Block the session when the version is not supported.							
Option	Description													
<i>allow</i>	Bypass the session when the version is not supported.													
<i>block</i>	Block the session when the version is not supported.													
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow										

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the cipher is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the cipher is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.					
	Option	Description										
	<i>allow</i>	Bypass the session when the cipher is not supported.										
<i>block</i>	Block the session when the cipher is not supported.											
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the negotiation is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the negotiation is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
	Option	Description										
	<i>allow</i>	Bypass the session when the negotiation is not supported.										
<i>block</i>	Block the session when the negotiation is not supported.											
expired-server-cert	Action based on server certificate is expired.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
	Option	Description										
	<i>allow</i>	Allow the server certificate.										
	<i>block</i>	Block the session.										
<i>ignore</i>	Re-sign the server certificate as trusted.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
	Option	Description										
	<i>allow</i>	Allow the server certificate.										
	<i>block</i>	Block the session.										
<i>ignore</i>	Re-sign the server certificate as trusted.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
	Option	Description										
	<i>allow</i>	Allow the server certificate.										
	<i>block</i>	Block the session.										
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
cert-validation-failure	Action based on certificate validation failure.	option	-	block
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable
	Option	Description		
	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.		
	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.		
	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.		

config ssh

Parameter	Description	Type	Size	Default						
ports	Ports to use for scanning.	integer	Minimum value: 1 Maximum value: 65535							
status	Configure protocol inspection status.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>				Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.
Option	Description									
<i>disable</i>	Disable.									
<i>deep-inspection</i>	Full SSL inspection.									

Parameter	Description	Type	Size	Default						
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
unsupported-version	Action based on SSH version being unsupported.	option	-	bypass						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass the session.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>block</i>	Block the session.			
Option	Description									
<i>bypass</i>	Bypass the session.									
<i>block</i>	Block the session.									
ssh-tun-policy-check	Enable/disable SSH tunnel policy check.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SSH tunnel policy check.</td></tr><tr><td><i>enable</i></td><td>Enable SSH tunnel policy check.</td></tr></table>	Option	Description	<i>disable</i>	Disable SSH tunnel policy check.	<i>enable</i>	Enable SSH tunnel policy check.			
Option	Description									
<i>disable</i>	Disable SSH tunnel policy check.									
<i>enable</i>	Enable SSH tunnel policy check.									
ssh-algorithm	Relative strength of encryption algorithms accepted during negotiation.	option	-	compatible						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>compatible</i></td><td>Allow a broader set of encryption algorithms for best compatibility.</td></tr><tr><td><i>high-encryption</i></td><td>Allow only AES-CTR, AES-GCM ciphers and high encryption algorithms.</td></tr></table>	Option	Description	<i>compatible</i>	Allow a broader set of encryption algorithms for best compatibility.	<i>high-encryption</i>	Allow only AES-CTR, AES-GCM ciphers and high encryption algorithms.			
Option	Description									
<i>compatible</i>	Allow a broader set of encryption algorithms for best compatibility.									
<i>high-encryption</i>	Allow only AES-CTR, AES-GCM ciphers and high encryption algorithms.									

config dot

Parameter	Description	Type	Size	Default
status	Configure protocol inspection status.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>deep-inspection</i>	Full SSL inspection.		
quic	QUIC inspection status.	option	-	inspect

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>inspect</i>	Inspect QUIC traffic.		
	<i>bypass</i>	Bypass QUIC traffic.		
	<i>block</i>	Block QUIC traffic.		
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
client-certificate	Action based on received client certificate.	option	-	bypass
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
	<i>bypass-on-cert-req</i>	Bypass on certificate request.		
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block
	Option	Description		
	<i>allow</i>	Bypass the session when the version is not supported.		
	<i>block</i>	Block the session when the version is not supported.		
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow
	Option	Description		
	<i>allow</i>	Bypass the session when the cipher is not supported.		
	<i>block</i>	Block the session when the cipher is not supported.		
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow

Parameter	Description	Type	Size	Default
	Option	Description		
	allow	Bypass the session when the negotiation is not supported.		
	block	Block the session when the negotiation is not supported.		
expired-server-cert	Action based on server certificate is expired.	option	-	block
	Option	Description		
	allow	Allow the server certificate.		
	block	Block the session.		
	ignore	Re-sign the server certificate as trusted.		
revoked-server-cert	Action based on server certificate is revoked.	option	-	block
	Option	Description		
	allow	Allow the server certificate.		
	block	Block the session.		
	ignore	Re-sign the server certificate as trusted.		
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow
	Option	Description		
	allow	Allow the server certificate.		
	block	Block the session.		
	ignore	Re-sign the server certificate as trusted.		
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow
	Option	Description		
	allow	Allow the server certificate.		
	block	Block the session.		
	ignore	Re-sign the server certificate as trusted.		
cert-validation-failure	Action based on certificate validation failure.	option	-	block

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable
	Option	Description		
	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.		
	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.		
	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.		

config ssl-client-certificate

Parameter	Description	Type	Size	Default
status	Configure SSL client certificate status.	option	-	do-not-offer
	Option	Description		
	<i>do-not-offer</i>	Do not offer SSL client certificate.		
	<i>keyring-list</i>	For authenticated users, offer matching SSL client certificate from keyring list.		
	<i>ca-sign</i>	For authenticated users, offer SSL client certificate signed by configured CA.		
	<i>static</i>	Offer static SSL client certificate.		
keyring-list	Keyring list used to find client certificate.	string	Maximum length: 35	
caname	CA certificate used to sign client certificate.	string	Maximum length: 35	Fortinet_CA_SSL
cert	Client certificate.	string	Maximum length: 35	

config ssl-exempt

Parameter	Description	Type	Size	Default
id	ID number.	integer	Minimum value: 0 Maximum value: 512	0
type	Type of address object (IPv4 or IPv6) or FortiGuard category.	option	-	fortiguard-category
	OptionDescription			
	fortiguard-category	FortiGuard category.		
	address	Firewall IPv4 address.		
	address6	Firewall IPv6 address.		
	wildcard-fqdn	Fully Qualified Domain Name with wildcard characters.		
	regex	Regular expression FQDN.		
	finger-print	TLS finger print.		
fortiguard-category	FortiGuard category ID.	integer	Minimum value: 0 Maximum value: 255	0
address	IPv4 address object.	string	Maximum length: 79	
address6	IPv6 address object.	string	Maximum length: 79	
wildcard-fqdn	Exempt servers by wildcard FQDN.	string	Maximum length: 79	
regex	Exempt servers by regular expression.	string	Maximum length: 255	
finger-print-category	Finger print platform.	option	-	android
	OptionDescription			
	unknown	Unknown clients.		
	firefox	Firefox.		
	chrome	Chrome.		
	safari	Safari.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>edge</i>	Edge.		
	<i>ie</i>	Internet Explorer.		
	<i>android</i>	Android applications.		
	<i>ios</i>	iOS applications.		
	<i>windows</i>	Windows applications.		

config ech-outer-sni

Parameter	Description	Type	Size	Default
name	ClientHelloOuter SNI name.	string	Maximum length: 79	
sni	ClientHelloOuter SNI to be blocked.	string	Maximum length: 255	

config ssl-server

Parameter	Description	Type	Size	Default
id	SSL server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	IPv4 address of the SSL server.	ipv4-address-any	Not Specified	0.0.0.0
https-client-certificate	Action based on received client certificate during the HTTPS handshake.	option	-	bypass
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
smtps-client-certificate	Action based on received client certificate during the SMTPS handshake.	option	-	bypass

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
pop3s-client-certificate	Action based on received client certificate during the POP3S handshake.	option	-	bypass
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
imaps-client-certificate	Action based on received client certificate during the IMAPS handshake.	option	-	bypass
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
ftps-client-certificate	Action based on received client certificate during the FTPS handshake.	option	-	bypass
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
ssl-other-client-certificate	Action based on received client certificate during an SSL protocol handshake.	option	-	bypass
	Option	Description		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		

config firewall ssl default-certificate

SSL default certificate.

```
config firewall ssl default-certificate
    Description: SSL default certificate.
    set default-ca {string}
    set default-untrusted-ca {string}
    set default-server-cert {string}
end
```

config firewall ssl default-certificate

Parameter	Description	Type	Size	Default
default-ca	Default CA certificate used by SSL inspection.	string	Maximum length: 35	Fortinet_CA_SSL
default-untrusted-ca	Default CA certificate used by SSL inspection.	string	Maximum length: 35	Fortinet_CA_Untrusted
default-server-cert	Default server certificate used by SSL inspection.	string	Maximum length: 35	Fortinet_Factory

config firewall ssl keyring-list

SSL keyring list.

```
config firewall ssl keyring-list
    Description: SSL keyring list.
    edit <name>
        set uuid {uuid}
    next
end
```

config firewall ssl keyring-list

Parameter	Description	Type	Size	Default
name	Keyring list name.	string	Maximum length: 35	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000

config firewall ssl setting

SSL proxy settings.

```
config firewall ssl setting
    Description: SSL proxy settings.
    set proxy-connect-timeout {integer}
    set ssl-dh-bits [768|1024|...]
    set ssl-send-empty-frags [enable|disable]
    set no-matching-cipher-action [bypass|drop]
    set cert-cache-capacity {integer}
    set cert-cache-timeout {integer}
    set session-cache-capacity {integer}
    set session-cache-timeout {integer}
    set abbreviate-handshake [enable|disable]
end
```

config firewall ssl setting

Parameter	Description	Type	Size	Default
proxy-connect-timeout	Time limit to make an internal connection to the appropriate proxy process.	integer	Minimum value: 1 Maximum value: 60	30
ssl-dh-bits	Bit-size of Diffie-Hellman.	option	-	2048
	Option Description			
	768	768-bit Diffie-Hellman prime.		
	1024	1024-bit Diffie-Hellman prime.		
	1536	1536-bit Diffie-Hellman prime.		
	2048	2048-bit Diffie-Hellman prime.		
ssl-send-empty-frags	Enable/disable sending empty fragments to avoid attack on CBC IV (for SSL 3.0 and TLS 1.0 only).	option	-	enable
	Option Description			
	enable	Send empty fragments.		
	disable	Do not send empty fragments.		
no-matching-cipher-action	Bypass or drop the connection when no matching cipher is found.	option	-	bypass
	Option Description			
	bypass	Bypass connection.		

Parameter	Description	Type	Size	Default
	Option	Description		
	drop	Drop connection.		
cert-cache-capacity	Maximum capacity of the host certificate cache.	integer	Minimum value: 0 Maximum value: 500	200
cert-cache-timeout	Time limit to keep certificate cache.	integer	Minimum value: 1 Maximum value: 120	10
session-cache-capacity	Capacity of the SSL session cache.	integer	Minimum value: 0 Maximum value: 1000	500
session-cache-timeout	Time limit to keep SSL session state.	integer	Minimum value: 1 Maximum value: 60	20
abbreviate-handshake	Enable/disable use of SSL abbreviated handshake.	option	-	enable
	Option	Description		
	enable	Enable use of SSL abbreviated handshake.		
	disable	Disable use of SSL abbreviated handshake.		

config firewall traffic-class

Configure names for shaping classes.

```
config firewall traffic-class
  Description: Configure names for shaping classes.
  edit <class-id>
    set class-name {string}
  next
end
```

config firewall traffic-class

Parameter	Description	Type	Size	Default
class-id	Class ID to be named.	integer	Minimum value: 2 Maximum value: 31	0
class-name	Define the name for this class-id.	string	Maximum length: 35	

config firewall ttl-policy

Configure TTL policies.

```
config firewall ttl-policy
  Description: Configure TTL policies.
  edit <id>
    set status [enable|disable]
    set action [accept|deny]
    set srcintf {string}
    set srcaddr <name1>, <name2>, ...
    set service <name1>, <name2>, ...
    set schedule {string}
    set ttl {user}
  next
end
```

config firewall ttl-policy

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
status	Enable/disable this TTL policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this TTL policy.</td></tr><tr><td><i>disable</i></td><td>Disable this TTL policy.</td></tr></table>				Option	Description	<i>enable</i>	Enable this TTL policy.	<i>disable</i>	Disable this TTL policy.
	Option	Description								
	<i>enable</i>	Enable this TTL policy.								
<i>disable</i>	Disable this TTL policy.									
action	Action to be performed on traffic matching this policy.	option	-	deny						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>accept</i>	Allow traffic matching this policy.		
	<i>deny</i>	Deny or block traffic matching this policy.		
srcintf	Source interface name from available interfaces.	string	Maximum length: 35	
srcaddr <name>	Source address object(s) from available options. Separate multiple names with a space. Address name.	string	Maximum length: 79	
service <name>	Service object(s) from available options. Separate multiple names with a space. Service name.	string	Maximum length: 79	
schedule	Schedule object from available options.	string	Maximum length: 35	
ttl	Value/range to match against the packet's Time to Live value.	user	Not Specified	

config firewall vendor-mac-summary

Vendor MAC database summary.

```
config firewall vendor-mac-summary
    Description: Vendor MAC database summary.
end
```

config firewall vendor-mac

Show vendor and the MAC address they have.

```
config firewall vendor-mac
    Description: Show vendor and the MAC address they have.
    edit <id>
        set name {string}
        set mac-number {integer}
        set obsolete {integer}
    next
end
```

config firewall vendor-mac

Parameter	Description	Type	Size	Default
id	Vendor ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Vendor name.	string	Maximum length: 63	
mac-number	Total number of MAC addresses.	integer	Minimum value: 0 Maximum value: 4294967295	0
obsolete	Indicates whether the Vendor ID can be used.	integer	Minimum value: 0 Maximum value: 255	0

config firewall vip

Configure virtual IP for IPv4.

```
config firewall vip
  Description: Configure virtual IP for IPv4.
  edit <name>
    set id {integer}
    set uuid {uuid}
    set comment {var-string}
    set type [static-nat|server-load-balance|...]
    set server-type [http|https|...]
    set ldb-method [static|round-robin|...]
    set extip {user}
    set h2-support [enable|disable]
    set h3-support [enable|disable]
  config quic
    Description: QUIC setting.
    set max-idle-timeout {integer}
    set max-udp-payload-size {integer}
    set active-connection-id-limit {integer}
    set ack-delay-exponent {integer}
    set max-ack-delay {integer}
    set max-datagram-frame-size {integer}
    set active-migration [enable|disable]
    set grease-quic-bit [enable|disable]
  end
```

```

set mappedip <range1>, <range2>, ...
set extintf {string}
set arp-reply [disable|enable]
set http-redirect [enable|disable]
set persistence [none|http-cookie|...]
set portforward [disable|enable]
set status [disable|enable]
set protocol [tcp|udp|...]
set extport {user}
set mappedport {user}
set gratuitous-arp-interval {integer}
config realservers
    Description: Select the real servers that this server load balancing VIP will
distribute traffic to.
    edit <id>
        set type [ip|address]
        set address {string}
        set ip {user}
        set port {integer}
        set status [active|standby|...]
        set weight {integer}
        set holddown-interval {integer}
        set healthcheck [disable|enable]
        set health-check-proto [ping|http]
        set http-host {string}
        set translate-host [enable|disable]
        set max-connections {integer}
        set client-ip {user}
    next
end
set http-cookie-domain-from-host [disable|enable]
set http-cookie-domain {string}
set http-cookie-path {string}
set http-cookie-generation {integer}
set http-cookie-age {integer}
set http-cookie-share [disable|same-ip]
set https-cookie-secure [disable|enable]
set http-multiplex [enable|disable]
set http-multiplex-ttl {integer}
set http-multiplex-max-request {integer}
set http-multiplex-max-concurrent-request {integer}
set http-ip-header [enable|disable]
set http-ip-header-name {string}
set outlook-web-access [disable|enable]
set weblogic-server [disable|enable]
set websphere-server [disable|enable]
set ssl-mode [half|full]
set ssl-certificate <name1>, <name2>, ...
set ssl-dh-bits [768|1024|...]
set ssl-algorithm [high|medium|...]
config ssl-cipher-suites
    Description: SSL/TLS cipher suites acceptable from a client, ordered by
priority.
    edit <priority>
        set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
        set versions {option1}, {option2}, ...

```



```

        next
    end
    set ssl-server-algorithm [high|medium|...]
    config ssl-server-cipher-suites
        Description: SSL/TLS cipher suites to offer to a server, ordered by priority.
        edit <priority>
            set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
            set versions {option1}, {option2}, ...
        next
    end
    set ssl-pfs [require|deny|...]
    set ssl-min-version [ssl-3.0|tls-1.0|...]
    set ssl-max-version [ssl-3.0|tls-1.0|...]
    set ssl-server-min-version [ssl-3.0|tls-1.0|...]
    set ssl-server-max-version [ssl-3.0|tls-1.0|...]
    set ssl-accept-ffdhe-groups [enable|disable]
    set ssl-send-empty-frags [enable|disable]
    set ssl-client-fallback [disable|enable]
    set ssl-client-renegotiation [allow|deny|...]
    set ssl-client-session-state-type [disable|time|...]
    set ssl-client-session-state-timeout {integer}
    set ssl-client-session-state-max {integer}
    set ssl-client-rekey-count {integer}
    set ssl-server-renegotiation [enable|disable]
    set ssl-server-session-state-type [disable|time|...]
    set ssl-server-session-state-timeout {integer}
    set ssl-server-session-state-max {integer}
    set ssl-http-location-conversion [enable|disable]
    set ssl-http-match-host [enable|disable]
    set ssl-hpkp [disable|enable|...]
    set ssl-hpkp-primary {string}
    set ssl-hpkp-backup {string}
    set ssl-hpkp-age {integer}
    set ssl-hpkp-report-uri {var-string}
    set ssl-hpkp-include-subdomains [disable|enable]
    set ssl-hsts [disable|enable]
    set ssl-hsts-age {integer}
    set ssl-hsts-include-subdomains [disable|enable]
    set max-embryonic-connections {integer}
    set color {integer}
next
end

```

config firewall vip

Parameter	Description	Type	Size	Default
name	Virtual IP name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
id	Custom defined ID.	integer	Minimum value: 0 Maximum value: 65535	0
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
comment	Comment.	var-string	Maximum length: 255	
type	Configure between a static NAT and access proxy VIP.	option	-	static-nat
	Option		Description	
	static-nat		Static NAT.	
	server-load-balance		Server load balance.	
	access-proxy		Access proxy.	
server-type	Protocol to be load balanced by the virtual server (also called the server load balance virtual IP).	option	-	
	Option		Description	
	http		HTTP.	
	https		HTTPS.	
	imaps		IMAPS.	
	pop3s		POP3S.	
	smtps		SMTPS.	
	ssl		SSL.	
	tcp		TCP.	
	udp		UDP.	
	ip		IP.	
ldb-method	Method used to distribute sessions to real servers.	option	-	static

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>static</i>	Distribute to server based on source IP.		
	<i>round-robin</i>	Distribute to server based round robin order.		
	<i>weighted</i>	Distribute to server based on weight.		
	<i>first-alive</i>	Distribute to the first server that is alive.		
	<i>http-host</i>	Distribute to server based on host field in HTTP header.		
extip	IP address or address range on the external interface that you want to map to an address or address range on the destination network.	user	Not Specified	
h2-support	Enable/disable HTTP2 support.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable HTTP2 support.		
	<i>disable</i>	Disable HTTP2 support.		
h3-support	Enable/disable HTTP3/QUIC support.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable HTTP3/QUIC support.		
	<i>disable</i>	Disable HTTP3/QUIC support.		
mappedip <range>	IP address or address range on the destination network to which the external IP address is mapped. Mapped IP range.	string	Maximum length: 79	
extintf	Interface connected to the source network that receives the packets that will be forwarded to the destination network.	string	Maximum length: 35	
arp-reply	Enable to respond to ARP requests for this virtual IP address. Enabled by default.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable ARP reply.		
	<i>enable</i>	Enable ARP reply.		
http-redirect	Enable/disable redirection of HTTP to HTTPS.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable redirection of HTTP to HTTPS.		
	<i>disable</i>	Disable redirection of HTTP to HTTPS.		
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none
	Option	Description		
	<i>none</i>	None.		
	<i>http-cookie</i>	HTTP cookie.		
	<i>ssl-session-id</i>	SSL session ID.		
portforward	Enable/disable port forwarding.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable port forward.		
	<i>enable</i>	Enable port forward.		
status	Enable/disable VIP.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable the VIP.		
	<i>enable</i>	Enable the VIP.		
protocol	Protocol to use when forwarding packets.	option	-	tcp
	Option	Description		
	<i>tcp</i>	TCP.		
	<i>udp</i>	UDP.		
	<i>sctp</i>	SCTP.		
	<i>icmp</i>	ICMP.		
extport	Incoming port number range that you want to map to a port number range on the destination network.	user	Not Specified	

Parameter	Description	Type	Size	Default						
mappedport	Port number range on the destination network to which the external port number range is mapped.	user	Not Specified							
gratuitous-arp-interval	Enable to have the VIP send gratuitous ARPs. 0=disabled. Set from 5 up to 8640000 seconds to enable.	integer	Minimum value: 5 Maximum value: 8640000	0						
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable use of HTTP cookie domain from host field in HTTP (use http-cookies-domain setting).</td></tr><tr><td>enable</td><td>Enable use of HTTP cookie domain from host field in HTTP.</td></tr></table>				Option	Description	disable	Disable use of HTTP cookie domain from host field in HTTP (use http-cookies-domain setting).	enable	Enable use of HTTP cookie domain from host field in HTTP.
	Option	Description								
	disable	Disable use of HTTP cookie domain from host field in HTTP (use http-cookies-domain setting).								
enable	Enable use of HTTP cookie domain from host field in HTTP.									
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35							
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35							
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295	0						
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600	60						
http-cookie-share	Control sharing of cookies across virtual servers. Use of same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Only allow HTTP cookie to match this virtual server.</td></tr><tr><td>same-ip</td><td>Allow HTTP cookie to match any virtual server with same IP.</td></tr></table>				Option	Description	disable	Only allow HTTP cookie to match this virtual server.	same-ip	Allow HTTP cookie to match any virtual server with same IP.
	Option	Description								
	disable	Only allow HTTP cookie to match this virtual server.								
same-ip	Allow HTTP cookie to match any virtual server with same IP.									
https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.		
	<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.		
http-multiplex	Enable/disable HTTP multiplexing.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable HTTP session multiplexing.		
	<i>disable</i>	Disable HTTP session multiplexing.		
http-multiplex-ttl	Time-to-live for idle connections to servers.	integer	Minimum value: 0 Maximum value: 2147483647	15
http-multiplex-max-request	Maximum number of requests that a multiplex server can handle before disconnecting sessions.	integer	Minimum value: 0 Maximum value: 2147483647	0
http-multiplex-max-concurrent-request	Maximum number of concurrent requests that a multiplex server can handle.	integer	Minimum value: 0 Maximum value: 2147483647	0
http-ip-header	For HTTP multiplexing, enable to add the original client IP address in the XForwarded-For HTTP header.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable adding HTTP header.		
	<i>disable</i>	Disable adding HTTP header.		
http-ip-header-name	For HTTP multiplexing, enter a custom HTTPS header name. The original client IP address is added to this header. If empty, X-Forwarded-For is used.	string	Maximum length: 35	
outlook-web-access	Enable to add the Front-End-Https header for Microsoft Outlook Web Access.	option	-	disable

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Outlook Web Access support.</td></tr><tr><td><i>enable</i></td><td>Enable Outlook Web Access support.</td></tr></table>	Option	Description	<i>disable</i>	Disable Outlook Web Access support.	<i>enable</i>	Enable Outlook Web Access support.							
Option	Description													
<i>disable</i>	Disable Outlook Web Access support.													
<i>enable</i>	Enable Outlook Web Access support.													
weblogic-server	Enable to add an HTTP header to indicate SSL offloading for a WebLogic server.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not add HTTP header indicating SSL offload for WebLogic server.</td></tr><tr><td><i>enable</i></td><td>Add HTTP header indicating SSL offload for WebLogic server.</td></tr></table>	Option	Description	<i>disable</i>	Do not add HTTP header indicating SSL offload for WebLogic server.	<i>enable</i>	Add HTTP header indicating SSL offload for WebLogic server.							
Option	Description													
<i>disable</i>	Do not add HTTP header indicating SSL offload for WebLogic server.													
<i>enable</i>	Add HTTP header indicating SSL offload for WebLogic server.													
websphere-server	Enable to add an HTTP header to indicate SSL offloading for a WebSphere server.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not add HTTP header indicating SSL offload for WebSphere server.</td></tr><tr><td><i>enable</i></td><td>Add HTTP header indicating SSL offload for WebSphere server.</td></tr></table>	Option	Description	<i>disable</i>	Do not add HTTP header indicating SSL offload for WebSphere server.	<i>enable</i>	Add HTTP header indicating SSL offload for WebSphere server.							
Option	Description													
<i>disable</i>	Do not add HTTP header indicating SSL offload for WebSphere server.													
<i>enable</i>	Add HTTP header indicating SSL offload for WebSphere server.													
ssl-mode	Apply SSL offloading between the client and the FortiProxy (half) or from the client to the FortiProxy and from the FortiProxy to the server (full).	option	-	half										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>half</i></td><td>Client to FortiProxy SSL.</td></tr><tr><td><i>full</i></td><td>Client to FortiProxy and FortiProxy to Server SSL.</td></tr></table>	Option	Description	<i>half</i>	Client to FortiProxy SSL.	<i>full</i>	Client to FortiProxy and FortiProxy to Server SSL.							
Option	Description													
<i>half</i>	Client to FortiProxy SSL.													
<i>full</i>	Client to FortiProxy and FortiProxy to Server SSL.													
ssl-certificate <name>	Name of the certificate to use for SSL handshake. Certificate list.	string	Maximum length: 79											
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>768</i></td><td>768-bit Diffie-Hellman prime.</td></tr><tr><td><i>1024</i></td><td>1024-bit Diffie-Hellman prime.</td></tr><tr><td><i>1536</i></td><td>1536-bit Diffie-Hellman prime.</td></tr><tr><td><i>2048</i></td><td>2048-bit Diffie-Hellman prime.</td></tr></table>	Option	Description	<i>768</i>	768-bit Diffie-Hellman prime.	<i>1024</i>	1024-bit Diffie-Hellman prime.	<i>1536</i>	1536-bit Diffie-Hellman prime.	<i>2048</i>	2048-bit Diffie-Hellman prime.			
Option	Description													
<i>768</i>	768-bit Diffie-Hellman prime.													
<i>1024</i>	1024-bit Diffie-Hellman prime.													
<i>1536</i>	1536-bit Diffie-Hellman prime.													
<i>2048</i>	2048-bit Diffie-Hellman prime.													

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>3072</td><td>3072-bit Diffie-Hellman prime.</td></tr><tr><td>4096</td><td>4096-bit Diffie-Hellman prime.</td></tr></table>	Option	Description	3072	3072-bit Diffie-Hellman prime.	4096	4096-bit Diffie-Hellman prime.									
	Option	Description														
	3072	3072-bit Diffie-Hellman prime.														
4096	4096-bit Diffie-Hellman prime.															
ssl-algorithm	Permitted encryption algorithms for SSL sessions according to encryption strength.	option	-	high												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high</td><td>High encryption. Allow only AES and ChaCha.</td></tr><tr><td>medium</td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td>low</td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr><tr><td>custom</td><td>Custom encryption. Use config ssl-cipher-suites to select the cipher suites that are allowed.</td></tr></table>	Option	Description	high	High encryption. Allow only AES and ChaCha.	medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.	custom	Custom encryption. Use config ssl-cipher-suites to select the cipher suites that are allowed.					
	Option	Description														
	high	High encryption. Allow only AES and ChaCha.														
	medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.														
	low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.														
custom	Custom encryption. Use config ssl-cipher-suites to select the cipher suites that are allowed.															
ssl-server-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-	client												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high</td><td>High encryption. Allow only AES and ChaCha.</td></tr><tr><td>medium</td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td>low</td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr><tr><td>custom</td><td>Custom encryption. Use ssl-server-cipher-suites to select the cipher suites that are allowed.</td></tr><tr><td>client</td><td>Use the same encryption algorithms for both client and server sessions.</td></tr></table>	Option	Description	high	High encryption. Allow only AES and ChaCha.	medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.	custom	Custom encryption. Use ssl-server-cipher-suites to select the cipher suites that are allowed.	client	Use the same encryption algorithms for both client and server sessions.			
	Option	Description														
	high	High encryption. Allow only AES and ChaCha.														
	medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.														
	low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.														
	custom	Custom encryption. Use ssl-server-cipher-suites to select the cipher suites that are allowed.														
client	Use the same encryption algorithms for both client and server sessions.															
ssl-pfs	Select the cipher suites that can be used for SSL perfect forward secrecy (PFS). Applies to both client and server sessions.	option	-	require												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>require</td><td>Allow only Diffie-Hellman cipher-suites, so PFS is applied.</td></tr><tr><td>deny</td><td>Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.</td></tr><tr><td>allow</td><td>Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.</td></tr></table>	Option	Description	require	Allow only Diffie-Hellman cipher-suites, so PFS is applied.	deny	Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.	allow	Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.							
	Option	Description														
	require	Allow only Diffie-Hellman cipher-suites, so PFS is applied.														
	deny	Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.														
allow	Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.															
ssl-min-version	Lowest SSL/TLS version acceptable from a client.	option	-	tls-1.1												

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ssl-3.0</td><td>SSL 3.0.</td></tr><tr><td>tls-1.0</td><td>TLS 1.0.</td></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr><tr><td>tls-1.2</td><td>TLS 1.2.</td></tr><tr><td>tls-1.3</td><td>TLS 1.3.</td></tr></table>	Option	Description	ssl-3.0	SSL 3.0.	tls-1.0	TLS 1.0.	tls-1.1	TLS 1.1.	tls-1.2	TLS 1.2.	tls-1.3	TLS 1.3.					
	Option	Description																
	ssl-3.0	SSL 3.0.																
	tls-1.0	TLS 1.0.																
	tls-1.1	TLS 1.1.																
	tls-1.2	TLS 1.2.																
	tls-1.3	TLS 1.3.																
ssl-max-version	Highest SSL/TLS version acceptable from a client.	option	-	tls-1.3														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ssl-3.0</td><td>SSL 3.0.</td></tr><tr><td>tls-1.0</td><td>TLS 1.0.</td></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr><tr><td>tls-1.2</td><td>TLS 1.2.</td></tr><tr><td>tls-1.3</td><td>TLS 1.3.</td></tr></table>	Option	Description	ssl-3.0	SSL 3.0.	tls-1.0	TLS 1.0.	tls-1.1	TLS 1.1.	tls-1.2	TLS 1.2.	tls-1.3	TLS 1.3.					
	Option	Description																
	ssl-3.0	SSL 3.0.																
	tls-1.0	TLS 1.0.																
	tls-1.1	TLS 1.1.																
	tls-1.2	TLS 1.2.																
	tls-1.3	TLS 1.3.																
ssl-server-min-version	Lowest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-	client														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ssl-3.0</td><td>SSL 3.0.</td></tr><tr><td>tls-1.0</td><td>TLS 1.0.</td></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr><tr><td>tls-1.2</td><td>TLS 1.2.</td></tr><tr><td>tls-1.3</td><td>TLS 1.3.</td></tr><tr><td>client</td><td>Use same value as client configuration.</td></tr></table>	Option	Description	ssl-3.0	SSL 3.0.	tls-1.0	TLS 1.0.	tls-1.1	TLS 1.1.	tls-1.2	TLS 1.2.	tls-1.3	TLS 1.3.	client	Use same value as client configuration.			
	Option	Description																
	ssl-3.0	SSL 3.0.																
	tls-1.0	TLS 1.0.																
	tls-1.1	TLS 1.1.																
	tls-1.2	TLS 1.2.																
	tls-1.3	TLS 1.3.																
client	Use same value as client configuration.																	
ssl-server-max-version	Highest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-	client														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ssl-3.0</td><td>SSL 3.0.</td></tr><tr><td>tls-1.0</td><td>TLS 1.0.</td></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr></table>	Option	Description	ssl-3.0	SSL 3.0.	tls-1.0	TLS 1.0.	tls-1.1	TLS 1.1.									
	Option	Description																
	ssl-3.0	SSL 3.0.																
	tls-1.0	TLS 1.0.																
tls-1.1	TLS 1.1.																	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>tls-1.2</i>	TLS 1.2.		
	<i>tls-1.3</i>	TLS 1.3.		
	<i>client</i>	Use same value as client configuration.		
ssl-accept-ffdhe-groups	Enable/disable FFDHE cipher suite for SSL key exchange.	option	-	enable
	Option	Description		
	<i>enable</i>	Accept FFDHE groups.		
	<i>disable</i>	Do not accept FFDHE groups.		
ssl-send-empty-frags	Enable/disable sending empty fragments to avoid CBC IV attacks (SSL 3.0 & TLS 1.0 only). May need to be disabled for compatibility with older systems.	option	-	enable
	Option	Description		
	<i>enable</i>	Send empty fragments.		
	<i>disable</i>	Do not send empty fragments.		
ssl-client-fallback	Enable/disable support for preventing Downgrade Attacks on client connections (RFC 7507).	option	-	enable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>enable</i>	Enable.		
ssl-client-renegotiation	Allow, deny, or require secure renegotiation of client sessions to comply with RFC 5746.	option	-	secure
	Option	Description		
	<i>allow</i>	Allow a SSL client to renegotiate.		
	<i>deny</i>	Abort any client initiated SSL re-negotiation attempt.		
	<i>secure</i>	Abort any client initiated SSL re-negotiation attempt that does not use RFC 5746 Secure Renegotiation.		
ssl-client-session-state-type	How to expire SSL sessions for the segment of the SSL connection between the client and the FortiProxy.	option	-	both

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not keep session states.</td></tr><tr><td><i>time</i></td><td>Expire session states after this many minutes.</td></tr><tr><td><i>count</i></td><td>Expire session states when this maximum is reached.</td></tr><tr><td><i>both</i></td><td>Expire session states based on time or count, whichever occurs first.</td></tr></table>	Option	Description	<i>disable</i>	Do not keep session states.	<i>time</i>	Expire session states after this many minutes.	<i>count</i>	Expire session states when this maximum is reached.	<i>both</i>	Expire session states based on time or count, whichever occurs first.			
	Option	Description												
	<i>disable</i>	Do not keep session states.												
	<i>time</i>	Expire session states after this many minutes.												
	<i>count</i>	Expire session states when this maximum is reached.												
<i>both</i>	Expire session states based on time or count, whichever occurs first.													
ssl-client-session-state-timeout	Number of minutes to keep client to FortiProxy SSL session state.	integer	Minimum value: 1 Maximum value: 14400	30										
ssl-client-session-state-max	Maximum number of client to FortiProxy SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000	1000										
ssl-client-rekey-count	Maximum length of data in MB before triggering a client rekey (0 = disable).	integer	Minimum value: 200 Maximum value: 1048576	0										
ssl-server-renegotiation	Enable/disable secure renegotiation to comply with RFC 5746.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable secure renegotiation.</td></tr><tr><td><i>disable</i></td><td>Disable secure renegotiation.</td></tr></table>	Option	Description	<i>enable</i>	Enable secure renegotiation.	<i>disable</i>	Disable secure renegotiation.							
	Option	Description												
	<i>enable</i>	Enable secure renegotiation.												
	<i>disable</i>	Disable secure renegotiation.												
ssl-server-session-state-type	How to expire SSL sessions for the segment of the SSL connection between the server and the FortiProxy.	option	-	both										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not keep session states.</td></tr><tr><td><i>time</i></td><td>Expire session states after this many minutes.</td></tr><tr><td><i>count</i></td><td>Expire session states when this maximum is reached.</td></tr><tr><td><i>both</i></td><td>Expire session states based on time or count, whichever occurs first.</td></tr></table>	Option	Description	<i>disable</i>	Do not keep session states.	<i>time</i>	Expire session states after this many minutes.	<i>count</i>	Expire session states when this maximum is reached.	<i>both</i>	Expire session states based on time or count, whichever occurs first.			
	Option	Description												
	<i>disable</i>	Do not keep session states.												
	<i>time</i>	Expire session states after this many minutes.												
	<i>count</i>	Expire session states when this maximum is reached.												
<i>both</i>	Expire session states based on time or count, whichever occurs first.													
ssl-server-session-state-timeout	Number of minutes to keep FortiProxy to Server SSL session state.	integer	Minimum value: 1 Maximum value: 14400	60										

Parameter	Description	Type	Size	Default								
ssl-server-session-state-max	Maximum number of FortiProxy to Server SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000	100								
ssl-http-location-conversion	Enable to replace HTTP with HTTPS in the reply's Location HTTP header field.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable HTTP location conversion.</td></tr><tr><td>disable</td><td>Disable HTTP location conversion.</td></tr></table>				Option	Description	enable	Enable HTTP location conversion.	disable	Disable HTTP location conversion.		
	Option	Description										
	enable	Enable HTTP location conversion.										
disable	Disable HTTP location conversion.											
ssl-http-match-host	Enable/disable HTTP host matching for location conversion.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Match HTTP host in response header.</td></tr><tr><td>disable</td><td>Do not match HTTP host.</td></tr></table>				Option	Description	enable	Match HTTP host in response header.	disable	Do not match HTTP host.		
	Option	Description										
	enable	Match HTTP host in response header.										
disable	Do not match HTTP host.											
ssl-hpkp	Enable/disable including HPKP header in response.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not add a HPKP header to each HTTP response.</td></tr><tr><td>enable</td><td>Add a HPKP header to each a HTTP response.</td></tr><tr><td>report-only</td><td>Add a HPKP Report-Only header to each HTTP response.</td></tr></table>				Option	Description	disable	Do not add a HPKP header to each HTTP response.	enable	Add a HPKP header to each a HTTP response.	report-only	Add a HPKP Report-Only header to each HTTP response.
	Option	Description										
	disable	Do not add a HPKP header to each HTTP response.										
	enable	Add a HPKP header to each a HTTP response.										
report-only	Add a HPKP Report-Only header to each HTTP response.											
ssl-hpkp-primary	Certificate to generate primary HPKP pin from.	string	Maximum length: 79									
ssl-hpkp-backup	Certificate to generate backup HPKP pin from.	string	Maximum length: 79									
ssl-hpkp-age	Number of seconds the client should honor the HPKP setting.	integer	Minimum value: 60 Maximum value: 157680000	5184000								
ssl-hpkp-report-uri	URL to report HPKP violations to.	var-string	Maximum length: 255									
ssl-hpkp-include-subdomains	Indicate that HPKP header applies to all subdomains.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	HPKP header does not apply to subdomains.		
	<i>enable</i>	HPKP header applies to subdomains.		
ssl-hsts	Enable/disable including HSTS header in response.	option	-	disable
	Option	Description		
	<i>disable</i>	Do not add a HSTS header to each a HTTP response.		
	<i>enable</i>	Add a HSTS header to each HTTP response.		
ssl-hsts-age	Number of seconds the client should honor the HSTS setting.	integer	Minimum value: 60 Maximum value: 157680000	5184000
ssl-hsts-include-subdomains	Indicate that HSTS header applies to all subdomains.	option	-	disable
	Option	Description		
	<i>disable</i>	HSTS header does not apply to subdomains.		
	<i>enable</i>	HSTS header applies to subdomains.		
max-embryonic-connections	Maximum number of incomplete connections.	integer	Minimum value: 0 Maximum value: 100000	1000
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0

config quic

Parameter	Description	Type	Size	Default
max-idle-timeout	Maximum idle timeout milliseconds.	integer	Minimum value: 1 Maximum value: 60000	30000

Parameter	Description	Type	Size	Default
max-udp-payload-size	Maximum UDP payload size in bytes.	integer	Minimum value: 1200 Maximum value: 1500	1500
active-connection-id-limit	Active connection ID limit.	integer	Minimum value: 1 Maximum value: 8	2
ack-delay-exponent	ACK delay exponent.	integer	Minimum value: 1 Maximum value: 20	3
max-ack-delay	Maximum ACK delay in milliseconds.	integer	Minimum value: 1 Maximum value: 16383	25
max-datagram-frame-size	Maximum datagram frame size in bytes.	integer	Minimum value: 1 Maximum value: 1500	1500
active-migration	Enable/disable active migration.	option	-	disable
	Option	Description		
	enable	Enable active migration.		
	disable	Disable active migration.		
grease-quic-bit	Enable/disable grease QUIC bit.	option	-	enable
	Option	Description		
	enable	Enable grease QUIC bit.		
	disable	Disable grease QUIC bit.		

config realservers

Parameter	Description	Type	Size	Default								
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
type	Type of address.	option	-	ip								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ip</i></td><td>Standard IPv4 address.</td></tr><tr><td><i>address</i></td><td>Dynamic address object.</td></tr></table>				Option	Description	<i>ip</i>	Standard IPv4 address.	<i>address</i>	Dynamic address object.		
Option	Description											
<i>ip</i>	Standard IPv4 address.											
<i>address</i>	Dynamic address object.											
address	Dynamic address of the real server.	string	Maximum length: 79									
ip	IP address of the real server.	user	Not Specified									
port	Port for communicating with the real server. Required if port forwarding is enabled.	integer	Minimum value: 1 Maximum value: 65535	0								
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-	active								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>active</i></td><td>Server status active.</td></tr><tr><td><i>standby</i></td><td>Server status standby.</td></tr><tr><td><i>disable</i></td><td>Server status disable.</td></tr></table>				Option	Description	<i>active</i>	Server status active.	<i>standby</i>	Server status standby.	<i>disable</i>	Server status disable.
Option	Description											
<i>active</i>	Server status active.											
<i>standby</i>	Server status standby.											
<i>disable</i>	Server status disable.											
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255	1								
holddown-interval	Time in seconds that the health check monitor continues to monitor and unresponsive server that should be active.	integer	Minimum value: 30 Maximum value: 65535	300								
healthcheck	Enable to check the responsiveness of the real server before forwarding traffic.	option	-									

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable per server health check.</td></tr><tr><td><i>enable</i></td><td>Enable per server health check.</td></tr></table>	Option	Description	<i>disable</i>	Disable per server health check.	<i>enable</i>	Enable per server health check.			
	Option	Description								
	<i>disable</i>	Disable per server health check.								
<i>enable</i>	Enable per server health check.									
health-check-proto	Protocol of the health check monitor to use when polling to determine server's connectivity status.	option	-	ping						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>Use PING to test the link with the server.</td></tr><tr><td><i>http</i></td><td>Use HTTP-GET to test the link with the server.</td></tr></table>	Option	Description	<i>ping</i>	Use PING to test the link with the server.	<i>http</i>	Use HTTP-GET to test the link with the server.			
	Option	Description								
	<i>ping</i>	Use PING to test the link with the server.								
<i>http</i>	Use HTTP-GET to test the link with the server.									
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63							
translate-host	Enable/disable translation of hostname/IP from virtual server to real server.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable virtual hostname/IP translation.</td></tr><tr><td><i>disable</i></td><td>Disable virtual hostname/IP translation.</td></tr></table>	Option	Description	<i>enable</i>	Enable virtual hostname/IP translation.	<i>disable</i>	Disable virtual hostname/IP translation.			
	Option	Description								
	<i>enable</i>	Enable virtual hostname/IP translation.								
<i>disable</i>	Disable virtual hostname/IP translation.									
max-connections	Max number of active connections that can be directed to the real server. When reached, sessions are sent to other real servers.	integer	Minimum value: 0 Maximum value: 2147483647	0						
client-ip	Only clients in this IP range can connect to this real server.	user	Not Specified							

config ssl-cipher-suites

Parameter	Description	Type	Size	Default
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295	0
cipher	Cipher suite name.	option	-	

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>TLS-AES-128-GCM-SHA256</td><td>Cipher suite TLS-AES-128-GCM-SHA256.</td></tr><tr><td>TLS-AES-256-GCM-SHA384</td><td>Cipher suite TLS-AES-256-GCM-SHA384.</td></tr><tr><td>TLS-CHACHA20-POLY1305-SHA256</td><td>Cipher suite TLS-CHACHA20-POLY1305-SHA256.</td></tr><tr><td>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</td><td>Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr><tr><td>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.</td></tr></table>	Option	Description	TLS-AES-128-GCM-SHA256	Cipher suite TLS-AES-128-GCM-SHA256.	TLS-AES-256-GCM-SHA384	Cipher suite TLS-AES-256-GCM-SHA384.	TLS-CHACHA20-POLY1305-SHA256	Cipher suite TLS-CHACHA20-POLY1305-SHA256.	TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.	TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.	TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.	TLS-DHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.	TLS-DHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.	TLS-DHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.	TLS-DHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.	TLS-DHE-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.			
Option	Description																											
TLS-AES-128-GCM-SHA256	Cipher suite TLS-AES-128-GCM-SHA256.																											
TLS-AES-256-GCM-SHA384	Cipher suite TLS-AES-256-GCM-SHA384.																											
TLS-CHACHA20-POLY1305-SHA256	Cipher suite TLS-CHACHA20-POLY1305-SHA256.																											
TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.																											
TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.																											
TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.																											
TLS-DHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.																											
TLS-DHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.																											
TLS-DHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.																											
TLS-DHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.																											
TLS-DHE-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.																											

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-DHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.		
	TLS-DHE-DSS-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.		
	TLS-DHE-DSS-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.		
	TLS-DHE-DSS-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.		
	TLS-DHE-DSS-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.		
	TLS-DHE-DSS-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.		
	TLS-DHE-DSS-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.		
	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.		
	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.		
	TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.		
	TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.		

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.</td></tr><tr><td><i>TLS-RSA-WITH-AES-128-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-AES-256-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.	<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.	<i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.	<i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.	<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.	<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.			
Option	Description																									
<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.																									
<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.																									
<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.																									
<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.																									
<i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.																									
<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.																									
<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.																									
<i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.																									
<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.																									
<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.																									

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-RSA-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-AES-256-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.</td></tr><tr><td><i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i></td><td>Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.	<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.	<i>TLS-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.	<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.			
Option	Description																											
<i>TLS-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.																											
<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.																											
<i>TLS-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.																											
<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.																											
<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.																											
<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.																											
<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.																											
<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.																											
<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.																											
<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.																											
<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.																											

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.		
	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.		
	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.		
	TLS-DHE-RSA-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.		
	TLS-DHE-DSS-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.		
	TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.		
TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.			

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-RSA-WITH-SEED-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.	<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.	<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.			
Option	Description																											
<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.																											
<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.																											
<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.																											
<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.																											
<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.																											
<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.																											
<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.																											
<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.																											
<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.																											
<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.																											
<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.																											

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-MD5</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-MD5.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-DES-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.			
	Option	Description																		
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.																		
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.																		
	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.																		
	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.																		
	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.																		
	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.																		
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.																			
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	ssl-3.0 tls-1.0 tls-1.1 tls-1.2 tls-1.3																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.							
	Option	Description																		
	<i>ssl-3.0</i>	SSL 3.0.																		
	<i>tls-1.0</i>	TLS 1.0.																		
	<i>tls-1.1</i>	TLS 1.1.																		
	<i>tls-1.2</i>	TLS 1.2.																		
<i>tls-1.3</i>	TLS 1.3.																			

config ssl-server-cipher-suites

Parameter	Description	Type	Size	Default
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295	0
cipher	Cipher suite name.	option	-	

Option	Description
<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.
<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.
<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.
<i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
<i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.
<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.
<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.

Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.</td></tr></table>	Option	Description	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.			
Option	Description																													
<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.																													
<i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.																													
<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.																													
<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.																													
<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.																													
<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.																													
<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.																													
<i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.																													
<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.																													
<i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.																													
<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.																													
<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.																													

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.		
	TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.		
	TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.		
	TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.		
	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.		
	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.		
	TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.		
	TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.		
	TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.		
TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.			

Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-RSA-WITH-AES-128-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-AES-256-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-AES-256-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.</td></tr><tr><td><i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.	<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.	<i>TLS-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.	<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.	<i>TLS-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.	<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.			
Option	Description																													
<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.																													
<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.																													
<i>TLS-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.																													
<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.																													
<i>TLS-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.																													
<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.																													
<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.																													
<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.																													
<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.																													
<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.																													
<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.																													
<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.																													

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i></td><td>Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr></table>	Option	Description	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.	<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.	<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.			
Option	Description																									
<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.																									
<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.																									
<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.																									
<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.																									
<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.																									
<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.																									
<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.																									
<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.																									
<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.																									
<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.																									

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-RSA-WITH-SEED-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.</td></tr></table>	Option	Description	<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.	<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.	<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.			
Option	Description																											
<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.																											
<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.																											
<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.																											
<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.																											
<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.																											
<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.																											
<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.																											
<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.																											
<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.																											
<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.																											
<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.																											

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-MD5</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-MD5.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-DES-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.			
	Option	Description																				
	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.																				
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.																				
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.																				
	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.																				
	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.																				
	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.																				
	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.																				
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.																					
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	ssl-3.0 tls-1.0 tls-1.1 tls-1.2 tls-1.3																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.									
	Option	Description																				
	<i>ssl-3.0</i>	SSL 3.0.																				
	<i>tls-1.0</i>	TLS 1.0.																				
	<i>tls-1.1</i>	TLS 1.1.																				
<i>tls-1.2</i>	TLS 1.2.																					
<i>tls-1.3</i>	TLS 1.3.																					

config firewall vipgrp

Configure IPv4 virtual IP groups.

```
config firewall vipgrp
  Description: Configure IPv4 virtual IP groups.
  edit <name>
    set uuid {uuid}
    set interface {string}
    set color {integer}
    set comments {var-string}
    set member <name1>, <name2>, ...
  next
end
```

config firewall vipgrp

Parameter	Description	Type	Size	Default
name	VIP group name.	string	Maximum length: 79	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
interface	Interface.	string	Maximum length: 35	
color	Integer value to determine the color of the icon in the GUI.	integer	Minimum value: 0 Maximum value: 32	0
comments	Comment.	var-string	Maximum length: 255	
member <name>	Member VIP objects of the group (Separate multiple objects with a space). VIP name.	string	Maximum length: 79	

config firewall wildcard-fqdn custom

Config global/VDOM Wildcard FQDN address.

```
config firewall wildcard-fqdn custom
  Description: Config global/VDOM Wildcard FQDN address.
  edit <name>
    set uuid {uuid}
    set wildcard-fqdn {string}
```

```

        set color {integer}
        set comment {var-string}
    next
end

```

config firewall wildcard-fqdn custom

Parameter	Description	Type	Size	Default
name	Address name.	string	Maximum length: 79	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
wildcard-fqdn	Wildcard FQDN.	string	Maximum length: 255	
color	GUI icon color.	integer	Minimum value: 0 Maximum value: 32	0
comment	Comment.	var-string	Maximum length: 255	

config firewall wildcard-fqdn group

Config global Wildcard FQDN address groups.

```

config firewall wildcard-fqdn group
    Description: Config global Wildcard FQDN address groups.
    edit <name>
        set uuid {uuid}
        set member <name1>, <name2>, ...
        set color {integer}
        set comment {var-string}
    next
end

```

config firewall wildcard-fqdn group

Parameter	Description	Type	Size	Default
name	Address group name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
member <name>	Address group members. Address name.	string	Maximum length: 79	
color	GUI icon color.	integer	Minimum value: 0 Maximum value: 32	0
comment	Comment.	var-string	Maximum length: 255	

ftp-proxy

This section includes syntax for the following commands:

- [config ftp-proxy explicit on page 386](#)

config ftp-proxy explicit

Configure explicit FTP proxy settings.

```
config ftp-proxy explicit
    Description: Configure explicit FTP proxy settings.
    set status [enable|disable]
    set incoming-port {user}
    set incoming-ip {ipv4-address-any}
    set outgoing-ip {ipv4-address-any}
    set sec-default-action [accept|deny]
    set server-data-mode [client|passive]
    set active-src-port [default|server]
    set ipv6-status [enable|disable]
    set incoming-ip6 {ipv6-address}
    set ssl [enable|disable]
    set ssl-cert <name1>, <name2>, ...
    set ssl-dh-bits [768|1024|...]
    set ssl-algorithm [high|medium|...]
end
```

config ftp-proxy explicit

Parameter	Description	Type	Size	Default
status	Enable/disable the explicit FTP proxy.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable the explicit FTP proxy.		
	<i>disable</i>	Disable the explicit FTP proxy.		
incoming-port	Accept incoming FTP requests on one or more ports.	user	Not Specified	
incoming-ip	Accept incoming FTP requests from this IP address. An interface must have this IP address.	ipv4-address-any	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default						
outgoing-ip	Outgoing FTP requests will leave from this IP address. An interface must have this IP address.	ipv4-address-any	Not Specified							
sec-default-action	Accept or deny explicit FTP proxy sessions when no FTP proxy firewall policy exists.	option	-	deny						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accept</i></td><td>Accept requests. All explicit FTP proxy traffic is accepted whether there is an explicit FTP proxy policy or not</td></tr><tr><td><i>deny</i></td><td>Deny requests unless there is a matching explicit FTP proxy policy.</td></tr></table>	Option	Description	<i>accept</i>	Accept requests. All explicit FTP proxy traffic is accepted whether there is an explicit FTP proxy policy or not	<i>deny</i>	Deny requests unless there is a matching explicit FTP proxy policy.			
Option	Description									
<i>accept</i>	Accept requests. All explicit FTP proxy traffic is accepted whether there is an explicit FTP proxy policy or not									
<i>deny</i>	Deny requests unless there is a matching explicit FTP proxy policy.									
server-data-mode	Determine mode of data session on FTP server side.	option	-	client						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>client</i></td><td>Use the same transmission mode for client and server data sessions.</td></tr><tr><td><i>passive</i></td><td>Use passive mode on server data session.</td></tr></table>	Option	Description	<i>client</i>	Use the same transmission mode for client and server data sessions.	<i>passive</i>	Use passive mode on server data session.			
Option	Description									
<i>client</i>	Use the same transmission mode for client and server data sessions.									
<i>passive</i>	Use passive mode on server data session.									
active-src-port	Determine port for data session to connect FTP client in active mode.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Use the incoming port - 1 to connect client data session in active mode.</td></tr><tr><td><i>server</i></td><td>Use the same port as FTP server source port to connect client data session in active mode.</td></tr></table>	Option	Description	<i>default</i>	Use the incoming port - 1 to connect client data session in active mode.	<i>server</i>	Use the same port as FTP server source port to connect client data session in active mode.			
Option	Description									
<i>default</i>	Use the incoming port - 1 to connect client data session in active mode.									
<i>server</i>	Use the same port as FTP server source port to connect client data session in active mode.									
ipv6-status	Enable/disable allowing an IPv6 ftp proxy destination in policies and all IPv6 related entries in this command.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable allowing an IPv6 ftp proxy destination.</td></tr><tr><td><i>disable</i></td><td>Disable allowing an IPv6 ftp proxy destination.</td></tr></table>	Option	Description	<i>enable</i>	Enable allowing an IPv6 ftp proxy destination.	<i>disable</i>	Disable allowing an IPv6 ftp proxy destination.			
Option	Description									
<i>enable</i>	Enable allowing an IPv6 ftp proxy destination.									
<i>disable</i>	Disable allowing an IPv6 ftp proxy destination.									
incoming-ip6	Restrict the explicit ftp proxy to only accept sessions from this IPv6 address. An interface must have this IPv6 address.	ipv6-address	Not Specified	::						
ssl	Enable/disable the explicit FTPS proxy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the explicit FTPS proxy.</td></tr><tr><td><i>disable</i></td><td>Disable the explicit FTPS proxy.</td></tr></table>	Option	Description	<i>enable</i>	Enable the explicit FTPS proxy.	<i>disable</i>	Disable the explicit FTPS proxy.			
Option	Description									
<i>enable</i>	Enable the explicit FTPS proxy.									
<i>disable</i>	Disable the explicit FTPS proxy.									

Parameter	Description	Type	Size	Default
ssl-cert <name>	List of certificate names to use for SSL connections to this server. Certificate list.	string	Maximum length: 79	
ssl-dh-bits	Bit-size of Diffie-Hellman.	option	-	2048
	Option Description			
	768	768-bit Diffie-Hellman prime.		
	1024	1024-bit Diffie-Hellman prime.		
	1536	1536-bit Diffie-Hellman prime.		
	2048	2048-bit Diffie-Hellman prime.		
ssl-algorithm	Relative strength of encryption algorithms accepted in negotiation.	option	-	high
	Option Description			
	high	High encryption. Allow only AES and ChaCha		
	medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.		
	low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.		

hardware

This section includes syntax for the following commands:

- [config hardware cpu on page 389](#)
- [config hardware memory on page 389](#)
- [config hardware nic on page 389](#)
- [config hardware status on page 390](#)

config hardware cpu

Display detailed information for all installed CPU(s).

```
config hardware cpu
    Description: Display detailed information for all installed CPU(s).
end
```

config hardware memory

Display system memory information.

```
config hardware memory
    Description: Display system memory information.
end
```

config hardware nic

Display NIC information.

```
config hardware nic
    Description: Display NIC information.
    set <nic> {string}
end
```

config hardware nic

Parameter	Description	Type	Size	Default
<nic>	NIC name.	string	Maximum length: -	

config hardware status

Hardware status.

```
config hardware status
    Description: Hardware status.
end
```

icap

This section includes syntax for the following commands:

- [config icap local-server on page 391](#)
- [config icap profile on page 394](#)
- [config icap remote-server-group on page 402](#)
- [config icap remote-server on page 403](#)

config icap local-server

Configure ICAP local server.

```
config icap local-server
  Description: Configure ICAP local server.
  edit <icap-server-id>
    set status [disable|enable]
    set secure-connection [disable|enable]
    set status-ipv6 [disable|enable]
    set icap-incoming-port {integer}
    set icap-incoming-ssl-port {integer}
    set interface {string}
    set incoming-ip {ipv4-address-any}
    set incoming-ipv6 {ipv6-address}
    set ssl-cert <name1>, <name2>, ...
    set strict-scheme-check [disable|enable]
    set message-preview [disable|enable]
    set srcaddr {string}
    set timeout {integer}
  config icap-service
    Description: Set up services for local ICAP server.
    edit <service-id>
      set name {string}
      set dlp-profile {string}
      set av-profile {string}
      set webfilter-profile {string}
      set image-analyzer-profile {string}
      set profile-protocol-options {string}
      set extension-headers {option1}, {option2}, ...
    next
  end
next
end
```

config icap local-server

Parameter	Description	Type	Size	Default						
icap-server-id	ICAP local server id.	integer	Minimum value: 0 Maximum value: 65535	0						
status	Enable/disable status for icap server network profile.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable the status for ipv4 in network-profile.</td></tr><tr><td>enable</td><td>Enable the status for ipv4 in network-profile.</td></tr></table>	Option	Description	disable	Disable the status for ipv4 in network-profile.	enable	Enable the status for ipv4 in network-profile.			
Option	Description									
disable	Disable the status for ipv4 in network-profile.									
enable	Enable the status for ipv4 in network-profile.									
secure-connection	Enable/disable status for secured icap server network profile.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable the status for ipv4 ssl in network-profile.</td></tr><tr><td>enable</td><td>Enable the status for ipv4 ssl in network-profile.</td></tr></table>	Option	Description	disable	Disable the status for ipv4 ssl in network-profile.	enable	Enable the status for ipv4 ssl in network-profile.			
Option	Description									
disable	Disable the status for ipv4 ssl in network-profile.									
enable	Enable the status for ipv4 ssl in network-profile.									
status-ipv6	Enable/disable status for icap server service ipv6.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable the status for ipv6 in network-profile.</td></tr><tr><td>enable</td><td>Enable the status for ipv6 in network-profile.</td></tr></table>	Option	Description	disable	Disable the status for ipv6 in network-profile.	enable	Enable the status for ipv6 in network-profile.			
Option	Description									
disable	Disable the status for ipv6 in network-profile.									
enable	Enable the status for ipv6 in network-profile.									
icap-incoming-port	Accept incoming ICAP requests on a port.	integer	Minimum value: 1 Maximum value: 65535	1344						
icap-incoming-ssl-port	Accept incoming secured ICAP requests on a port.	integer	Minimum value: 1 Maximum value: 65535	11344						
interface	Interface name	string	Maximum length: 15							
incoming-ip	Restrict the ICAP server to only accept sessions from this IP address. An interface must have this IP address.	ipv4-address-any	Not Specified	0.0.0.0						

Parameter	Description	Type	Size	Default						
incoming-ipv6	Restrict the ICAP server to only accept sessions from this IPv6 address. An interface must have this IPv6 address.	ipv6-address	Not Specified	::						
ssl-cert <name>	SSL certificate for SSL interception. Certificate list.	string	Maximum length: 79							
strict-scheme-check	Enable/disable strict check of scheme.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable strict check of scheme.</td></tr><tr><td><i>enable</i></td><td>Enable strict check of scheme.</td></tr></table>	Option	Description	<i>disable</i>	Disable strict check of scheme.	<i>enable</i>	Enable strict check of scheme.			
Option	Description									
<i>disable</i>	Disable strict check of scheme.									
<i>enable</i>	Enable strict check of scheme.									
message-preview	Enable/disable message preview support. Max preview data length is 4096 bytes.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable message preview support.</td></tr><tr><td><i>enable</i></td><td>Enable message preview support.</td></tr></table>	Option	Description	<i>disable</i>	Disable message preview support.	<i>enable</i>	Enable message preview support.			
Option	Description									
<i>disable</i>	Disable message preview support.									
<i>enable</i>	Enable message preview support.									
srcaddr	Source address name.	string	Maximum length: 79							
timeout	ICAP server idle timeout in seconds.	integer	Minimum value: 30 Maximum value: 3600	300						

config icap-service

Parameter	Description	Type	Size	Default
service-id	ID of the ICAP server service.	integer	Minimum value: 0 Maximum value: 65535	0
name	Name of ICAP service profile.	string	Maximum length: 35	
dlp-profile	Name of an existing DLP profile.	string	Maximum length: 35	
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35	
image-analyzer-profile	Name of an existing Image analyzer profile.	string	Maximum length: 35	
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35	default
extension-headers	Configure the extension headers of icap server response.	option	-	

Option	Description
<i>X-Virus-id</i>	Enable X-Virus-ID ICAP extension header.
<i>X-Infection-Found</i>	Enable X-Infection-Found ICAP extension header.
<i>X-Violation-Found</i>	Enable X-Violation-Found ICAP extension header.

config icap profile

Configure ICAP profiles.

```
config icap profile
  Description: Configure ICAP profiles.
  edit <name>
    set replacemsg-group {string}
    set comment {var-string}
    set request [disable|enable]
    set response [disable|enable]
    set file-transfer {option1}, {option2}, ...
    set streaming-content-bypass [disable|enable]
    set ocr_only [disable|enable]
    set 204-size-limit {integer}
    set 204-response [disable|enable]
    set preview [disable|enable]
    set preview-data-length {integer}
    set request-server {string}
    set response-server {string}
    set file-transfer-server {string}
    set request-failure [error|bypass]
    set response-failure [error|bypass]
    set file-transfer-failure [error|bypass]
    set request-path {string}
    set response-path {string}
    set file-transfer-path {string}
```

```

set methods {option1}, {option2}, ...
set response-req-hdr [disable|enable]
set respmod-default-action [forward|bypass]
set icap-block-log [disable|enable]
set chunk-encap [disable|enable]
set extension-feature {option1}, {option2}, ...
set scan-progress-interval {integer}
set timeout {integer}
set scan-size-limit {integer}
set scan-oversize-log [disable|enable]
config icap-headers
    Description: Configure ICAP forwarded request headers.
    edit <id>
        set name {string}
        set source [content|http-header|...]
        set content {string}
        set http-header {string}
        set session-info-type [client-ip|user|...]
        set base64-encoding [disable|enable]
    next
end
config respmod-forward-rules
    Description: ICAP response mode forward rules.
    edit <name>
        set host {string}
        config header-group
            Description: HTTP header group.
            edit <id>
                set header-name {string}
                set header {string}
                set case-sensitivity [disable|enable]
            next
        end
        set action [forward|bypass]
        set http-resp-status-code <code1>, <code2>, ...
    next
end
next
end

```

config icap profile

Parameter	Description	Type	Size	Default
replacemsg-group	Replacement message group.	string	Maximum length: 35	
name	ICAP profile name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default						
request	Enable/disable whether an HTTP request is passed to an ICAP server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable HTTP request passing to ICAP server.</td></tr><tr><td>enable</td><td>Enable HTTP request passing to ICAP server.</td></tr></table>	Option	Description	disable	Disable HTTP request passing to ICAP server.	enable	Enable HTTP request passing to ICAP server.			
Option	Description									
disable	Disable HTTP request passing to ICAP server.									
enable	Enable HTTP request passing to ICAP server.									
response	Enable/disable whether an HTTP response is passed to an ICAP server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable HTTP response passing to ICAP server.</td></tr><tr><td>enable</td><td>Enable HTTP response passing to ICAP server.</td></tr></table>	Option	Description	disable	Disable HTTP response passing to ICAP server.	enable	Enable HTTP response passing to ICAP server.			
Option	Description									
disable	Disable HTTP response passing to ICAP server.									
enable	Enable HTTP response passing to ICAP server.									
file-transfer	Configure the file transfer protocols to pass transferred files to an ICAP server as REQMOD.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ssh</td><td>Forward file transfer with SSH protocol to ICAP server for further processing.</td></tr><tr><td>ftp</td><td>Forward file transfer with FTP protocol to ICAP server for further processing.</td></tr></table>	Option	Description	ssh	Forward file transfer with SSH protocol to ICAP server for further processing.	ftp	Forward file transfer with FTP protocol to ICAP server for further processing.			
Option	Description									
ssh	Forward file transfer with SSH protocol to ICAP server for further processing.									
ftp	Forward file transfer with FTP protocol to ICAP server for further processing.									
streaming-content-bypass	Enable/disable bypassing of ICAP server for streaming content.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable bypassing of ICAP server for streaming content.</td></tr><tr><td>enable</td><td>Enable bypassing of ICAP server for streaming content.</td></tr></table>	Option	Description	disable	Disable bypassing of ICAP server for streaming content.	enable	Enable bypassing of ICAP server for streaming content.			
Option	Description									
disable	Disable bypassing of ICAP server for streaming content.									
enable	Enable bypassing of ICAP server for streaming content.									
ocr_only	Enable/disable only passing OCR scan request to ICAP server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable only passing OCR scan request to ICAP server.</td></tr><tr><td>enable</td><td>Enable only passing OCR scan request to ICAP server.</td></tr></table>	Option	Description	disable	Disable only passing OCR scan request to ICAP server.	enable	Enable only passing OCR scan request to ICAP server.			
Option	Description									
disable	Disable only passing OCR scan request to ICAP server.									
enable	Enable only passing OCR scan request to ICAP server.									
204-size-limit	Allow 204 size limit to be saved by ICAP client.	integer	Minimum value: 1 Maximum value: 10	1						
204-response	Enable/disable allowance of 204 response from ICAP server.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable allowance of 204 response from ICAP server.		
	<i>enable</i>	Enable allowance of 204 response from ICAP server.		
preview	Enable/disable preview of data to ICAP server.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable preview of data to ICAP server.		
	<i>enable</i>	Enable preview of data to ICAP server.		
preview-data-length	Preview data length to be sent to ICAP server.	integer	Minimum value: 0 Maximum value: 4096	0
request-server	ICAP server to use for an HTTP request.	string	Maximum length: 63	
response-server	ICAP server to use for an HTTP response.	string	Maximum length: 63	
file-transfer-server	ICAP server to use for a file transfer.	string	Maximum length: 63	
request-failure	Action to take if the ICAP server cannot be contacted when processing an HTTP request.	option	-	error
	Option	Description		
	<i>error</i>	Error.		
	<i>bypass</i>	Bypass.		
response-failure	Action to take if the ICAP server cannot be contacted when processing an HTTP response.	option	-	error
	Option	Description		
	<i>error</i>	Error.		
	<i>bypass</i>	Bypass.		
file-transfer-failure	Action to take if the ICAP server cannot be contacted when processing a file transfer.	option	-	error
	Option	Description		
	<i>error</i>	Error.		
	<i>bypass</i>	Bypass.		

Parameter	Description	Type	Size	Default
request-path	Path component of the ICAP URI that identifies the HTTP request processing service.	string	Maximum length: 127	
response-path	Path component of the ICAP URI that identifies the HTTP response processing service.	string	Maximum length: 127	
file-transfer-path	Path component of the ICAP URI that identifies the file transfer processing service.	string	Maximum length: 127	
methods	The allowed HTTP methods that will be sent to ICAP server for further processing.	option	-	delete get head options post put trace connect other

Option	Description
<i>delete</i>	Forward HTTP request or response with DELETE method to ICAP server for further processing.
<i>get</i>	Forward HTTP request or response with GET method to ICAP server for further processing.
<i>head</i>	Forward HTTP request or response with HEAD method to ICAP server for further processing.
<i>options</i>	Forward HTTP request or response with OPTIONS method to ICAP server for further processing.
<i>post</i>	Forward HTTP request or response with POST method to ICAP server for further processing.
<i>put</i>	Forward HTTP request or response with PUT method to ICAP server for further processing.
<i>trace</i>	Forward HTTP request or response with TRACE method to ICAP server for further processing.
<i>connect</i>	Forward HTTP request or response with CONNECT method to ICAP server for further processing.
<i>other</i>	Forward HTTP request or response with All other methods to ICAP server for further processing.

response-req-hdr	Enable/disable addition of req-hdr for ICAP response modification (respmod) processing.	option	-	enable

Option	Description
<i>disable</i>	Do not add req-hdr for response modification (respmod) processing.

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Add req-hdr for response modification (respmod) processing.</td></tr></table>	Option	Description	<i>enable</i>	Add req-hdr for response modification (respmod) processing.					
	Option	Description								
	<i>enable</i>	Add req-hdr for response modification (respmod) processing.								
respmod-default-action	Default action to ICAP response modification (respmod) processing.	option	-	forward						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>forward</i></td><td>Forward response to ICAP server unless a rule specifies not to.</td></tr><tr><td><i>bypass</i></td><td>Don't forward request to ICAP server unless a rule specifies to forward the request.</td></tr></table>	Option	Description	<i>forward</i>	Forward response to ICAP server unless a rule specifies not to.	<i>bypass</i>	Don't forward request to ICAP server unless a rule specifies to forward the request.			
	Option	Description								
	<i>forward</i>	Forward response to ICAP server unless a rule specifies not to.								
<i>bypass</i>	Don't forward request to ICAP server unless a rule specifies to forward the request.									
icap-block-log	Enable/disable UTM log when infection found.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable UTM log when infection found.</td></tr><tr><td><i>enable</i></td><td>Enable UTM log when infection found.</td></tr></table>	Option	Description	<i>disable</i>	Disable UTM log when infection found.	<i>enable</i>	Enable UTM log when infection found.			
	Option	Description								
	<i>disable</i>	Disable UTM log when infection found.								
<i>enable</i>	Enable UTM log when infection found.									
chunk-encap	Enable/disable chunked encapsulation.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not encapsulate chunked data.</td></tr><tr><td><i>enable</i></td><td>Encapsulate chunked data into a new chunk.</td></tr></table>	Option	Description	<i>disable</i>	Do not encapsulate chunked data.	<i>enable</i>	Encapsulate chunked data into a new chunk.			
	Option	Description								
	<i>disable</i>	Do not encapsulate chunked data.								
<i>enable</i>	Encapsulate chunked data into a new chunk.									
extension-feature	Enable/disable ICAP extension features.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>scan-progress</i></td><td>Support X-Scan-Progress-Interval ICAP header.</td></tr></table>	Option	Description	<i>scan-progress</i>	Support X-Scan-Progress-Interval ICAP header.					
	Option	Description								
<i>scan-progress</i>	Support X-Scan-Progress-Interval ICAP header.									
scan-progress-interval	Scan progress interval value.	integer	Minimum value: 5 Maximum value: 30	10						
timeout	Time (in seconds) that ICAP client waits for the response from ICAP server.	integer	Minimum value: 30 Maximum value: 3600	30						
scan-size-limit	ICAP server scan size limit for an single request.	integer	Minimum value: 0 Maximum value: 4096	0						

Parameter	Description	Type	Size	Default
scan-oversize-log	Enable/disable scan oversize log.	option	-	enable
	Option Description			
	<i>disable</i>	Disable scan oversize log.		
	<i>enable</i>	Enable scan oversize log.		

config icap-headers

Parameter	Description	Type	Size	Default
id	HTTP forwarded header ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	HTTP forwarded header name.	string	Maximum length: 79	
source	HTTP append header source.	option	-	content
	Option Description			
	<i>content</i>	Create ICAP header from content.		
	<i>http-header</i>	Create ICAP header from HTTP header.		
	<i>session</i>	Create ICAP header from session info.		
content	HTTP header content.	string	Maximum length: 255	
http-header	HTTP header-field name.	string	Maximum length: 79	
session-info-type	Session info type.	option	-	client-ip
	Option Description			
	<i>client-ip</i>	Client ip address.		
	<i>user</i>	Authentication user name.		
	<i>upn</i>	Authentication user principal name.		
	<i>domain</i>	User domain name.		
	<i>local-grp</i>	Firewall group name.		

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>remote-grp</i></td><td>Group name from authentication server.</td></tr><tr><td><i>proxy-name</i></td><td>Proxy realm name.</td></tr><tr><td><i>auth-user-uri</i></td><td>Authenticated user uri.</td></tr><tr><td><i>auth-group-uri</i></td><td>Authenticated group uri.</td></tr></table>				Option	Description	<i>remote-grp</i>	Group name from authentication server.	<i>proxy-name</i>	Proxy realm name.	<i>auth-user-uri</i>	Authenticated user uri.	<i>auth-group-uri</i>	Authenticated group uri.
	Option	Description												
	<i>remote-grp</i>	Group name from authentication server.												
	<i>proxy-name</i>	Proxy realm name.												
	<i>auth-user-uri</i>	Authenticated user uri.												
<i>auth-group-uri</i>	Authenticated group uri.													
base64-encoding	Enable/disable use of base64 encoding of HTTP content.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use of base64 encoding of HTTP content.</td></tr><tr><td><i>enable</i></td><td>Enable use of base64 encoding of HTTP content.</td></tr></table>				Option	Description	<i>disable</i>	Disable use of base64 encoding of HTTP content.	<i>enable</i>	Enable use of base64 encoding of HTTP content.				
	Option	Description												
	<i>disable</i>	Disable use of base64 encoding of HTTP content.												
<i>enable</i>	Enable use of base64 encoding of HTTP content.													

config respmod-forward-rules

Parameter	Description	Type	Size	Default						
name	Address name.	string	Maximum length: 63							
host	Address object for the host.	string	Maximum length: 79							
action	Action to be taken for ICAP server.	option	-	forward						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>forward</i></td><td>Forward request to ICAP server when this rule is matched.</td></tr><tr><td><i>bypass</i></td><td>Don't forward request to ICAP server when this rule is matched.</td></tr></table>				Option	Description	<i>forward</i>	Forward request to ICAP server when this rule is matched.	<i>bypass</i>	Don't forward request to ICAP server when this rule is matched.
Option	Description									
<i>forward</i>	Forward request to ICAP server when this rule is matched.									
<i>bypass</i>	Don't forward request to ICAP server when this rule is matched.									
http-resp-status-code <code>	HTTP response status code. HTTP response status code.	integer	Minimum value: 100 Maximum value: 599							

config header-group

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
header-name	HTTP header.	string	Maximum length: 79	
header	HTTP header regular expression.	string	Maximum length: 255	
case-sensitivity	Enable/disable case sensitivity when matching header.	option	-	disable
	Option	Description		
	disable	Ignore case when matching header.		
	enable	Do not ignore case when matching header.		

config icap remote-server-group

Configure an ICAP remote server group consisting of multiple forward servers. Supports failover and load balancing.

```
config icap remote-server-group
    Description: Configure an ICAP remote server group consisting of multiple forward
servers. Supports failover and load balancing.
    edit <name>
        set ldb-method [weighted|least-session|...]
        config server-list
            Description: Add ICAP remote servers to a list to form a server group.
Optionally assign weights to each server.
            edit <name>
                set weight {integer}
            next
        end
    next
end
```

config icap remote-server-group

Parameter	Description	Type	Size	Default								
name	Configure an ICAP remote server group consisting one or multiple forward servers. Supports failover and load balancing.	string	Maximum length: 63									
ldb-method	Load balance method.	option	-	weighted								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>weighted</i></td><td>Load balance traffic to forward servers based on assigned weights.</td></tr><tr><td><i>least-session</i></td><td>Send new sessions to the server with lowest session count.</td></tr><tr><td><i>active-passive</i></td><td>Send new sessions to active server with high weight.</td></tr></table>				Option	Description	<i>weighted</i>	Load balance traffic to forward servers based on assigned weights.	<i>least-session</i>	Send new sessions to the server with lowest session count.	<i>active-passive</i>	Send new sessions to active server with high weight.
Option	Description											
<i>weighted</i>	Load balance traffic to forward servers based on assigned weights.											
<i>least-session</i>	Send new sessions to the server with lowest session count.											
<i>active-passive</i>	Send new sessions to active server with high weight.											

config server-list

Parameter	Description	Type	Size	Default
name	ICAP remote server name.	string	Maximum length: 63	
weight	Optionally assign a weight of the forwarding server for weighted load balancing.	integer	Minimum value: 1 Maximum value: 100	10

config icap remote-server

Configure ICAP servers.

```

config icap remote-server
  Description: Configure ICAP servers.
  edit <name>
    set addr-type [ip4|ip6|...]
    set ip-address {ipv4-address-any}
    set ip6-address {ipv6-address}
    set fqdn {string}
    set secure [disable|enable]
    set port {integer}
    set max-connections {integer}
    set ssl-cert {string}
    set healthcheck [disable|enable]
    set healthcheck-service {string}
  next
end

```

config icap remote-server

Parameter	Description	Type	Size	Default
name	Server name.	string	Maximum length: 63	
addr-type	Address type of the remote ICAP server: IPv4, IPv6 or FQDN.	option	-	ip4
	Option	Description		
	<i>ip4</i>	Use an IPv4 address for the remote ICAP server.		
	<i>ip6</i>	Use an IPv6 address for the remote ICAP server.		
	<i>fqdn</i>	Use the FQDN for the remote ICAP server.		
ip-address	IPv4 address of the ICAP server.	ipv4-address-any	Not Specified	0.0.0.0
ip6-address	IPv6 address of the ICAP server.	ipv6-address	Not Specified	::
fqdn	ICAP remote server Fully Qualified Domain Name (FQDN).	string	Maximum length: 255	
secure	Enable/disable secure connection to ICAP server.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable connection to secure ICAP server.		
	<i>enable</i>	Enable connection to secure ICAP server.		
port	ICAP server port.	integer	Minimum value: 1 Maximum value: 65535	1344
max-connections	Maximum number of concurrent connections to ICAP server. Must not be less than wad-worker-count.	integer	Minimum value: 0 Maximum value: 4294967295	100
ssl-cert	CA certificate name.	string	Maximum length: 79	
healthcheck	Enable/disable ICAP remote server health checking. Attempts to connect to the remote ICAP server to verify that the server is operating normally.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable health checking.		
	<i>enable</i>	Enable health checking.		
healthcheck-service	ICAP Service name to use for health checks.	string	Maximum length: 127	

image-analyzer

This section includes syntax for the following commands:

- [config image-analyzer profile on page 406](#)

config image-analyzer profile

Configure image analyzer profiles

```
config image-analyzer profile
  Description: Configure image analyzer profiles
  edit <name>
    set comment {var-string}
    set alcohol-block-strictness-level {integer}
    set alcohol-status [allow|deny|...]
    set drugs-block-strictness-level {integer}
    set drugs-status [allow|deny|...]
    set extremism-block-strictness-level {integer}
    set extremism-status [allow|deny|...]
    set gambling-block-strictness-level {integer}
    set gambling-status [allow|deny|...]
    set gore-block-strictness-level {integer}
    set gore-status [allow|deny|...]
    set porn-block-strictness-level {integer}
    set porn-status [allow|deny|...]
    set swim_underwear-block-strictness-level {integer}
    set swim_underwear-status [allow|deny|...]
    set weapons-block-strictness-level {integer}
    set weapons-status [allow|deny|...]
    set image-skip-size {integer}
    set image-skip-width {integer}
    set image-skip-height {integer}
    set log-option [all|violation]
    set source-url [enable|disable]
    set blocked-img-cache [enable|disable]
    set rating-err-action [block|pass]
    set replace-image {string}
    set optical-character-recognition [enable|disable]
    set ocr-activation-threshold {integer}
  next
end
```

config image-analyzer profile

Parameter	Description	Type	Size	Default
name	Profile name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
alcohol-block-strictness-level	Higher value means an image is more likely to be blocked.	integer	Minimum value: 0 Maximum value: 100	30
alcohol-status	Allow/deny/monitor the category image.	option	-	deny
	Option	Description		
	<i>allow</i>	Allow the category image.		
	<i>deny</i>	Deny the category image.		
	<i>monitor</i>	Monitor the category image.		
drugs-block-strictness-level	Higher value means an image is more likely to be blocked.	integer	Minimum value: 0 Maximum value: 100	30
drugs-status	Allow/deny/monitor the category image.	option	-	deny
	Option	Description		
	<i>allow</i>	Allow the category image.		
	<i>deny</i>	Deny the category image.		
	<i>monitor</i>	Monitor the category image.		
extremism-block-strictness-level	Higher value means an image is more likely to be blocked.	integer	Minimum value: 0 Maximum value: 100	30
extremism-status	Allow/deny/monitor the category image.	option	-	deny
	Option	Description		
	<i>allow</i>	Allow the category image.		
	<i>deny</i>	Deny the category image.		
	<i>monitor</i>	Monitor the category image.		

Parameter	Description	Type	Size	Default								
gambling-block-strictness-level	Higher value means an image is more likely to be blocked.	integer	Minimum value: 0 Maximum value: 100	30								
gambling-status	Allow/deny/monitor the category image.	option	-	deny								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the category image.</td></tr><tr><td><i>deny</i></td><td>Deny the category image.</td></tr><tr><td><i>monitor</i></td><td>Monitor the category image.</td></tr></table>	Option	Description	<i>allow</i>	Allow the category image.	<i>deny</i>	Deny the category image.	<i>monitor</i>	Monitor the category image.			
Option	Description											
<i>allow</i>	Allow the category image.											
<i>deny</i>	Deny the category image.											
<i>monitor</i>	Monitor the category image.											
gore-block-strictness-level	Higher value means an image is more likely to be blocked.	integer	Minimum value: 0 Maximum value: 100	30								
gore-status	Allow/deny/monitor the category image.	option	-	deny								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the category image.</td></tr><tr><td><i>deny</i></td><td>Deny the category image.</td></tr><tr><td><i>monitor</i></td><td>Monitor the category image.</td></tr></table>	Option	Description	<i>allow</i>	Allow the category image.	<i>deny</i>	Deny the category image.	<i>monitor</i>	Monitor the category image.			
Option	Description											
<i>allow</i>	Allow the category image.											
<i>deny</i>	Deny the category image.											
<i>monitor</i>	Monitor the category image.											
porn-block-strictness-level	Higher value means an image is more likely to be blocked.	integer	Minimum value: 0 Maximum value: 100	30								
porn-status	Allow/deny/monitor the category image.	option	-	deny								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the category image.</td></tr><tr><td><i>deny</i></td><td>Deny the category image.</td></tr><tr><td><i>monitor</i></td><td>Monitor the category image.</td></tr></table>	Option	Description	<i>allow</i>	Allow the category image.	<i>deny</i>	Deny the category image.	<i>monitor</i>	Monitor the category image.			
Option	Description											
<i>allow</i>	Allow the category image.											
<i>deny</i>	Deny the category image.											
<i>monitor</i>	Monitor the category image.											
swim_underwear-block-strictness-level	Higher value means an image is more likely to be blocked.	integer	Minimum value: 0 Maximum value: 100	30								

Parameter	Description	Type	Size	Default								
swim_underwear-status	Allow/deny/monitor the category image.	option	-	deny								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the category image.</td></tr><tr><td><i>deny</i></td><td>Deny the category image.</td></tr><tr><td><i>monitor</i></td><td>Monitor the category image.</td></tr></table>	Option	Description	<i>allow</i>	Allow the category image.	<i>deny</i>	Deny the category image.	<i>monitor</i>	Monitor the category image.			
Option	Description											
<i>allow</i>	Allow the category image.											
<i>deny</i>	Deny the category image.											
<i>monitor</i>	Monitor the category image.											
weapons-block-strictness-level	Higher value means an image is more likely to be blocked.	integer	Minimum value: 0 Maximum value: 100	30								
weapons-status	Allow/deny/monitor the category image.	option	-	deny								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the category image.</td></tr><tr><td><i>deny</i></td><td>Deny the category image.</td></tr><tr><td><i>monitor</i></td><td>Monitor the category image.</td></tr></table>	Option	Description	<i>allow</i>	Allow the category image.	<i>deny</i>	Deny the category image.	<i>monitor</i>	Monitor the category image.			
Option	Description											
<i>allow</i>	Allow the category image.											
<i>deny</i>	Deny the category image.											
<i>monitor</i>	Monitor the category image.											
image-skip-size	Image skip rating size.	integer	Minimum value: 0 Maximum value: 2048	1								
image-skip-width	Image skip rating width(min. 5 pixel).	integer	Minimum value: 5 Maximum value: 2147483647	30								
image-skip-height	Image skip rating height(min. 5 pixel).	integer	Minimum value: 5 Maximum value: 2147483647	30								
log-option	Log option for the inspected image result.	option	-	violation								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Log all image result.</td></tr><tr><td><i>violation</i></td><td>Log only violation image result.</td></tr></table>	Option	Description	<i>all</i>	Log all image result.	<i>violation</i>	Log only violation image result.					
Option	Description											
<i>all</i>	Log all image result.											
<i>violation</i>	Log only violation image result.											

Parameter	Description	Type	Size	Default
source-url	Enable/disable source url in the image search result.	option	-	enable
	Option Description			
	<i>enable</i>	Enable source url in image search.		
	<i>disable</i>	Disable source url in image search.		
blocked-img-cache	Enable/disable saving blocked images in ram disk.	option	-	disable
	Option Description			
	<i>enable</i>	Enable caching.		
	<i>disable</i>	Disable caching.		
rating-err-action	Actions when image rating error.	option	-	pass
	Option Description			
	<i>block</i>	Block.		
	<i>pass</i>	Pass.		
replace-image	Specify replacement image.	string	Maximum length: 35	
optical-character-recognition	Enable/disable optical character recognition.	option	-	disable
	Option Description			
	<i>enable</i>	Enable optical character recognition.		
	<i>disable</i>	Disable optical character recognition.		
ocr-activation-threshold	Threshold to activate optical character recognition.	integer	Minimum value: 0 Maximum value: 100	30

ips

This section includes syntax for the following commands:

- [config ips custom on page 411](#)
- [config ips decoder on page 413](#)
- [config ips global on page 413](#)
- [config ips rule-settings on page 417](#)
- [config ips rule on page 417](#)
- [config ips sensor on page 419](#)
- [config ips session on page 425](#)
- [config ips settings on page 425](#)
- [config ips view-map on page 426](#)

config ips custom

Configure IPS custom signature.

```
config ips custom
  Description: Configure IPS custom signature.
  edit <tag>
    set signature {var-string}
    set rule-id {integer}
    set severity {user}
    set location {user}
    set os {user}
    set application {user}
    set protocol {user}
    set status [disable|enable]
    set log [disable|enable]
    set log-packet [disable|enable]
    set action [pass|block]
    set comment {string}
  next
end
```

config ips custom

Parameter	Description	Type	Size	Default
tag	Signature tag.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default						
signature	Custom signature enclosed in single quotes.	var-string	Maximum length: 4095							
rule-id	Signature ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
severity	Relative severity of the signature, from info to critical. Log messages generated by the signature include the severity.	user	Not Specified							
location	Protect client or server traffic.	user	Not Specified							
os	Operating system(s) that the signature protects. Blank for all operating systems.	user	Not Specified							
application	Applications to be protected. Blank for all applications.	user	Not Specified							
protocol	Protocol(s) that the signature scans. Blank for all protocols.	user	Not Specified							
status	Enable/disable this signature.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable status.</td></tr><tr><td>enable</td><td>Enable status.</td></tr></table>				Option	Description	disable	Disable status.	enable	Enable status.
Option	Description									
disable	Disable status.									
enable	Enable status.									
log	Enable/disable logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable logging.</td></tr><tr><td>enable</td><td>Enable logging.</td></tr></table>				Option	Description	disable	Disable logging.	enable	Enable logging.
Option	Description									
disable	Disable logging.									
enable	Enable logging.									
log-packet	Enable/disable packet logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable packet logging.</td></tr><tr><td>enable</td><td>Enable packet logging.</td></tr></table>				Option	Description	disable	Disable packet logging.	enable	Enable packet logging.
Option	Description									
disable	Disable packet logging.									
enable	Enable packet logging.									
action	Default action (pass or block) for this signature.	option	-	pass						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>pass</td><td>Pass or allow matching traffic.</td></tr></table>				Option	Description	pass	Pass or allow matching traffic.		
Option	Description									
pass	Pass or allow matching traffic.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>block</i>	Block or drop matching traffic.		
comment	Comment.	string	Maximum length: 63	

config ips decoder

Configure IPS decoder.

```
config ips decoder
  Description: Configure IPS decoder.
  edit <name>
    config parameter
      Description: IPS group parameters.
      edit <name>
        set value {string}
      next
    end
  next
end
```

config ips decoder

Parameter	Description	Type	Size	Default
name	Decoder name.	string	Maximum length: 63	

config parameter

Parameter	Description	Type	Size	Default
name	Parameter name.	string	Maximum length: 31	
value	Parameter value.	string	Maximum length: 199	

config ips global

Configure IPS global parameter.

```

config ips global
    Description: Configure IPS global parameter.
    set fail-open [enable|disable]
    set database [regular|extended]
    set traffic-submit [enable|disable]
    set anomaly-mode [periodical|continuous]
    set session-limit-mode [accurate|heuristic]
    set socket-size {integer}
    set engine-count {integer}
    set sync-session-ttl [enable|disable]
    set deep-app-insp-timeout {integer}
    set deep-app-insp-db-limit {integer}
    set exclude-signatures [none|industrial]
    set packet-log-queue-depth {integer}
    config tls-active-probe
        Description: TLS active probe configuration.
        set interface-select-method [auto|sdwan|...]
        set interface {string}
        set vdom {string}
        set source-ip {ipv4-address}
        set source-ip6 {ipv6-address}
    end
end

```

config ips global

Parameter	Description	Type	Size	Default						
fail-open	Enable to allow traffic if the IPS buffer is full. Default is disable and IPS traffic is blocked when the IPS buffer is full.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS fail open.</td></tr><tr><td><i>disable</i></td><td>Disable IPS fail open.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPS fail open.	<i>disable</i>	Disable IPS fail open.			
Option	Description									
<i>enable</i>	Enable IPS fail open.									
<i>disable</i>	Disable IPS fail open.									
database	Regular or extended IPS database. Regular protects against the latest common and in-the-wild attacks. Extended includes protection from legacy attacks.	option	-	extended						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>regular</i></td><td>IPS regular database package.</td></tr><tr><td><i>extended</i></td><td>IPS extended database package.</td></tr></table>	Option	Description	<i>regular</i>	IPS regular database package.	<i>extended</i>	IPS extended database package.			
Option	Description									
<i>regular</i>	IPS regular database package.									
<i>extended</i>	IPS extended database package.									
traffic-submit	Enable/disable submitting attack data found by this FortiProxy to FortiGuard.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable traffic submit.		
	<i>disable</i>	Disable traffic submit.		
anomaly-mode	Global blocking mode for rate-based anomalies.	option	-	continuous
	Option	Description		
	<i>periodical</i>	After an anomaly is detected, allow the number of packets per second according to the anomaly configuration.		
	<i>continuous</i>	Block packets once an anomaly is detected. Overrides individual anomaly settings.		
session-limit-mode	Method of counting concurrent sessions used by session limit anomalies. Choose between greater accuracy (accurate) or improved performance (heuristics).	option	-	heuristic
	Option	Description		
	<i>accurate</i>	Accurately count concurrent sessions, demands more resources.		
	<i>heuristic</i>	Use heuristics to estimate the number of concurrent sessions. Acceptable in most cases.		
socket-size	IPS socket buffer size. Max and default value depend on available memory. Can be changed to tune performance.	integer	Minimum value: 0 Maximum value: 128	64
engine-count	Number of IPS engines running. If set to the default value of 0, FortiProxy sets the number to optimize performance depending on the number of CPU cores.	integer	Minimum value: 0 Maximum value: 255	0
sync-session-ttl	Enable/disable use of kernel session TTL for IPS sessions.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable use of kernel session TTL for IPS sessions.		
	<i>disable</i>	Disable use of kernel session TTL for IPS sessions.		

Parameter	Description	Type	Size	Default						
deep-app-insp-timeout	Timeout for Deep application inspection.	integer	Minimum value: 0 Maximum value: 2147483647	0						
deep-app-insp-db-limit	Limit on number of entries in deep application inspection database.	integer	Minimum value: 0 Maximum value: 2147483647	0						
exclude-signatures	Excluded signatures.	option	-	industrial						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No signatures excluded.</td></tr><tr><td><i>industrial</i></td><td>Exclude industrial signatures.</td></tr></table>				Option	Description	<i>none</i>	No signatures excluded.	<i>industrial</i>	Exclude industrial signatures.
	Option	Description								
	<i>none</i>	No signatures excluded.								
<i>industrial</i>	Exclude industrial signatures.									
packet-log-queue-depth	Packet/pcap log queue depth per IPS engine.	integer	Minimum value: 128 Maximum value: 4096	128						

config tls-active-probe

Parameter	Description	Type	Size	Default
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
vdom	Virtual domain name for TLS active probe.	string	Maximum length: 31	
source-ip	Source IP address used for TLS active probe.	ipv4-address	Not Specified	0.0.0.0
source-ip6	Source IPv6 address used for TLS active probe.	ipv6-address	Not Specified	::

config ips rule-settings

Configure IPS rule setting.

```
config ips rule-settings
    Description: Configure IPS rule setting.
    edit <id>
        next
    end
```

config ips rule-settings

Parameter	Description	Type	Size	Default
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config ips rule

Configure IPS rules.

```
config ips rule
    Description: Configure IPS rules.
    edit <name>
        set log [disable|enable]
        set log-packet [disable|enable]
        set action [pass|block]
        set group {string}
        set severity {user}
        set location {user}
        set os {user}
        set application {user}
        set service {user}
        set rule-id {integer}
        set rev {integer}
        set date {integer}
        config metadata
            Description: Meta data.
            edit <id>
                set metaid {integer}
                set valueid {integer}
            next
        end
    next
end
```

config ips rule

Parameter	Description	Type	Size	Default						
name	Rule name.	string	Maximum length: 63							
log	Enable/disable logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging.</td></tr><tr><td><i>enable</i></td><td>Enable logging.</td></tr></table>				Option	Description	<i>disable</i>	Disable logging.	<i>enable</i>	Enable logging.
	Option	Description								
	<i>disable</i>	Disable logging.								
<i>enable</i>	Enable logging.									
log-packet	Enable/disable packet logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable packet logging.</td></tr><tr><td><i>enable</i></td><td>Enable packet logging.</td></tr></table>				Option	Description	<i>disable</i>	Disable packet logging.	<i>enable</i>	Enable packet logging.
	Option	Description								
	<i>disable</i>	Disable packet logging.								
<i>enable</i>	Enable packet logging.									
action	Action.	option	-	pass						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Pass or allow matching traffic.</td></tr><tr><td><i>block</i></td><td>Block or drop matching traffic.</td></tr></table>				Option	Description	<i>pass</i>	Pass or allow matching traffic.	<i>block</i>	Block or drop matching traffic.
	Option	Description								
	<i>pass</i>	Pass or allow matching traffic.								
<i>block</i>	Block or drop matching traffic.									
group	Group.	string	Maximum length: 63							
severity	Severity.	user	Not Specified							
location	Vulnerable location.	user	Not Specified							
os	Vulnerable operation systems.	user	Not Specified							
application	Vulnerable applications.	user	Not Specified							
service	Vulnerable service.	user	Not Specified							
rule-id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
rev	Revision.	integer	Minimum value: 0 Maximum value: 4294967295	0						

Parameter	Description	Type	Size	Default
date	Date.	integer	Minimum value: 0 Maximum value: 4294967295	0

config metadata

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
metaid	Meta ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
valueid	Value ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config ips sensor

Configure IPS sensor.

```
config ips sensor
  Description: Configure IPS sensor.
  edit <name>
    set comment {var-string}
    set replacemsg-group {string}
    set block-malicious-url [disable|enable]
    set scan-botnet-connections [disable|block|...]
    set extended-log [enable|disable]
    config entries
      Description: IPS sensor filter.
      edit <id>
        set rule <id1>, <id2>, ...
        set location {user}
        set severity {user}
        set protocol {user}
```

```

set os {user}
set application {user}
set default-action [all|pass|...]
set default-status [all|enable|...]
set cve <cve-entry1>, <cve-entry2>, ...
set vuln-type <id1>, <id2>, ...
set last-modified {user}
set status [disable|enable|...]
set log [disable|enable]
set log-packet [disable|enable]
set log-attack-context [disable|enable]
set action [pass|block|...]
set rate-count {integer}
set rate-duration {integer}
set rate-mode [periodical|continuous]
set rate-track [none|src-ip|...]
config exempt-ip
    Description: Traffic from selected source or destination IP addresses is
exempt from this signature.
    edit <id>
        set src-ip {ipv4-classnet}
        set dst-ip {ipv4-classnet}
    next
end
set quarantine [none|attacker]
set quarantine-expiry {user}
set quarantine-log [disable|enable]
next
end
next
end

```

config ips sensor

Parameter	Description	Type	Size	Default
name	Sensor name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
replacemsg-group	Replacement message group.	string	Maximum length: 35	
block-malicious-url	Enable/disable malicious URL blocking.	option	-	disable
		Option	Description	
		<i>disable</i>	Disable malicious URL blocking.	
		<i>enable</i>	Enable malicious URL blocking.	

Parameter	Description	Type	Size	Default								
scan-botnet-connections	Block or monitor connections to Botnet servers, or disable Botnet scanning.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not scan connections to botnet servers.</td></tr><tr><td><i>block</i></td><td>Block connections to botnet servers.</td></tr><tr><td><i>monitor</i></td><td>Log connections to botnet servers.</td></tr></table>	Option	Description	<i>disable</i>	Do not scan connections to botnet servers.	<i>block</i>	Block connections to botnet servers.	<i>monitor</i>	Log connections to botnet servers.			
Option	Description											
<i>disable</i>	Do not scan connections to botnet servers.											
<i>block</i>	Block connections to botnet servers.											
<i>monitor</i>	Log connections to botnet servers.											
extended-log	Enable/disable extended logging.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											

config entries

Parameter	Description	Type	Size	Default
id	Rule ID in IPS database.	integer	Minimum value: 0 Maximum value: 4294967295	0
rule <id>	Identifies the predefined or custom IPS signatures to add to the sensor. Rule IPS.	integer	Minimum value: 0 Maximum value: 4294967295	
location	Protect client or server traffic.	user	Not Specified	all
severity	Relative severity of the signature, from info to critical. Log messages generated by the signature include the severity.	user	Not Specified	all
protocol	Protocols to be examined. Use all for every protocol and other for unlisted protocols.	user	Not Specified	all
os	Operating systems to be protected. Use all for every operating system and other for unlisted operating systems.	user	Not Specified	all
application	Operating systems to be protected. Use all for every application and other for unlisted application.	user	Not Specified	all
default-action	Signature default action filter.	option	-	all

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Selects signatures with any default action.</td></tr><tr><td><i>pass</i></td><td>Selects signatures with default action 'pass'.</td></tr><tr><td><i>block</i></td><td>Selects signatures with default action 'block'.</td></tr></table>	Option	Description	<i>all</i>	Selects signatures with any default action.	<i>pass</i>	Selects signatures with default action 'pass'.	<i>block</i>	Selects signatures with default action 'block'.			
	Option	Description										
	<i>all</i>	Selects signatures with any default action.										
	<i>pass</i>	Selects signatures with default action 'pass'.										
<i>block</i>	Selects signatures with default action 'block'.											
default-status	Signature default status filter.	option	-	all								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Selects signatures with any default status.</td></tr><tr><td><i>enable</i></td><td>Selects signatures enabled by default.</td></tr><tr><td><i>disable</i></td><td>Selects signatures disabled by default.</td></tr></table>	Option	Description	<i>all</i>	Selects signatures with any default status.	<i>enable</i>	Selects signatures enabled by default.	<i>disable</i>	Selects signatures disabled by default.			
	Option	Description										
	<i>all</i>	Selects signatures with any default status.										
	<i>enable</i>	Selects signatures enabled by default.										
<i>disable</i>	Selects signatures disabled by default.											
cve <cve-entry>	List of CVE IDs of the signatures to add to the sensor. CVE IDs or CVE wildcards.	string	Maximum length: 19									
vuln-type <id>	List of signature vulnerability types to filter by. Vulnerability type ID.	integer	Minimum value: 0 Maximum value: 4294967295									
last-modified	Filter by signature last modified date. Formats: before <date>, after <date>, between <start-date> <end-date>.	user	Not Specified									
status	Status of the signatures included in filter. Only those filters with a status to enable are used.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status of selected rules.</td></tr><tr><td><i>enable</i></td><td>Enable status of selected rules.</td></tr><tr><td><i>default</i></td><td>Default.</td></tr></table>	Option	Description	<i>disable</i>	Disable status of selected rules.	<i>enable</i>	Enable status of selected rules.	<i>default</i>	Default.			
	Option	Description										
	<i>disable</i>	Disable status of selected rules.										
	<i>enable</i>	Enable status of selected rules.										
<i>default</i>	Default.											
log	Enable/disable logging of signatures included in filter.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging of selected rules.</td></tr><tr><td><i>enable</i></td><td>Enable logging of selected rules.</td></tr></table>	Option	Description	<i>disable</i>	Disable logging of selected rules.	<i>enable</i>	Enable logging of selected rules.					
	Option	Description										
	<i>disable</i>	Disable logging of selected rules.										
<i>enable</i>	Enable logging of selected rules.											

Parameter	Description	Type	Size	Default										
log-packet	Enable/disable packet logging. Enable to save the packet that triggers the filter. You can download the packets in pcap format for diagnostic use.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable packet logging of selected rules.</td></tr><tr><td><i>enable</i></td><td>Enable packet logging of selected rules.</td></tr></table>	Option	Description	<i>disable</i>	Disable packet logging of selected rules.	<i>enable</i>	Enable packet logging of selected rules.							
Option	Description													
<i>disable</i>	Disable packet logging of selected rules.													
<i>enable</i>	Enable packet logging of selected rules.													
log-attack-context	Enable/disable logging of attack context: URL buffer, header buffer, body buffer, packet buffer.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging of detailed attack context.</td></tr><tr><td><i>enable</i></td><td>Enable logging of detailed attack context.</td></tr></table>	Option	Description	<i>disable</i>	Disable logging of detailed attack context.	<i>enable</i>	Enable logging of detailed attack context.							
Option	Description													
<i>disable</i>	Disable logging of detailed attack context.													
<i>enable</i>	Enable logging of detailed attack context.													
action	Action taken with traffic in which signatures are detected.	option	-	default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Pass or allow matching traffic.</td></tr><tr><td><i>block</i></td><td>Block or drop matching traffic.</td></tr><tr><td><i>reset</i></td><td>Reset sessions for matching traffic.</td></tr><tr><td><i>default</i></td><td>Pass or drop matching traffic, depending on the default action of the signature.</td></tr></table>	Option	Description	<i>pass</i>	Pass or allow matching traffic.	<i>block</i>	Block or drop matching traffic.	<i>reset</i>	Reset sessions for matching traffic.	<i>default</i>	Pass or drop matching traffic, depending on the default action of the signature.			
Option	Description													
<i>pass</i>	Pass or allow matching traffic.													
<i>block</i>	Block or drop matching traffic.													
<i>reset</i>	Reset sessions for matching traffic.													
<i>default</i>	Pass or drop matching traffic, depending on the default action of the signature.													
rate-count	Count of the rate.	integer	Minimum value: 0 Maximum value: 65535	0										
rate-duration	Duration (sec) of the rate.	integer	Minimum value: 1 Maximum value: 65535	60										
rate-mode	Rate limit mode.	option	-	continuous										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>periodical</i></td><td>Allow configured number of packets every rate-duration.</td></tr><tr><td><i>continuous</i></td><td>Block packets once the rate is reached.</td></tr></table>	Option	Description	<i>periodical</i>	Allow configured number of packets every rate-duration.	<i>continuous</i>	Block packets once the rate is reached.							
Option	Description													
<i>periodical</i>	Allow configured number of packets every rate-duration.													
<i>continuous</i>	Block packets once the rate is reached.													
rate-track	Track the packet protocol field.	option	-	none										

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>none</td></tr><tr><td><i>src-ip</i></td><td>Source IP.</td></tr><tr><td><i>dest-ip</i></td><td>Destination IP.</td></tr><tr><td><i>dhcp-client-mac</i></td><td>DHCP client.</td></tr><tr><td><i>dns-domain</i></td><td>DNS domain.</td></tr></table>	Option	Description	<i>none</i>	none	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.	<i>dhcp-client-mac</i>	DHCP client.	<i>dns-domain</i>	DNS domain.			
	Option	Description														
	<i>none</i>	none														
	<i>src-ip</i>	Source IP.														
	<i>dest-ip</i>	Destination IP.														
	<i>dhcp-client-mac</i>	DHCP client.														
<i>dns-domain</i>	DNS domain.															
quarantine	Quarantine method.	option	-	none												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Quarantine is disabled.</td></tr><tr><td><i>attacker</i></td><td>Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.</td></tr></table>	Option	Description	<i>none</i>	Quarantine is disabled.	<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.									
	Option	Description														
	<i>none</i>	Quarantine is disabled.														
<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.															
quarantine-expiry	Duration of quarantine. Requires quarantine set to attacker.	user	Not Specified	5m												
quarantine-log	Enable/disable quarantine logging.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable quarantine logging.</td></tr><tr><td><i>enable</i></td><td>Enable quarantine logging.</td></tr></table>	Option	Description	<i>disable</i>	Disable quarantine logging.	<i>enable</i>	Enable quarantine logging.									
	Option	Description														
	<i>disable</i>	Disable quarantine logging.														
<i>enable</i>	Enable quarantine logging.															

config exempt-ip

Parameter	Description	Type	Size	Default
id	Exempt IP ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
src-ip	Source IP address and netmask (applies to packet matching the signature).	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
dst-ip	Destination IP address and netmask (applies to packet matching the signature).	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

config ips session

Session status.

```
config ips session
    Description: Session status.
end
```

config ips settings

Configure IPS VDOM parameter.

```
config ips settings
    Description: Configure IPS VDOM parameter.
    set packet-log-history {integer}
    set packet-log-post-attack {integer}
    set packet-log-memory {integer}
    set ips-packet-quota {integer}
    set proxy-inline-ips [disable|enable]
end
```

config ips settings

Parameter	Description	Type	Size	Default
packet-log-history	Number of packets to capture before and including the one in which the IPS signature is detected.	integer	Minimum value: 1 Maximum value: 255	1
packet-log-post-attack	Number of packets to log after the IPS signature is detected.	integer	Minimum value: 0 Maximum value: 255	0
packet-log-memory	Maximum memory can be used by packet log.	integer	Minimum value: 64 Maximum value: 8192	256
ips-packet-quota	Maximum amount of disk space in MB for logged packets when logging to disk. Range depends on disk size.	integer	Minimum value: 0 Maximum value: 4294967295	0
proxy-inline-ips	Enable/disable firewall policy inline IPS support.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Do not allow inline IPS in firewall policy.		
	<i>enable</i>	Allow inline IPS in firewall policy.		

config ips view-map

Configure IPS view-map.

```
config ips view-map
  Description: Configure IPS view-map.
  edit <id>
    set vdom-id {integer}
    set policy-id {integer}
    set id-policy-id {integer}
    set which {option}
  next
end
```

config ips view-map

Parameter	Description	Type	Size	Default
id	View ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
vdom-id	VDOM ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
policy-id	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
id-policy-id	ID-based policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
which	Policy.	option	-	firewall
		Option	Description	
		<i>firewall</i>	Firewall policy.	

ipsec

This section includes syntax for the following commands:

- [config ipsec tunnel on page 428](#)

config ipsec tunnel

IPsec tunnel.

```
config ipsec tunnel
    Description: IPsec tunnel.
end
```

isolator

This section includes syntax for the following commands:

- [config isolator profile on page 429](#)
- [config isolator setting on page 430](#)

config isolator profile

Configure isolator profiles.

```
config isolator profile
  Description: Configure isolator profiles.
  edit <name>
    set comments {var-string}
    set disclaimer {string}
    config entries
      Description: Isolator profile entries.
      edit <id>
        set proxy-address {string}
        set action [isolate|freeze|...]
        set status [enable|disable]
      next
    end
  next
end
```

config isolator profile

Parameter	Description	Type	Size	Default
name	Profile name.	string	Maximum length: 35	
comments	Comment.	var-string	Maximum length: 255	
disclaimer	A customized replacement message page for installer.	string	Maximum length: 35	

config entries

Parameter	Description	Type	Size	Default										
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0										
proxy-address	Choose the proxy-address for this isolator profile entry.	string	Maximum length: 79											
action	Choose the action for this isolator entry.	option	-	isolate										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>isolate</i></td><td>Open the website in an isolator instead of the client.</td></tr><tr><td><i>freeze</i></td><td>Freeze the website. The user is able to unfreeze and get access to the website when they accept the risk.</td></tr><tr><td><i>block</i></td><td>Block the traffic to the website.</td></tr><tr><td><i>allow</i></td><td>Bypass the traffic to the website.</td></tr></table>				Option	Description	<i>isolate</i>	Open the website in an isolator instead of the client.	<i>freeze</i>	Freeze the website. The user is able to unfreeze and get access to the website when they accept the risk.	<i>block</i>	Block the traffic to the website.	<i>allow</i>	Bypass the traffic to the website.
	Option	Description												
	<i>isolate</i>	Open the website in an isolator instead of the client.												
	<i>freeze</i>	Freeze the website. The user is able to unfreeze and get access to the website when they accept the risk.												
	<i>block</i>	Block the traffic to the website.												
<i>allow</i>	Bypass the traffic to the website.													
status	Enable/disable this isolator entry.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this entry.</td></tr><tr><td><i>disable</i></td><td>Disable this entry.</td></tr></table>				Option	Description	<i>enable</i>	Enable this entry.	<i>disable</i>	Disable this entry.				
	Option	Description												
	<i>enable</i>	Enable this entry.												
<i>disable</i>	Disable this entry.													

config isolator setting

Configure isolator setting.

```
config isolator setting
    Description: Configure isolator setting.
    set default-isolator-profile {string}
    set defective-session [use-default-profile|pass|...]
    set unmatched-session [use-default-profile|pass|...]
end
```

config isolator setting

Parameter	Description	Type	Size	Default								
default-isolator-profile	Name of an existing isolator profile. This profile is used when no policy is matched.	string	Maximum length: 35									
defective-session	Choose the way to handle rating requests for sessions with missing information.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>use-default-profile</i></td><td>Use default isolator profile to handle the session.</td></tr><tr><td><i>pass</i></td><td>Return bypass response to the rating request of the session.</td></tr><tr><td><i>block</i></td><td>Return block response to the rating request of the session.</td></tr></table>	Option	Description	<i>use-default-profile</i>	Use default isolator profile to handle the session.	<i>pass</i>	Return bypass response to the rating request of the session.	<i>block</i>	Return block response to the rating request of the session.			
Option	Description											
<i>use-default-profile</i>	Use default isolator profile to handle the session.											
<i>pass</i>	Return bypass response to the rating request of the session.											
<i>block</i>	Return block response to the rating request of the session.											
unmatched-session	Choose the way to handle rating requests for sessions that are unable to match any policy.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>use-default-profile</i></td><td>Use default isolator profile to handle the session.</td></tr><tr><td><i>pass</i></td><td>Return bypass response to the rating request of the session.</td></tr><tr><td><i>block</i></td><td>Return block response to the rating request of the session.</td></tr></table>	Option	Description	<i>use-default-profile</i>	Use default isolator profile to handle the session.	<i>pass</i>	Return bypass response to the rating request of the session.	<i>block</i>	Return block response to the rating request of the session.			
Option	Description											
<i>use-default-profile</i>	Use default isolator profile to handle the session.											
<i>pass</i>	Return bypass response to the rating request of the session.											
<i>block</i>	Return block response to the rating request of the session.											

log

This section includes syntax for the following commands:

- [config log custom-field on page 433](#)
- [config log disk filter on page 434](#)
- [config log disk setting on page 437](#)
- [config log eventfilter on page 442](#)
- [config log fortianalyzer-cloud filter on page 446](#)
- [config log fortianalyzer-cloud override-filter on page 450](#)
- [config log fortianalyzer-cloud override-setting on page 453](#)
- [config log fortianalyzer-cloud setting on page 454](#)
- [config log fortianalyzer2 filter on page 457](#)
- [config log fortianalyzer2 override-filter on page 461](#)
- [config log fortianalyzer2 override-setting on page 464](#)
- [config log fortianalyzer2 setting on page 468](#)
- [config log fortianalyzer3 filter on page 473](#)
- [config log fortianalyzer3 override-filter on page 476](#)
- [config log fortianalyzer3 override-setting on page 480](#)
- [config log fortianalyzer3 setting on page 484](#)
- [config log fortianalyzer filter on page 488](#)
- [config log fortianalyzer override-filter on page 492](#)
- [config log fortianalyzer override-setting on page 495](#)
- [config log fortianalyzer setting on page 499](#)
- [config log fortiguard filter on page 504](#)
- [config log fortiguard override-filter on page 507](#)
- [config log fortiguard override-setting on page 510](#)
- [config log fortiguard setting on page 512](#)
- [config log gui-display on page 515](#)
- [config log memory filter on page 515](#)
- [config log memory global-setting on page 519](#)
- [config log memory setting on page 519](#)
- [config log null-device filter on page 520](#)
- [config log null-device setting on page 523](#)
- [config log setting on page 524](#)
- [config log syslogd2 filter on page 528](#)
- [config log syslogd2 override-filter on page 531](#)
- [config log syslogd2 override-setting on page 535](#)
- [config log syslogd2 setting on page 539](#)
- [config log syslogd3 filter on page 544](#)
- [config log syslogd3 override-filter on page 548](#)

- [config log syslogd3 override-setting on page 551](#)
- [config log syslogd3 setting on page 556](#)
- [config log syslogd4 filter on page 561](#)
- [config log syslogd4 override-filter on page 564](#)
- [config log syslogd4 override-setting on page 568](#)
- [config log syslogd4 setting on page 572](#)
- [config log syslogd filter on page 577](#)
- [config log syslogd override-filter on page 581](#)
- [config log syslogd override-setting on page 584](#)
- [config log syslogd setting on page 589](#)
- [config log tacacs+accounting2 filter on page 594](#)
- [config log tacacs+accounting2 setting on page 595](#)
- [config log tacacs+accounting3 filter on page 596](#)
- [config log tacacs+accounting3 setting on page 597](#)
- [config log tacacs+accounting filter on page 598](#)
- [config log tacacs+accounting setting on page 599](#)
- [config log threat-weight on page 599](#)
- [config log webtrends filter on page 610](#)
- [config log webtrends setting on page 613](#)

config log custom-field

Configure custom log fields.

```
config log custom-field
    Description: Configure custom log fields.
    edit <id>
        set name {string}
        set value {string}
    next
end
```

config log custom-field

Parameter	Description	Type	Size	Default
id	Field ID string.	string	Maximum length: 35	
name	Field name (max: 15 characters).	string	Maximum length: 15	
value	Field value (max: 15 characters).	string	Maximum length: 15	

config log disk filter

Configure filters for local disk logging. Use these filters to determine the log messages to record according to severity and type.

```
config log disk filter
    Description: Configure filters for local disk logging. Use these filters to determine
the log messages to record according to severity and type.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    set dlp-archive [enable|disable]
config free-style
    Description: Free style filters.
    edit <id>
        set category [traffic|event|...]
        set filter {string}
        set filter-type [include|exclude]
    next
end
end
```

config log disk filter

Parameter	Description	Type	Size	Default
severity	Log to disk every message above and including this severity level.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable DLP archive logging.		
	<i>disable</i>	Disable DLP archive logging.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option	Description		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		

config log disk setting

Settings for local disk logging.

```

config log disk setting
    Description: Settings for local disk logging.
    set status [enable|disable]
    set ips-archive [enable|disable]
    set max-log-file-size {integer}
    set max-policy-packet-capture-size {integer}
    set roll-schedule [daily|weekly]
    set roll-day {option1}, {option2}, ...
    set roll-time {user}
    set diskfull [overwrite|nolog]
    set log-quota {integer}
    set dlp-archive-quota {integer}
    set report-quota {integer}
    set maximum-log-age {integer}
    set upload [enable|disable]
    set upload-destination {option}
    set uploadip {ipv4-address}
    set uploadport {integer}
    set source-ip {ipv4-address}
    set uploaduser {string}

```

```

set uploadpass {password}
set uploadaddr {string}
set uploadtype {option1}, {option2}, ...
set uploadsched [disable|enable]
set uploadtime {user}
set upload-delete-files [enable|disable]
set upload-ssl-conn [default|high|...]
set full-first-warning-threshold {integer}
set full-second-warning-threshold {integer}
set full-final-warning-threshold {integer}
set interface-select-method [auto|specify]
set interface {string}

```

end

config log disk setting

Parameter	Description	Type	Size	Default
status	Enable/disable local disk logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Log to local disk.		
	<i>disable</i>	Do not log to local disk.		
ips-archive	Enable/disable IPS packet archiving to the local disk.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable IPS packet archiving.		
	<i>disable</i>	Disable IPS packet archiving.		
max-log-file-size	Maximum log file size before rolling.	integer	Minimum value: 1 Maximum value: 100	20
max-policy-packet-capture-size	Maximum size of policy sniffer in MB (0 means unlimited).	integer	Minimum value: 0 Maximum value: 4294967295	100
roll-schedule	Frequency to check log file for rolling.	option	-	daily
	Option	Description		
	<i>daily</i>	Check the log file once a day.		
	<i>weekly</i>	Check the log file once a week.		

Parameter	Description	Type	Size	Default																
roll-day	Day of week on which to roll log file.	option	-	sunday																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sunday</i></td><td>Sunday</td></tr><tr><td><i>monday</i></td><td>Monday</td></tr><tr><td><i>tuesday</i></td><td>Tuesday</td></tr><tr><td><i>wednesday</i></td><td>Wednesday</td></tr><tr><td><i>thursday</i></td><td>Thursday</td></tr><tr><td><i>friday</i></td><td>Friday</td></tr><tr><td><i>saturday</i></td><td>Saturday</td></tr></table>	Option	Description	<i>sunday</i>	Sunday	<i>monday</i>	Monday	<i>tuesday</i>	Tuesday	<i>wednesday</i>	Wednesday	<i>thursday</i>	Thursday	<i>friday</i>	Friday	<i>saturday</i>	Saturday			
	Option	Description																		
	<i>sunday</i>	Sunday																		
	<i>monday</i>	Monday																		
	<i>tuesday</i>	Tuesday																		
	<i>wednesday</i>	Wednesday																		
	<i>thursday</i>	Thursday																		
	<i>friday</i>	Friday																		
	<i>saturday</i>	Saturday																		
roll-time	Time of day to roll the log file (hh:mm).	user	Not Specified																	
diskfull	Action to take when disk is full. The system can overwrite the oldest log messages or stop logging when the disk is full.	option	-	overwrite																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>overwrite</i></td><td>Overwrite the oldest logs when the log disk is full.</td></tr><tr><td><i>nolog</i></td><td>Stop logging when the log disk is full.</td></tr></table>	Option	Description	<i>overwrite</i>	Overwrite the oldest logs when the log disk is full.	<i>nolog</i>	Stop logging when the log disk is full.													
	Option	Description																		
	<i>overwrite</i>	Overwrite the oldest logs when the log disk is full.																		
<i>nolog</i>	Stop logging when the log disk is full.																			
log-quota	Disk log quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0																
dlp-archive-quota	DLP archive quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0																
report-quota	Report db quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0																
maximum-log-age	Delete log files older than (days).	integer	Minimum value: 0 Maximum value: 3650	7																

Parameter	Description	Type	Size	Default
upload	Enable/disable uploading log files when they are rolled.	option	-	disable
	Option Description			
	<i>enable</i>	Enable uploading log files when they are rolled.		
	<i>disable</i>	Disable uploading log files when they are rolled.		
upload-destination	The type of server to upload log files to. Only FTP is currently supported.	option	-	ftp-server
	Option Description			
	<i>ftp-server</i>	Upload rolled log files to an FTP server.		
uploadip	IP address of the FTP server to upload log files to.	ipv4-address	Not Specified	0.0.0.0
uploadport	TCP port to use for communicating with the FTP server.	integer	Minimum value: 0 Maximum value: 65535	21
source-ip	Source IP address to use for uploading disk log files.	ipv4-address	Not Specified	0.0.0.0
uploaduser	Username required to log into the FTP server to upload disk log files.	string	Maximum length: 35	
uploadpass	Password required to log into the FTP server to upload disk log files.	password	Not Specified	
uploaddir	The remote directory on the FTP server to upload log files to.	string	Maximum length: 63	
uploadtype	Types of log files to upload. Separate multiple entries with a space.	option	-	traffic event virus webfilter IPS emailfilter dlp-archive anomaly voip dlp app-ctrl waf dns ssh ssl
	Option Description			
	<i>traffic</i>	Upload traffic log.		

Parameter	Description	Type	Size	Default																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>event</i></td><td>Upload event log.</td></tr><tr><td><i>virus</i></td><td>Upload anti-virus log.</td></tr><tr><td><i>webfilter</i></td><td>Upload web filter log.</td></tr><tr><td><i>IPS</i></td><td>Upload IPS log.</td></tr><tr><td><i>emailfilter</i></td><td>Upload spam filter log.</td></tr><tr><td><i>dlp-archive</i></td><td>Upload DLP archive.</td></tr><tr><td><i>anomaly</i></td><td>Upload anomaly log.</td></tr><tr><td><i>voip</i></td><td>Upload VoIP log.</td></tr><tr><td><i>dlp</i></td><td>Upload DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Upload application control log.</td></tr><tr><td><i>waf</i></td><td>Upload web application firewall log.</td></tr><tr><td><i>dns</i></td><td>Upload DNS log.</td></tr><tr><td><i>ssh</i></td><td>Upload SSH log.</td></tr><tr><td><i>ssl</i></td><td>Upload SSL log.</td></tr><tr><td><i>file-filter</i></td><td>Upload file-filter log.</td></tr><tr><td><i>icap</i></td><td>Upload ICAP log.</td></tr></table>	Option	Description	<i>event</i>	Upload event log.	<i>virus</i>	Upload anti-virus log.	<i>webfilter</i>	Upload web filter log.	<i>IPS</i>	Upload IPS log.	<i>emailfilter</i>	Upload spam filter log.	<i>dlp-archive</i>	Upload DLP archive.	<i>anomaly</i>	Upload anomaly log.	<i>voip</i>	Upload VoIP log.	<i>dlp</i>	Upload DLP log.	<i>app-ctrl</i>	Upload application control log.	<i>waf</i>	Upload web application firewall log.	<i>dns</i>	Upload DNS log.	<i>ssh</i>	Upload SSH log.	<i>ssl</i>	Upload SSL log.	<i>file-filter</i>	Upload file-filter log.	<i>icap</i>	Upload ICAP log.			
	Option	Description																																				
	<i>event</i>	Upload event log.																																				
	<i>virus</i>	Upload anti-virus log.																																				
	<i>webfilter</i>	Upload web filter log.																																				
	<i>IPS</i>	Upload IPS log.																																				
	<i>emailfilter</i>	Upload spam filter log.																																				
	<i>dlp-archive</i>	Upload DLP archive.																																				
	<i>anomaly</i>	Upload anomaly log.																																				
	<i>voip</i>	Upload VoIP log.																																				
	<i>dlp</i>	Upload DLP log.																																				
	<i>app-ctrl</i>	Upload application control log.																																				
	<i>waf</i>	Upload web application firewall log.																																				
	<i>dns</i>	Upload DNS log.																																				
	<i>ssh</i>	Upload SSH log.																																				
	<i>ssl</i>	Upload SSL log.																																				
	<i>file-filter</i>	Upload file-filter log.																																				
<i>icap</i>	Upload ICAP log.																																					
uploadsched	Set the schedule for uploading log files to the FTP server.	option	-	disable																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Upload when rolling.</td></tr><tr><td><i>enable</i></td><td>Scheduled upload.</td></tr></table>	Option	Description	<i>disable</i>	Upload when rolling.	<i>enable</i>	Scheduled upload.																															
	Option	Description																																				
	<i>disable</i>	Upload when rolling.																																				
<i>enable</i>	Scheduled upload.																																					
uploadtime	Time of day at which log files are uploaded if uploadsched is enabled (hh:mm or hh).	user	Not Specified																																			
upload-delete-files	Delete log files after uploading.	option	-	enable																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Delete log files after uploading.</td></tr><tr><td><i>disable</i></td><td>Do not delete log files after uploading.</td></tr></table>	Option	Description	<i>enable</i>	Delete log files after uploading.	<i>disable</i>	Do not delete log files after uploading.																															
	Option	Description																																				
	<i>enable</i>	Delete log files after uploading.																																				
<i>disable</i>	Do not delete log files after uploading.																																					

Parameter	Description	Type	Size	Default										
upload-ssl-conn	Enable/disable encrypted FTPS communication to upload log files.	option	-	default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>FTPS with high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>FTPS with high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>FTPS with low encryption algorithms.</td></tr><tr><td><i>disable</i></td><td>Disable FTPS communication.</td></tr></table>	Option	Description	<i>default</i>	FTPS with high and medium encryption algorithms.	<i>high</i>	FTPS with high encryption algorithms.	<i>low</i>	FTPS with low encryption algorithms.	<i>disable</i>	Disable FTPS communication.			
Option	Description													
<i>default</i>	FTPS with high and medium encryption algorithms.													
<i>high</i>	FTPS with high encryption algorithms.													
<i>low</i>	FTPS with low encryption algorithms.													
<i>disable</i>	Disable FTPS communication.													
full-first-warning-threshold	Log full first warning threshold as a percent.	integer	Minimum value: 1 Maximum value: 98	75										
full-second-warning-threshold	Log full second warning threshold as a percent.	integer	Minimum value: 2 Maximum value: 99	90										
full-final-warning-threshold	Log full final warning threshold as a percent.	integer	Minimum value: 3 Maximum value: 100	95										
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.							
Option	Description													
<i>auto</i>	Set outgoing interface automatically.													
<i>specify</i>	Set outgoing interface manually.													
interface	Specify outgoing interface to reach server.	string	Maximum length: 15											

config log eventfilter

Configure log event filters.

```
config log eventfilter
  Description: Configure log event filters.
  set event [enable|disable]
  set system [enable|disable]
  set vpn [enable|disable]
  set user [enable|disable]
  set router [enable|disable]
```

```

set wireless-activity [enable|disable]
set wan-opt [enable|disable]
set endpoint [enable|disable]
set ha [enable|disable]
set security-rating [enable|disable]
set fortiextender [enable|disable]
set connector [enable|disable]
set sdwan [enable|disable]
set cifs [enable|disable]
set switch-controller [enable|disable]
set wcs [enable|disable]
set wdb [enable|disable]
set aggd [enable|disable]
set crwl [enable|disable]
set rest-api [enable|disable]
set webproxy [enable|disable]
set iptables [enable|disable]

```

```
end
```

config log eventfilter

Parameter	Description	Type	Size	Default						
event	Enable/disable event logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable event logging.</td></tr><tr><td><i>disable</i></td><td>Disable event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable event logging.	<i>disable</i>	Disable event logging.			
Option	Description									
<i>enable</i>	Enable event logging.									
<i>disable</i>	Disable event logging.									
system	Enable/disable system event logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable system event logging.</td></tr><tr><td><i>disable</i></td><td>Disable system event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable system event logging.	<i>disable</i>	Disable system event logging.			
Option	Description									
<i>enable</i>	Enable system event logging.									
<i>disable</i>	Disable system event logging.									
vpn	Enable/disable VPN event logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VPN event logging.</td></tr><tr><td><i>disable</i></td><td>Disable VPN event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable VPN event logging.	<i>disable</i>	Disable VPN event logging.			
Option	Description									
<i>enable</i>	Enable VPN event logging.									
<i>disable</i>	Disable VPN event logging.									
user	Enable/disable user authentication event logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable user authentication event logging.</td></tr><tr><td><i>disable</i></td><td>Disable user authentication event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable user authentication event logging.	<i>disable</i>	Disable user authentication event logging.			
Option	Description									
<i>enable</i>	Enable user authentication event logging.									
<i>disable</i>	Disable user authentication event logging.									

Parameter	Description	Type	Size	Default
router	Enable/disable router event logging.	option	-	enable
	Option	Description		
	enable	Enable router event logging.		
	disable	Disable router event logging.		
wireless-activity	Enable/disable wireless event logging.	option	-	enable
	Option	Description		
	enable	Enable wireless event logging.		
	disable	Disable wireless event logging.		
wan-opt	Enable/disable WAN optimization event logging.	option	-	enable
	Option	Description		
	enable	Enable WAN optimization event logging.		
	disable	Disable WAN optimization event logging.		
endpoint	Enable/disable endpoint event logging.	option	-	enable
	Option	Description		
	enable	Enable endpoint event logging.		
	disable	Disable endpoint event logging.		
ha	Enable/disable ha event logging.	option	-	enable
	Option	Description		
	enable	Enable ha event logging.		
	disable	Disable ha event logging.		
security-rating	Enable/disable Security Rating result logging.	option	-	enable
	Option	Description		
	enable	Enable Security Fabric audit result logging.		
	disable	Disable Security Fabric audit result logging.		
fortiextender	Enable/disable FortiExtender logging.	option	-	enable
	Option	Description		
	enable	Enable Forti-Extender logging.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable Forti-Extender logging.		
connector	Enable/disable SDN connector logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable SDN connector logging.		
	<i>disable</i>	Disable SDN connector logging.		
sdwan	Enable/disable SD-WAN logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable SD-WAN logging.		
	<i>disable</i>	Disable SD-WAN logging.		
cifs	Enable/disable CIFS logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable CIFS logging.		
	<i>disable</i>	Disable CIFS logging.		
switch-controller	Enable/disable Switch-Controller logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Switch-Controller logging.		
	<i>disable</i>	Disable Switch-Controller logging.		
wcs	Enable/disable log for wcs events.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Switch-Controller logging.		
	<i>disable</i>	Disable Switch-Controller logging.		
wdb	Enable/disable log for wdb events.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Switch-Controller logging.		
	<i>disable</i>	Disable Switch-Controller logging.		

Parameter	Description	Type	Size	Default						
aggd	Enable/disable log for aggd events.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Switch-Controller logging.</td></tr><tr><td><i>disable</i></td><td>Disable Switch-Controller logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Switch-Controller logging.	<i>disable</i>	Disable Switch-Controller logging.			
Option	Description									
<i>enable</i>	Enable Switch-Controller logging.									
<i>disable</i>	Disable Switch-Controller logging.									
crwl	Enable/disable log for crwl events.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Switch-Controller logging.</td></tr><tr><td><i>disable</i></td><td>Disable Switch-Controller logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Switch-Controller logging.	<i>disable</i>	Disable Switch-Controller logging.			
Option	Description									
<i>enable</i>	Enable Switch-Controller logging.									
<i>disable</i>	Disable Switch-Controller logging.									
rest-api	Enable/disable REST API logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable REST API logging.</td></tr><tr><td><i>disable</i></td><td>Disable REST API logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable REST API logging.	<i>disable</i>	Disable REST API logging.			
Option	Description									
<i>enable</i>	Enable REST API logging.									
<i>disable</i>	Disable REST API logging.									
webproxy	Enable/disable web proxy event logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Web Proxy event logging.</td></tr><tr><td><i>disable</i></td><td>Disable Web Proxy event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Web Proxy event logging.	<i>disable</i>	Disable Web Proxy event logging.			
Option	Description									
<i>enable</i>	Enable Web Proxy event logging.									
<i>disable</i>	Disable Web Proxy event logging.									
iptables	Enable/disable iptables event logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable iptables event logging.</td></tr><tr><td><i>disable</i></td><td>Disable iptables event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable iptables event logging.	<i>disable</i>	Disable iptables event logging.			
Option	Description									
<i>enable</i>	Enable iptables event logging.									
<i>disable</i>	Disable iptables event logging.									

config log fortianalyzer-cloud filter

Filters for FortiAnalyzer Cloud.

```
config log fortianalyzer-cloud filter
  Description: Filters for FortiAnalyzer Cloud.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set ztna-traffic [enable|disable]
```

```

set http-transaction [enable|disable]
set anomaly [enable|disable]
set voip [enable|disable]
set dlp-archive [enable|disable]
config free-style
    Description: Free style filters.
    edit <id>
        set category [traffic|event|...]
        set filter {string}
        set filter-type [include|exclude]
    next
end
end

```

config log fortianalyzer-cloud filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable DLP archive logging.		
	<i>disable</i>	Disable DLP archive logging.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option	Description		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		

config log fortianalyzer-cloud override-filter

Override filters for FortiAnalyzer Cloud.

```
config log fortianalyzer-cloud override-filter
    Description: Override filters for FortiAnalyzer Cloud.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    set dlp-archive [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log fortianalyzer-cloud override-filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable DLP archive logging.		
	<i>disable</i>	Disable DLP archive logging.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr></table>	Option	Description	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.			
	Option	Description																				
	<i>dlp</i>	DLP log.																				
	<i>app-ctrl</i>	Application control log.																				
	<i>waf</i>	Web application firewall log.																				
	<i>dns</i>	DNS detail log.																				
	<i>ssh</i>	SSH log.																				
	<i>ssl</i>	SSL log.																				
	<i>file-filter</i>	File filter log.																				
<i>icap</i>	ICAP log.																					
filter	Free style filter string.	string	Maximum length: 1023																			
filter-type	Include/exclude logs that match the filter.	option	-	include																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.															
	Option	Description																				
	<i>include</i>	Include logs that match the filter.																				
<i>exclude</i>	Exclude logs that match the filter.																					

config log fortianalyzer-cloud override-setting

Override FortiAnalyzer Cloud settings.

```
config log fortianalyzer-cloud override-setting
    Description: Override FortiAnalyzer Cloud settings.
    set status [enable|disable]
end
```

config log fortianalyzer-cloud override-setting

Parameter	Description	Type	Size	Default						
status	Enable/disable logging to FortiAnalyzer.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging to FortiAnalyzer.</td></tr><tr><td><i>disable</i></td><td>Disable logging to FortiAnalyzer.</td></tr></table>				Option	Description	<i>enable</i>	Enable logging to FortiAnalyzer.	<i>disable</i>	Disable logging to FortiAnalyzer.
Option	Description									
<i>enable</i>	Enable logging to FortiAnalyzer.									
<i>disable</i>	Disable logging to FortiAnalyzer.									

config log fortianalyzer-cloud setting

Global FortiAnalyzer Cloud settings.

```
config log fortianalyzer-cloud setting
    Description: Global FortiAnalyzer Cloud settings.
    set status [enable|disable]
    set ips-archive [enable|disable]
    set certificate-verification [enable|disable]
    set serial <name1>, <name2>, ...
    set preshared-key {string}
    set access-config [enable|disable]
    set hmac-algorithm [sha256|sha1]
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set conn-timeout {integer}
    set monitor-keepalive-period {integer}
    set monitor-failure-retry-period {integer}
    set certificate {string}
    set source-ip {string}
    set upload-option [store-and-upload|realtime|...]
    set upload-interval [daily|weekly|...]
    set upload-day {user}
    set upload-time {user}
    set priority [default|low]
    set max-log-rate {integer}
    set interface-select-method [auto|specify]
    set interface {string}
end
```

config log fortianalyzer-cloud setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to FortiAnalyzer.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging to FortiAnalyzer.		
	<i>disable</i>	Disable logging to FortiAnalyzer.		
ips-archive	Enable/disable IPS packet archive logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IPS packet archive logging.		
	<i>disable</i>	Disable IPS packet archive logging.		
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.		
	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.		
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79	
preshaed-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63	
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.		
	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.		
hmac-algorithm	OFTP login hash algorithm.	option	-	sha256
	Option	Description		
	<i>sha256</i>	Use SHA256 as HMAC algorithm.		
	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.		
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high
	Option	Description		
	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.		
	<i>high</i>	Encrypt logs using high encryption algorithms.		
	<i>low</i>	Encrypt logs using all encryption algorithms.		
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default
	Option	Description		
	<i>default</i>	Follow system global setting.		
	<i>SSLv3</i>	SSLv3.		
	<i>TLSv1</i>	TLSv1.		
	<i>TLSv1-1</i>	TLSv1.1.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLSv1-2</i>	TLSv1.2.		
	<i>TLSv1-3</i>	TLSv1.3.		
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35	
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63	
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute
	Option	Description		
	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.		
	<i>realtime</i>	Log directly to FortiAnalyzer in real time.		
	<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.		
	<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.		
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily
	Option	Description		
	<i>daily</i>	Upload log files to FortiAnalyzer once a day.		
	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.		
	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.		

Parameter	Description	Type	Size	Default						
upload-day	Day of week (month) to upload logs.	user	Not Specified							
upload-time	Time to upload logs (hh:mm).	user	Not Specified							
priority	Set log transmission priority.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set FortiAnalyzer log transmission priority to default.</td></tr><tr><td>low</td><td>Set FortiAnalyzer log transmission priority to low.</td></tr></table>				Option	Description	default	Set FortiAnalyzer log transmission priority to default.	low	Set FortiAnalyzer log transmission priority to low.
Option	Description									
default	Set FortiAnalyzer log transmission priority to default.									
low	Set FortiAnalyzer log transmission priority to low.									
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0						
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	auto	Set outgoing interface automatically.	specify	Set outgoing interface manually.
Option	Description									
auto	Set outgoing interface automatically.									
specify	Set outgoing interface manually.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							

config log fortianalyzer2 filter

Filters for FortiAnalyzer.

```
config log fortianalyzer2 filter
  Description: Filters for FortiAnalyzer.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set ztna-traffic [enable|disable]
  set http-transaction [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
```

```

        set category [traffic|event|...]
        set filter {string}
        set filter-type [include|exclude]
    next
end
end

```

config log fortianalyzer2 filter

Parameter	Description	Type	Size	Default
severity	Log every message above and including this severity level.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		

Parameter	Description	Type	Size	Default						
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.			
Option	Description									
<i>enable</i>	Enable sniffer traffic logging.									
<i>disable</i>	Disable sniffer traffic logging.									
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ztna traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable ztna traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable ztna traffic logging.	<i>disable</i>	Disable ztna traffic logging.			
Option	Description									
<i>enable</i>	Enable ztna traffic logging.									
<i>disable</i>	Disable ztna traffic logging.									
http-transaction	Enable/disable log http-transaction messages.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable http transaction logging.</td></tr><tr><td><i>disable</i></td><td>Disable http transaction logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable http transaction logging.	<i>disable</i>	Disable http transaction logging.			
Option	Description									
<i>enable</i>	Enable http transaction logging.									
<i>disable</i>	Disable http transaction logging.									
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
voip	Enable/disable VoIP logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VoIP logging.</td></tr><tr><td><i>disable</i></td><td>Disable VoIP logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP logging.									
dlp-archive	Enable/disable DLP archive logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DLP archive logging.</td></tr><tr><td><i>disable</i></td><td>Disable DLP archive logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable DLP archive logging.	<i>disable</i>	Disable DLP archive logging.			
Option	Description									
<i>enable</i>	Enable DLP archive logging.									
<i>disable</i>	Disable DLP archive logging.									

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	OptionDescription			
	traffic	Traffic log.		
	event	Event log.		
	virus	Antivirus log.		
	webfilter	Web filter log.		
	attack	Attack log.		
	spam	Antispam log.		
	anomaly	Anomaly log.		
	voip	VoIP log.		
	dlp	DLP log.		
	app-ctrl	Application control log.		
	waf	Web application firewall log.		
	dns	DNS detail log.		
	ssh	SSH log.		
	ssl	SSL log.		
	file-filter	File filter log.		
	icap	ICAP log.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	OptionDescription			
	include	Include logs that match the filter.		
	exclude	Exclude logs that match the filter.		

config log fortianalyzer2 override-filter

Override filters for FortiAnalyzer.

```
config log fortianalyzer2 override-filter
  Description: Override filters for FortiAnalyzer.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set ztna-traffic [enable|disable]
  set http-transaction [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}
      set filter-type [include|exclude]
    next
  end
end
```

config log fortianalyzer2 override-filter

Parameter	Description	Type	Size	Default
severity	Log every message above and including this severity level.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable DLP archive logging.		
	<i>disable</i>	Disable DLP archive logging.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option	Description		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		

config log fortianalyzer2 override-setting

Override FortiAnalyzer settings.

```
config log fortianalyzer2 override-setting
    Description: Override FortiAnalyzer settings.
    set use-management-vdom [enable|disable]
    set status [enable|disable]
    set ips-archive [enable|disable]
    set server {string}
    set alt-server {string}
    set fallback-to-primary [enable|disable]
    set certificate-verification [enable|disable]
    set serial <name1>, <name2>, ...
    set server-cert-ca {string}
    set preshared-key {string}
    set access-config [enable|disable]
    set hmac-algorithm [sha256|sha1]
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set conn-timeout {integer}
    set monitor-keepalive-period {integer}
    set monitor-failure-retry-period {integer}
    set certificate {string}
```



```

set source-ip {string}
set upload-option [store-and-upload|realtime|...]
set upload-interval [daily|weekly|...]
set upload-day {user}
set upload-time {user}
set reliable [enable|disable]
set priority [default|low]
set max-log-rate {integer}
set interface-select-method [auto|specify]
set interface {string}

```

```
end
```

config log fortianalyzer2 override-setting

Parameter	Description	Type	Size	Default
use-management-vdom	Enable/disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.		
	<i>disable</i>	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.		
status	Enable/disable logging to FortiAnalyzer.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging to FortiAnalyzer.		
	<i>disable</i>	Disable logging to FortiAnalyzer.		
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable IPS packet archive logging.		
	<i>disable</i>	Disable IPS packet archive logging.		
server	The remote FortiAnalyzer.	string	Maximum length: 127	
alt-server	Alternate FortiAnalyzer.	string	Maximum length: 127	
fallback-to-primary	Enable/disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	option	-	enable

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.</td></tr><tr><td><i>disable</i></td><td>Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.</td></tr></table>	Option	Description	<i>enable</i>	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	<i>disable</i>	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.					
	Option	Description										
	<i>enable</i>	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.										
<i>disable</i>	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.											
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable identity verification of FortiAnalyzer by use of certificate.</td></tr><tr><td><i>disable</i></td><td>Disable identity verification of FortiAnalyzer by use of certificate.</td></tr></table>	Option	Description	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.					
	Option	Description										
	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.										
<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.											
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79									
server-cert-ca	Mandatory CA on FortiGate in certificate chain of server.	string	Maximum length: 79									
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63									
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiAnalyzer access to configuration and data.</td></tr><tr><td><i>disable</i></td><td>Disable FortiAnalyzer access to configuration and data.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.					
	Option	Description										
	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.										
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.											
hmac-algorithm	OFTP login hash algorithm.	option	-	sha256								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sha256</i></td><td>Use SHA256 as HMAC algorithm.</td></tr><tr><td><i>sha1</i></td><td>Step down to SHA1 as the HMAC algorithm.</td></tr></table>	Option	Description	<i>sha256</i>	Use SHA256 as HMAC algorithm.	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.					
	Option	Description										
	<i>sha256</i>	Use SHA256 as HMAC algorithm.										
<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.											
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>Encrypt logs using high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>Encrypt logs using high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>Encrypt logs using all encryption algorithms.</td></tr></table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.			
	Option	Description										
	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.										
	<i>high</i>	Encrypt logs using high encryption algorithms.										
<i>low</i>	Encrypt logs using all encryption algorithms.											

Parameter	Description	Type	Size	Default														
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr><tr><td>TLSv1-3</td><td>TLSv1.3.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.	TLSv1-3	TLSv1.3.			
	Option	Description																
	default	Follow system global setting.																
	SSLv3	SSLv3.																
	TLSv1	TLSv1.																
	TLSv1-1	TLSv1.1.																
	TLSv1-2	TLSv1.2.																
TLSv1-3	TLSv1.3.																	
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10														
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5														
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5														
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35															
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63															
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>store-and-upload</td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr><tr><td>realtime</td><td>Log directly to FortiAnalyzer in real time.</td></tr><tr><td>1-minute</td><td>Log directly to FortiAnalyzer at least every 1 minute.</td></tr><tr><td>5-minute</td><td>Log directly to FortiAnalyzer at least every 5 minutes.</td></tr></table>	Option	Description	store-and-upload	Log to hard disk and then upload to FortiAnalyzer.	realtime	Log directly to FortiAnalyzer in real time.	1-minute	Log directly to FortiAnalyzer at least every 1 minute.	5-minute	Log directly to FortiAnalyzer at least every 5 minutes.							
	Option	Description																
	store-and-upload	Log to hard disk and then upload to FortiAnalyzer.																
	realtime	Log directly to FortiAnalyzer in real time.																
	1-minute	Log directly to FortiAnalyzer at least every 1 minute.																
5-minute	Log directly to FortiAnalyzer at least every 5 minutes.																	
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily														

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>daily</i></td><td>Upload log files to FortiAnalyzer once a day.</td></tr><tr><td><i>weekly</i></td><td>Upload log files to FortiAnalyzer once a week.</td></tr><tr><td><i>monthly</i></td><td>Upload log files to FortiAnalyzer once a month.</td></tr></table>	Option	Description	<i>daily</i>	Upload log files to FortiAnalyzer once a day.	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.			
	Option	Description										
	<i>daily</i>	Upload log files to FortiAnalyzer once a day.										
	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.										
<i>monthly</i>	Upload log files to FortiAnalyzer once a month.											
upload-day	Day of week (month) to upload logs.	user	Not Specified									
upload-time	Time to upload logs (hh:mm).	user	Not Specified									
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable reliable logging to FortiAnalyzer.</td></tr><tr><td><i>disable</i></td><td>Disable reliable logging to FortiAnalyzer.</td></tr></table>	Option	Description	<i>enable</i>	Enable reliable logging to FortiAnalyzer.	<i>disable</i>	Disable reliable logging to FortiAnalyzer.					
	Option	Description										
	<i>enable</i>	Enable reliable logging to FortiAnalyzer.										
<i>disable</i>	Disable reliable logging to FortiAnalyzer.											
priority	Set log transmission priority.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Set FortiAnalyzer log transmission priority to default.</td></tr><tr><td><i>low</i></td><td>Set FortiAnalyzer log transmission priority to low.</td></tr></table>	Option	Description	<i>default</i>	Set FortiAnalyzer log transmission priority to default.	<i>low</i>	Set FortiAnalyzer log transmission priority to low.					
	Option	Description										
	<i>default</i>	Set FortiAnalyzer log transmission priority to default.										
<i>low</i>	Set FortiAnalyzer log transmission priority to low.											
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.					
	Option	Description										
	<i>auto</i>	Set outgoing interface automatically.										
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

config log fortianalyzer2 setting

Global FortiAnalyzer settings.

```

config log fortianalyzer2 setting
    Description: Global FortiAnalyzer settings.
    set status [enable|disable]
    set ips-archive [enable|disable]
    set server {string}
    set alt-server {string}
    set fallback-to-primary [enable|disable]
    set certificate-verification [enable|disable]
    set serial <name1>, <name2>, ...
    set server-cert-ca {string}
    set preshared-key {string}
    set access-config [enable|disable]
    set hmac-algorithm [sha256|sha1]
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set conn-timeout {integer}
    set monitor-keepalive-period {integer}
    set monitor-failure-retry-period {integer}
    set certificate {string}
    set source-ip {string}
    set upload-option [store-and-upload|realtime|...]
    set upload-interval [daily|weekly|...]
    set upload-day {user}
    set upload-time {user}
    set reliable [enable|disable]
    set priority [default|low]
    set max-log-rate {integer}
    set interface-select-method [auto|specify]
    set interface {string}
end

```

config log fortianalyzer2 setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to FortiAnalyzer.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging to FortiAnalyzer.		
	<i>disable</i>	Disable logging to FortiAnalyzer.		
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable IPS packet archive logging.		
	<i>disable</i>	Disable IPS packet archive logging.		
server	The remote FortiAnalyzer.	string	Maximum length: 127	

Parameter	Description	Type	Size	Default						
alt-server	Alternate FortiAnalyzer.	string	Maximum length: 127							
fallback-to-primary	Enable/disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.</td></tr><tr><td><i>disable</i></td><td>Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.</td></tr></table>	Option	Description	<i>enable</i>	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	<i>disable</i>	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.			
Option	Description									
<i>enable</i>	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.									
<i>disable</i>	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.									
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable identity verification of FortiAnalyzer by use of certificate.</td></tr><tr><td><i>disable</i></td><td>Disable identity verification of FortiAnalyzer by use of certificate.</td></tr></table>	Option	Description	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.			
Option	Description									
<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.									
<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.									
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79							
server-cert-ca	Mandatory CA on FortiGate in certificate chain of server.	string	Maximum length: 79							
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63							
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiAnalyzer access to configuration and data.</td></tr><tr><td><i>disable</i></td><td>Disable FortiAnalyzer access to configuration and data.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.			
Option	Description									
<i>enable</i>	Enable FortiAnalyzer access to configuration and data.									
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.									
hmac-algorithm	OFTP login hash algorithm.	option	-	sha256						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sha256</i></td><td>Use SHA256 as HMAC algorithm.</td></tr><tr><td><i>sha1</i></td><td>Step down to SHA1 as the HMAC algorithm.</td></tr></table>	Option	Description	<i>sha256</i>	Use SHA256 as HMAC algorithm.	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.			
Option	Description									
<i>sha256</i>	Use SHA256 as HMAC algorithm.									
<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.									
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high						

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>Encrypt logs using high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>Encrypt logs using high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>Encrypt logs using all encryption algorithms.</td></tr></table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.									
	Option	Description																
	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.																
	<i>high</i>	Encrypt logs using high encryption algorithms.																
<i>low</i>	Encrypt logs using all encryption algorithms.																	
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr><tr><td><i>TLSv1-3</i></td><td>TLSv1.3.</td></tr></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.	<i>TLSv1-3</i>	TLSv1.3.			
	Option	Description																
	<i>default</i>	Follow system global setting.																
	<i>SSLv3</i>	SSLv3.																
	<i>TLSv1</i>	TLSv1.																
	<i>TLSv1-1</i>	TLSv1.1.																
	<i>TLSv1-2</i>	TLSv1.2.																
<i>TLSv1-3</i>	TLSv1.3.																	
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10														
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5														
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5														
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35															
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63															
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute														

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.		
	<i>realtime</i>	Log directly to FortiAnalyzer in real time.		
	<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.		
	<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.		
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily
	Option	Description		
	<i>daily</i>	Upload log files to FortiAnalyzer once a day.		
	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.		
	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.		
upload-day	Day of week (month) to upload logs.	user	Not Specified	
upload-time	Time to upload logs (hh:mm).	user	Not Specified	
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable reliable logging to FortiAnalyzer.		
	<i>disable</i>	Disable reliable logging to FortiAnalyzer.		
priority	Set log transmission priority.	option	-	default
	Option	Description		
	<i>default</i>	Set FortiAnalyzer log transmission priority to default.		
	<i>low</i>	Set FortiAnalyzer log transmission priority to low.		
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config log fortianalyzer3 filter

Filters for FortiAnalyzer.

```
config log fortianalyzer3 filter
    Description: Filters for FortiAnalyzer.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    set dlp-archive [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log fortianalyzer3 filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

Parameter	Description	Type	Size	Default						
http-transaction	Enable/disable log http-transaction messages.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable http transaction logging.</td></tr><tr><td><i>disable</i></td><td>Disable http transaction logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable http transaction logging.	<i>disable</i>	Disable http transaction logging.			
Option	Description									
<i>enable</i>	Enable http transaction logging.									
<i>disable</i>	Disable http transaction logging.									
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
voip	Enable/disable VoIP logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VoIP logging.</td></tr><tr><td><i>disable</i></td><td>Disable VoIP logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP logging.									
dlp-archive	Enable/disable DLP archive logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DLP archive logging.</td></tr><tr><td><i>disable</i></td><td>Disable DLP archive logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable DLP archive logging.	<i>disable</i>	Disable DLP archive logging.			
Option	Description									
<i>enable</i>	Enable DLP archive logging.									
<i>disable</i>	Disable DLP archive logging.									

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	Option	Description		
	traffic	Traffic log.		
	event	Event log.		

Parameter	Description	Type	Size	Default																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>virus</i></td><td>Antivirus log.</td></tr><tr><td><i>webfilter</i></td><td>Web filter log.</td></tr><tr><td><i>attack</i></td><td>Attack log.</td></tr><tr><td><i>spam</i></td><td>Antispam log.</td></tr><tr><td><i>anomaly</i></td><td>Anomaly log.</td></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr></table>	Option	Description	<i>virus</i>	Antivirus log.	<i>webfilter</i>	Web filter log.	<i>attack</i>	Attack log.	<i>spam</i>	Antispam log.	<i>anomaly</i>	Anomaly log.	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.			
	Option	Description																																
	<i>virus</i>	Antivirus log.																																
	<i>webfilter</i>	Web filter log.																																
	<i>attack</i>	Attack log.																																
	<i>spam</i>	Antispam log.																																
	<i>anomaly</i>	Anomaly log.																																
	<i>voip</i>	VoIP log.																																
	<i>dlp</i>	DLP log.																																
	<i>app-ctrl</i>	Application control log.																																
	<i>waf</i>	Web application firewall log.																																
	<i>dns</i>	DNS detail log.																																
	<i>ssh</i>	SSH log.																																
	<i>ssl</i>	SSL log.																																
	<i>file-filter</i>	File filter log.																																
<i>icap</i>	ICAP log.																																	
filter	Free style filter string.	string	Maximum length: 1023																															
filter-type	Include/exclude logs that match the filter.	option	-	include																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																											
	Option	Description																																
	<i>include</i>	Include logs that match the filter.																																
<i>exclude</i>	Exclude logs that match the filter.																																	

config log fortianalyzer3 override-filter

Override filters for FortiAnalyzer.

```
config log fortianalyzer3 override-filter
  Description: Override filters for FortiAnalyzer.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set ztna-traffic [enable|disable]
  set http-transaction [enable|disable]
```

```

set anomaly [enable|disable]
set voip [enable|disable]
set dlp-archive [enable|disable]
config free-style
    Description: Free style filters.
    edit <id>
        set category [traffic|event|...]
        set filter {string}
        set filter-type [include|exclude]
    next
end
end

```

config log fortianalyzer3 override-filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable DLP archive logging.		
	<i>disable</i>	Disable DLP archive logging.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
<i>icap</i>	ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option	Description		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		

config log fortianalyzer3 override-setting

Override FortiAnalyzer settings.

```
config log fortianalyzer3 override-setting
    Description: Override FortiAnalyzer settings.
    set use-management-vdom [enable|disable]
    set status [enable|disable]
    set ips-archive [enable|disable]
    set server {string}
    set alt-server {string}
    set fallback-to-primary [enable|disable]
    set certificate-verification [enable|disable]
    set serial <name1>, <name2>, ...
    set server-cert-ca {string}
    set preshared-key {string}
    set access-config [enable|disable]
    set hmac-algorithm [sha256|sha1]
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set conn-timeout {integer}
    set monitor-keepalive-period {integer}
    set monitor-failure-retry-period {integer}
    set certificate {string}
    set source-ip {string}
    set upload-option [store-and-upload|realtime|...]
    set upload-interval [daily|weekly|...]
    set upload-day {user}
    set upload-time {user}
    set reliable [enable|disable]
    set priority [default|low]
    set max-log-rate {integer}
    set interface-select-method [auto|specify]
    set interface {string}
end
```

config log fortianalyzer3 override-setting

Parameter	Description	Type	Size	Default						
use-management-vdom	Enable/disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.</td></tr><tr><td><i>disable</i></td><td>Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	<i>disable</i>	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.			
Option	Description									
<i>enable</i>	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.									
<i>disable</i>	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.									

Parameter	Description	Type	Size	Default
status	Enable/disable logging to FortiAnalyzer.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging to FortiAnalyzer.		
	<i>disable</i>	Disable logging to FortiAnalyzer.		
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable IPS packet archive logging.		
	<i>disable</i>	Disable IPS packet archive logging.		
server	The remote FortiAnalyzer.	string	Maximum length: 127	
alt-server	Alternate FortiAnalyzer.	string	Maximum length: 127	
fallback-to-primary	Enable/disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.		
	<i>disable</i>	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.		
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.		
	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.		
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79	
server-cert-ca	Mandatory CA on FortiGate in certificate chain of server.	string	Maximum length: 79	
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63	
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiAnalyzer access to configuration and data.</td></tr><tr><td><i>disable</i></td><td>Disable FortiAnalyzer access to configuration and data.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.											
	Option	Description																
	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.																
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.																	
hmac-algorithm	OFTP login hash algorithm.	option	-	sha256														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sha256</i></td><td>Use SHA256 as HMAC algorithm.</td></tr><tr><td><i>sha1</i></td><td>Step down to SHA1 as the HMAC algorithm.</td></tr></table>	Option	Description	<i>sha256</i>	Use SHA256 as HMAC algorithm.	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.											
	Option	Description																
	<i>sha256</i>	Use SHA256 as HMAC algorithm.																
<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.																	
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>Encrypt logs using high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>Encrypt logs using high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>Encrypt logs using all encryption algorithms.</td></tr></table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.									
	Option	Description																
	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.																
	<i>high</i>	Encrypt logs using high encryption algorithms.																
<i>low</i>	Encrypt logs using all encryption algorithms.																	
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr><tr><td><i>TLSv1-3</i></td><td>TLSv1.3.</td></tr></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.	<i>TLSv1-3</i>	TLSv1.3.			
	Option	Description																
	<i>default</i>	Follow system global setting.																
	<i>SSLv3</i>	SSLv3.																
	<i>TLSv1</i>	TLSv1.																
	<i>TLSv1-1</i>	TLSv1.1.																
<i>TLSv1-2</i>	TLSv1.2.																	
<i>TLSv1-3</i>	TLSv1.3.																	
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10														
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5														

Parameter	Description	Type	Size	Default										
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5										
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35											
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63											
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>store-and-upload</td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr><tr><td>realtime</td><td>Log directly to FortiAnalyzer in real time.</td></tr><tr><td>1-minute</td><td>Log directly to FortiAnalyzer at least every 1 minute.</td></tr><tr><td>5-minute</td><td>Log directly to FortiAnalyzer at least every 5 minutes.</td></tr></table>				Option	Description	store-and-upload	Log to hard disk and then upload to FortiAnalyzer.	realtime	Log directly to FortiAnalyzer in real time.	1-minute	Log directly to FortiAnalyzer at least every 1 minute.	5-minute	Log directly to FortiAnalyzer at least every 5 minutes.
Option	Description													
store-and-upload	Log to hard disk and then upload to FortiAnalyzer.													
realtime	Log directly to FortiAnalyzer in real time.													
1-minute	Log directly to FortiAnalyzer at least every 1 minute.													
5-minute	Log directly to FortiAnalyzer at least every 5 minutes.													
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>daily</td><td>Upload log files to FortiAnalyzer once a day.</td></tr><tr><td>weekly</td><td>Upload log files to FortiAnalyzer once a week.</td></tr><tr><td>monthly</td><td>Upload log files to FortiAnalyzer once a month.</td></tr></table>				Option	Description	daily	Upload log files to FortiAnalyzer once a day.	weekly	Upload log files to FortiAnalyzer once a week.	monthly	Upload log files to FortiAnalyzer once a month.		
Option	Description													
daily	Upload log files to FortiAnalyzer once a day.													
weekly	Upload log files to FortiAnalyzer once a week.													
monthly	Upload log files to FortiAnalyzer once a month.													
upload-day	Day of week (month) to upload logs.	user	Not Specified											
upload-time	Time to upload logs (hh:mm).	user	Not Specified											
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable reliable logging to FortiAnalyzer.</td></tr><tr><td>disable</td><td>Disable reliable logging to FortiAnalyzer.</td></tr></table>				Option	Description	enable	Enable reliable logging to FortiAnalyzer.	disable	Disable reliable logging to FortiAnalyzer.				
Option	Description													
enable	Enable reliable logging to FortiAnalyzer.													
disable	Disable reliable logging to FortiAnalyzer.													
priority	Set log transmission priority.	option	-	default										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>default</i>	Set FortiAnalyzer log transmission priority to default.		
	<i>low</i>	Set FortiAnalyzer log transmission priority to low.		
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config log fortianalyzer3 setting

Global FortiAnalyzer settings.

```
config log fortianalyzer3 setting
  Description: Global FortiAnalyzer settings.
  set status [enable|disable]
  set ips-archive [enable|disable]
  set server {string}
  set alt-server {string}
  set fallback-to-primary [enable|disable]
  set certificate-verification [enable|disable]
  set serial <name1>, <name2>, ...
  set server-cert-ca {string}
  set preshared-key {string}
  set access-config [enable|disable]
  set hmac-algorithm [sha256|sha1]
  set enc-algorithm [high-medium|high|...]
  set ssl-min-proto-version [default|SSLv3|...]
  set conn-timeout {integer}
  set monitor-keepalive-period {integer}
  set monitor-failure-retry-period {integer}
  set certificate {string}
  set source-ip {string}
  set upload-option [store-and-upload|realtime|...]
  set upload-interval [daily|weekly|...]
  set upload-day {user}
```

```

set upload-time {user}
set reliable [enable|disable]
set priority [default|low]
set max-log-rate {integer}
set interface-select-method [auto|specify]
set interface {string}
end

```

config log fortianalyzer3 setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to FortiAnalyzer.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging to FortiAnalyzer.		
	<i>disable</i>	Disable logging to FortiAnalyzer.		
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable IPS packet archive logging.		
	<i>disable</i>	Disable IPS packet archive logging.		
server	The remote FortiAnalyzer.	string	Maximum length: 127	
alt-server	Alternate FortiAnalyzer.	string	Maximum length: 127	
fallback-to-primary	Enable/disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.		
	<i>disable</i>	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.		
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.		
	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.		

Parameter	Description	Type	Size	Default
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79	
server-cert-ca	Mandatory CA on FortiGate in certificate chain of server.	string	Maximum length: 79	
preshaed-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63	
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.		
	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.		
hmac-algorithm	OFTP login hash algorithm.	option	-	sha256
	Option	Description		
	<i>sha256</i>	Use SHA256 as HMAC algorithm.		
	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.		
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high
	Option	Description		
	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.		
	<i>high</i>	Encrypt logs using high encryption algorithms.		
	<i>low</i>	Encrypt logs using all encryption algorithms.		
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default
	Option	Description		
	<i>default</i>	Follow system global setting.		
	<i>SSLv3</i>	SSLv3.		
	<i>TLSv1</i>	TLSv1.		
	<i>TLSv1-1</i>	TLSv1.1.		
	<i>TLSv1-2</i>	TLSv1.2.		
	<i>TLSv1-3</i>	TLSv1.3.		

Parameter	Description	Type	Size	Default										
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10										
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5										
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5										
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35											
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63											
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>store-and-upload</td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr><tr><td>realtime</td><td>Log directly to FortiAnalyzer in real time.</td></tr><tr><td>1-minute</td><td>Log directly to FortiAnalyzer at least every 1 minute.</td></tr><tr><td>5-minute</td><td>Log directly to FortiAnalyzer at least every 5 minutes.</td></tr></table>				Option	Description	store-and-upload	Log to hard disk and then upload to FortiAnalyzer.	realtime	Log directly to FortiAnalyzer in real time.	1-minute	Log directly to FortiAnalyzer at least every 1 minute.	5-minute	Log directly to FortiAnalyzer at least every 5 minutes.
Option	Description													
store-and-upload	Log to hard disk and then upload to FortiAnalyzer.													
realtime	Log directly to FortiAnalyzer in real time.													
1-minute	Log directly to FortiAnalyzer at least every 1 minute.													
5-minute	Log directly to FortiAnalyzer at least every 5 minutes.													
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>daily</td><td>Upload log files to FortiAnalyzer once a day.</td></tr><tr><td>weekly</td><td>Upload log files to FortiAnalyzer once a week.</td></tr><tr><td>monthly</td><td>Upload log files to FortiAnalyzer once a month.</td></tr></table>				Option	Description	daily	Upload log files to FortiAnalyzer once a day.	weekly	Upload log files to FortiAnalyzer once a week.	monthly	Upload log files to FortiAnalyzer once a month.		
Option	Description													
daily	Upload log files to FortiAnalyzer once a day.													
weekly	Upload log files to FortiAnalyzer once a week.													
monthly	Upload log files to FortiAnalyzer once a month.													
upload-day	Day of week (month) to upload logs.	user	Not Specified											
upload-time	Time to upload logs (hh:mm).	user	Not Specified											
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable reliable logging to FortiAnalyzer.		
	<i>disable</i>	Disable reliable logging to FortiAnalyzer.		
priority	Set log transmission priority.	option	-	default
	Option	Description		
	<i>default</i>	Set FortiAnalyzer log transmission priority to default.		
	<i>low</i>	Set FortiAnalyzer log transmission priority to low.		
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config log fortianalyzer filter

Filters for FortiAnalyzer.

```
config log fortianalyzer filter
  Description: Filters for FortiAnalyzer.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set ztna-traffic [enable|disable]
  set http-transaction [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  set dlp-archive [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
```



```

        set category [traffic|event|...]
        set filter {string}
        set filter-type [include|exclude]
    next
end
end

```

config log fortianalyzer filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		

Parameter	Description	Type	Size	Default						
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.			
Option	Description									
<i>enable</i>	Enable sniffer traffic logging.									
<i>disable</i>	Disable sniffer traffic logging.									
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ztna traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable ztna traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable ztna traffic logging.	<i>disable</i>	Disable ztna traffic logging.			
Option	Description									
<i>enable</i>	Enable ztna traffic logging.									
<i>disable</i>	Disable ztna traffic logging.									
http-transaction	Enable/disable log http-transaction messages.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable http transaction logging.</td></tr><tr><td><i>disable</i></td><td>Disable http transaction logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable http transaction logging.	<i>disable</i>	Disable http transaction logging.			
Option	Description									
<i>enable</i>	Enable http transaction logging.									
<i>disable</i>	Disable http transaction logging.									
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
voip	Enable/disable VoIP logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VoIP logging.</td></tr><tr><td><i>disable</i></td><td>Disable VoIP logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP logging.									
dlp-archive	Enable/disable DLP archive logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DLP archive logging.</td></tr><tr><td><i>disable</i></td><td>Disable DLP archive logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable DLP archive logging.	<i>disable</i>	Disable DLP archive logging.			
Option	Description									
<i>enable</i>	Enable DLP archive logging.									
<i>disable</i>	Disable DLP archive logging.									

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	OptionDescription			
	traffic	Traffic log.		
	event	Event log.		
	virus	Antivirus log.		
	webfilter	Web filter log.		
	attack	Attack log.		
	spam	Antispam log.		
	anomaly	Anomaly log.		
	voip	VoIP log.		
	dlp	DLP log.		
	app-ctrl	Application control log.		
	waf	Web application firewall log.		
	dns	DNS detail log.		
	ssh	SSH log.		
	ssl	SSL log.		
	file-filter	File filter log.		
icap	ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	OptionDescription			
	include	Include logs that match the filter.		
	exclude	Exclude logs that match the filter.		

config log fortianalyzer override-filter

Override filters for FortiAnalyzer.

```
config log fortianalyzer override-filter
    Description: Override filters for FortiAnalyzer.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    set dlp-archive [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log fortianalyzer override-filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable DLP archive logging.		
	<i>disable</i>	Disable DLP archive logging.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option	Description		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		

config log fortianalyzer override-setting

Override FortiAnalyzer settings.

```
config log fortianalyzer override-setting
    Description: Override FortiAnalyzer settings.
    set use-management-vdom [enable|disable]
    set status [enable|disable]
    set ips-archive [enable|disable]
    set server {string}
    set alt-server {string}
    set fallback-to-primary [enable|disable]
    set certificate-verification [enable|disable]
    set serial <name1>, <name2>, ...
    set server-cert-ca {string}
    set preshared-key {string}
    set access-config [enable|disable]
    set hmac-algorithm [sha256|sha1]
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set conn-timeout {integer}
    set monitor-keepalive-period {integer}
    set monitor-failure-retry-period {integer}
    set certificate {string}
```

```

set source-ip {string}
set upload-option [store-and-upload|realtime|...]
set upload-interval [daily|weekly|...]
set upload-day {user}
set upload-time {user}
set reliable [enable|disable]
set priority [default|low]
set max-log-rate {integer}
set interface-select-method [auto|specify]
set interface {string}

```

```
end
```

config log fortianalyzer override-setting

Parameter	Description	Type	Size	Default
use-management-vdom	Enable/disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.		
	<i>disable</i>	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.		
status	Enable/disable logging to FortiAnalyzer.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging to FortiAnalyzer.		
	<i>disable</i>	Disable logging to FortiAnalyzer.		
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable IPS packet archive logging.		
	<i>disable</i>	Disable IPS packet archive logging.		
server	The remote FortiAnalyzer.	string	Maximum length: 127	
alt-server	Alternate FortiAnalyzer.	string	Maximum length: 127	
fallback-to-primary	Enable/disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	option	-	enable

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.</td></tr><tr><td><i>disable</i></td><td>Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.</td></tr></table>	Option	Description	<i>enable</i>	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	<i>disable</i>	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.					
	Option	Description										
	<i>enable</i>	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.										
<i>disable</i>	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.											
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable identity verification of FortiAnalyzer by use of certificate.</td></tr><tr><td><i>disable</i></td><td>Disable identity verification of FortiAnalyzer by use of certificate.</td></tr></table>	Option	Description	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.					
	Option	Description										
	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.										
<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.											
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79									
server-cert-ca	Mandatory CA on FortiGate in certificate chain of server.	string	Maximum length: 79									
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63									
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiAnalyzer access to configuration and data.</td></tr><tr><td><i>disable</i></td><td>Disable FortiAnalyzer access to configuration and data.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.					
	Option	Description										
	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.										
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.											
hmac-algorithm	OFTP login hash algorithm.	option	-	sha256								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sha256</i></td><td>Use SHA256 as HMAC algorithm.</td></tr><tr><td><i>sha1</i></td><td>Step down to SHA1 as the HMAC algorithm.</td></tr></table>	Option	Description	<i>sha256</i>	Use SHA256 as HMAC algorithm.	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.					
	Option	Description										
	<i>sha256</i>	Use SHA256 as HMAC algorithm.										
<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.											
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>Encrypt logs using high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>Encrypt logs using high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>Encrypt logs using all encryption algorithms.</td></tr></table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.			
	Option	Description										
	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.										
	<i>high</i>	Encrypt logs using high encryption algorithms.										
<i>low</i>	Encrypt logs using all encryption algorithms.											

Parameter	Description	Type	Size	Default														
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr><tr><td>TLSv1-3</td><td>TLSv1.3.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.	TLSv1-3	TLSv1.3.			
	Option	Description																
	default	Follow system global setting.																
	SSLv3	SSLv3.																
	TLSv1	TLSv1.																
	TLSv1-1	TLSv1.1.																
	TLSv1-2	TLSv1.2.																
TLSv1-3	TLSv1.3.																	
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10														
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5														
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5														
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35															
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63															
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>store-and-upload</td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr><tr><td>realtime</td><td>Log directly to FortiAnalyzer in real time.</td></tr><tr><td>1-minute</td><td>Log directly to FortiAnalyzer at least every 1 minute.</td></tr><tr><td>5-minute</td><td>Log directly to FortiAnalyzer at least every 5 minutes.</td></tr></table>	Option	Description	store-and-upload	Log to hard disk and then upload to FortiAnalyzer.	realtime	Log directly to FortiAnalyzer in real time.	1-minute	Log directly to FortiAnalyzer at least every 1 minute.	5-minute	Log directly to FortiAnalyzer at least every 5 minutes.							
	Option	Description																
	store-and-upload	Log to hard disk and then upload to FortiAnalyzer.																
	realtime	Log directly to FortiAnalyzer in real time.																
	1-minute	Log directly to FortiAnalyzer at least every 1 minute.																
5-minute	Log directly to FortiAnalyzer at least every 5 minutes.																	
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily														

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>daily</i>	Upload log files to FortiAnalyzer once a day.		
	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.		
	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.		
upload-day	Day of week (month) to upload logs.	user	Not Specified	
upload-time	Time to upload logs (hh:mm).	user	Not Specified	
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable reliable logging to FortiAnalyzer.		
	<i>disable</i>	Disable reliable logging to FortiAnalyzer.		
priority	Set log transmission priority.	option	-	default
	Option	Description		
	<i>default</i>	Set FortiAnalyzer log transmission priority to default.		
	<i>low</i>	Set FortiAnalyzer log transmission priority to low.		
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config log fortianalyzer setting

Global FortiAnalyzer settings.

```

config log fortianalyzer setting
    Description: Global FortiAnalyzer settings.
    set status [enable|disable]
    set ips-archive [enable|disable]
    set server {string}
    set alt-server {string}
    set fallback-to-primary [enable|disable]
    set certificate-verification [enable|disable]
    set serial <name1>, <name2>, ...
    set server-cert-ca {string}
    set preshared-key {string}
    set access-config [enable|disable]
    set hmac-algorithm [sha256|sha1]
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set conn-timeout {integer}
    set monitor-keepalive-period {integer}
    set monitor-failure-retry-period {integer}
    set certificate {string}
    set source-ip {string}
    set upload-option [store-and-upload|realtime|...]
    set upload-interval [daily|weekly|...]
    set upload-day {user}
    set upload-time {user}
    set reliable [enable|disable]
    set priority [default|low]
    set max-log-rate {integer}
    set interface-select-method [auto|specify]
    set interface {string}
end

```

config log fortianalyzer setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to FortiAnalyzer.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging to FortiAnalyzer.		
	<i>disable</i>	Disable logging to FortiAnalyzer.		
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable IPS packet archive logging.		
	<i>disable</i>	Disable IPS packet archive logging.		
server	The remote FortiAnalyzer.	string	Maximum length: 127	

Parameter	Description	Type	Size	Default						
alt-server	Alternate FortiAnalyzer.	string	Maximum length: 127							
fallback-to-primary	Enable/disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.</td></tr><tr><td><i>disable</i></td><td>Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.</td></tr></table>	Option	Description	<i>enable</i>	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.	<i>disable</i>	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.			
Option	Description									
<i>enable</i>	Enable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.									
<i>disable</i>	Disable this FortiGate unit to fallback to the primary FortiAnalyzer when it is available.									
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable identity verification of FortiAnalyzer by use of certificate.</td></tr><tr><td><i>disable</i></td><td>Disable identity verification of FortiAnalyzer by use of certificate.</td></tr></table>	Option	Description	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.			
Option	Description									
<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.									
<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.									
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79							
server-cert-ca	Mandatory CA on FortiGate in certificate chain of server.	string	Maximum length: 79							
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63							
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiAnalyzer access to configuration and data.</td></tr><tr><td><i>disable</i></td><td>Disable FortiAnalyzer access to configuration and data.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.			
Option	Description									
<i>enable</i>	Enable FortiAnalyzer access to configuration and data.									
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.									
hmac-algorithm	OFTP login hash algorithm.	option	-	sha256						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sha256</i></td><td>Use SHA256 as HMAC algorithm.</td></tr><tr><td><i>sha1</i></td><td>Step down to SHA1 as the HMAC algorithm.</td></tr></table>	Option	Description	<i>sha256</i>	Use SHA256 as HMAC algorithm.	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.			
Option	Description									
<i>sha256</i>	Use SHA256 as HMAC algorithm.									
<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.									
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high						

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>Encrypt logs using high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>Encrypt logs using high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>Encrypt logs using all encryption algorithms.</td></tr></table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.									
	Option	Description																
	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.																
	<i>high</i>	Encrypt logs using high encryption algorithms.																
<i>low</i>	Encrypt logs using all encryption algorithms.																	
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr><tr><td><i>TLSv1-3</i></td><td>TLSv1.3.</td></tr></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.	<i>TLSv1-3</i>	TLSv1.3.			
	Option	Description																
	<i>default</i>	Follow system global setting.																
	<i>SSLv3</i>	SSLv3.																
	<i>TLSv1</i>	TLSv1.																
	<i>TLSv1-1</i>	TLSv1.1.																
	<i>TLSv1-2</i>	TLSv1.2.																
<i>TLSv1-3</i>	TLSv1.3.																	
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10														
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5														
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5														
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35															
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63															
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute														

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.		
	<i>realtime</i>	Log directly to FortiAnalyzer in real time.		
	<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.		
	<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.		
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily
	Option	Description		
	<i>daily</i>	Upload log files to FortiAnalyzer once a day.		
	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.		
	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.		
upload-day	Day of week (month) to upload logs.	user	Not Specified	
upload-time	Time to upload logs (hh:mm).	user	Not Specified	
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable reliable logging to FortiAnalyzer.		
	<i>disable</i>	Disable reliable logging to FortiAnalyzer.		
priority	Set log transmission priority.	option	-	default
	Option	Description		
	<i>default</i>	Set FortiAnalyzer log transmission priority to default.		
	<i>low</i>	Set FortiAnalyzer log transmission priority to low.		
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config log fortiguard filter

Filters for FortiCloud.

```
config log fortiguard filter
    Description: Filters for FortiCloud.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log fortiguard filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

Parameter	Description	Type	Size	Default						
http-transaction	Enable/disable log http-transaction messages.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable http transaction logging.</td></tr><tr><td><i>disable</i></td><td>Disable http transaction logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable http transaction logging.	<i>disable</i>	Disable http transaction logging.			
Option	Description									
<i>enable</i>	Enable http transaction logging.									
<i>disable</i>	Disable http transaction logging.									
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
voip	Enable/disable VoIP logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VoIP logging.</td></tr><tr><td><i>disable</i></td><td>Disable VoIP logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP logging.									

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	Option	Description		
	traffic	Traffic log.		
	event	Event log.		
	virus	Antivirus log.		
	webfilter	Web filter log.		
	attack	Attack log.		
	spam	Antispam log.		
	anomaly	Anomaly log.		

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr></table>	Option	Description	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.			
	Option	Description																						
	<i>voip</i>	VoIP log.																						
	<i>dlp</i>	DLP log.																						
	<i>app-ctrl</i>	Application control log.																						
	<i>waf</i>	Web application firewall log.																						
	<i>dns</i>	DNS detail log.																						
	<i>ssh</i>	SSH log.																						
	<i>ssl</i>	SSL log.																						
	<i>file-filter</i>	File filter log.																						
<i>icap</i>	ICAP log.																							
filter	Free style filter string.	string	Maximum length: 1023																					
filter-type	Include/exclude logs that match the filter.	option	-	include																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																	
	Option	Description																						
	<i>include</i>	Include logs that match the filter.																						
<i>exclude</i>	Exclude logs that match the filter.																							

config log fortiguard override-filter

Override filters for FortiCloud.

```
config log fortiguard override-filter
  Description: Override filters for FortiCloud.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set ztna-traffic [enable|disable]
  set http-transaction [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}
      set filter-type [include|exclude]
    next
  next
end
```

log

end
end

config log fortiguard override-filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic

Parameter	Description	Type	Size	Default																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>traffic</i></td><td>Traffic log.</td></tr><tr><td><i>event</i></td><td>Event log.</td></tr><tr><td><i>virus</i></td><td>Antivirus log.</td></tr><tr><td><i>webfilter</i></td><td>Web filter log.</td></tr><tr><td><i>attack</i></td><td>Attack log.</td></tr><tr><td><i>spam</i></td><td>Antispam log.</td></tr><tr><td><i>anomaly</i></td><td>Anomaly log.</td></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr></table>	Option	Description	<i>traffic</i>	Traffic log.	<i>event</i>	Event log.	<i>virus</i>	Antivirus log.	<i>webfilter</i>	Web filter log.	<i>attack</i>	Attack log.	<i>spam</i>	Antispam log.	<i>anomaly</i>	Anomaly log.	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.			
	Option	Description																																				
	<i>traffic</i>	Traffic log.																																				
	<i>event</i>	Event log.																																				
	<i>virus</i>	Antivirus log.																																				
	<i>webfilter</i>	Web filter log.																																				
	<i>attack</i>	Attack log.																																				
	<i>spam</i>	Antispam log.																																				
	<i>anomaly</i>	Anomaly log.																																				
	<i>voip</i>	VoIP log.																																				
	<i>dlp</i>	DLP log.																																				
	<i>app-ctrl</i>	Application control log.																																				
	<i>waf</i>	Web application firewall log.																																				
	<i>dns</i>	DNS detail log.																																				
	<i>ssh</i>	SSH log.																																				
	<i>ssl</i>	SSL log.																																				
	<i>file-filter</i>	File filter log.																																				
<i>icap</i>	ICAP log.																																					
filter	Free style filter string.	string	Maximum length: 1023																																			
filter-type	Include/exclude logs that match the filter.	option	-	include																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																															
	Option	Description																																				
	<i>include</i>	Include logs that match the filter.																																				
<i>exclude</i>	Exclude logs that match the filter.																																					

config log fortiguard override-setting

Override global FortiCloud logging settings for this VDOM.

```
config log fortiguard override-setting
  Description: Override global FortiCloud logging settings for this VDOM.
  set override [enable|disable]
  set status [enable|disable]
  set upload-option [store-and-upload|realtime|...]
  set upload-interval [daily|weekly|...]
```

```

set upload-day {user}
set upload-time {user}
set priority [default|low]
set max-log-rate {integer}
set access-config [enable|disable]
end

```

config log fortiguard override-setting

Parameter	Description	Type	Size	Default
override	Overriding FortiCloud settings for this VDOM or use global settings.	option	-	disable
	Option	Description		
	<i>enable</i>	Override FortiCloud logging settings.		
	<i>disable</i>	Use global FortiCloud logging settings.		
status	Enable/disable logging to FortiCloud.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging to FortiCloud.		
	<i>disable</i>	Disable logging to FortiCloud.		
upload-option	Configure how log messages are sent to FortiCloud.	option	-	5-minute
	Option	Description		
	<i>store-and-upload</i>	Log to the hard disk and then upload logs to FortiCloud.		
	<i>realtime</i>	Log directly to FortiCloud in real time.		
	<i>1-minute</i>	Log directly to FortiCloud at 1-minute intervals.		
	<i>5-minute</i>	Log directly to FortiCloud at 5-minute intervals.		
upload-interval	Frequency of uploading log files to FortiCloud.	option	-	daily
	Option	Description		
	<i>daily</i>	Upload log files to FortiCloud once a day.		
	<i>weekly</i>	Upload log files to FortiCloud once a week.		
	<i>monthly</i>	Upload log files to FortiCloud once a month.		
upload-day	Day of week to roll logs.	user	Not Specified	

Parameter	Description	Type	Size	Default						
upload-time	Time of day to roll logs (hh:mm).	user	Not Specified							
priority	Set log transmission priority.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set FortiCloud log transmission priority to default.</td></tr><tr><td>low</td><td>Set FortiCloud log transmission priority to low.</td></tr></table>				Option	Description	default	Set FortiCloud log transmission priority to default.	low	Set FortiCloud log transmission priority to low.
Option	Description									
default	Set FortiCloud log transmission priority to default.									
low	Set FortiCloud log transmission priority to low.									
max-log-rate	FortiCloud maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0						
access-config	Enable/disable FortiCloud access to configuration and data.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiCloud access to configuration and data.</td></tr><tr><td>disable</td><td>Disable FortiCloud access to configuration and data.</td></tr></table>				Option	Description	enable	Enable FortiCloud access to configuration and data.	disable	Disable FortiCloud access to configuration and data.
Option	Description									
enable	Enable FortiCloud access to configuration and data.									
disable	Disable FortiCloud access to configuration and data.									

config log fortiguard setting

Configure logging to FortiCloud.

```
config log fortiguard setting
    Description: Configure logging to FortiCloud.
    set status [enable|disable]
    set upload-option [store-and-upload|realtime|...]
    set upload-interval [daily|weekly|...]
    set upload-day {user}
    set upload-time {user}
    set priority [default|low]
    set max-log-rate {integer}
    set access-config [enable|disable]
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set conn-timeout {integer}
    set source-ip {ipv4-address}
    set interface-select-method [auto|specify]
    set interface {string}
end
```


config log fortiguard setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to FortiCloud.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging to FortiCloud.		
	<i>disable</i>	Disable logging to FortiCloud.		
upload-option	Configure how log messages are sent to FortiCloud.	option	-	5-minute
	Option	Description		
	<i>store-and-upload</i>	Log to the hard disk and then upload logs to FortiCloud.		
	<i>realtime</i>	Log directly to FortiCloud in real time.		
	<i>1-minute</i>	Log directly to FortiCloud at 1-minute intervals.		
	<i>5-minute</i>	Log directly to FortiCloud at 5-minute intervals.		
upload-interval	Frequency of uploading log files to FortiCloud.	option	-	daily
	Option	Description		
	<i>daily</i>	Upload log files to FortiCloud once a day.		
	<i>weekly</i>	Upload log files to FortiCloud once a week.		
	<i>monthly</i>	Upload log files to FortiCloud once a month.		
upload-day	Day of week to roll logs.	user	Not Specified	
upload-time	Time of day to roll logs (hh:mm).	user	Not Specified	
priority	Set log transmission priority.	option	-	default
	Option	Description		
	<i>default</i>	Set FortiCloud log transmission priority to default.		
	<i>low</i>	Set FortiCloud log transmission priority to low.		
max-log-rate	FortiCloud maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0

Parameter	Description	Type	Size	Default												
access-config	Enable/disable FortiCloud access to configuration and data.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiCloud access to configuration and data.</td></tr><tr><td><i>disable</i></td><td>Disable FortiCloud access to configuration and data.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiCloud access to configuration and data.	<i>disable</i>	Disable FortiCloud access to configuration and data.									
Option	Description															
<i>enable</i>	Enable FortiCloud access to configuration and data.															
<i>disable</i>	Disable FortiCloud access to configuration and data.															
enc-algorithm	Configure the level of SSL protection for secure communication with FortiCloud.	option	-	high												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>Encrypt logs using high and medium encryption.</td></tr><tr><td><i>high</i></td><td>Encrypt logs using high encryption.</td></tr><tr><td><i>low</i></td><td>Encrypt logs using low encryption.</td></tr></table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption.	<i>high</i>	Encrypt logs using high encryption.	<i>low</i>	Encrypt logs using low encryption.							
Option	Description															
<i>high-medium</i>	Encrypt logs using high and medium encryption.															
<i>high</i>	Encrypt logs using high encryption.															
<i>low</i>	Encrypt logs using low encryption.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
conn-timeout	FortiProxy Cloud connection timeout in seconds.	integer	Minimum value: 1 Maximum value: 3600	10												
source-ip	Source IP address used to connect FortiCloud.	ipv4-address	Not Specified	0.0.0.0												
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.									
Option	Description															
<i>auto</i>	Set outgoing interface automatically.															
<i>specify</i>	Set outgoing interface manually.															
interface	Specify outgoing interface to reach server.	string	Maximum length: 15													

config log gui-display

Configure how log messages are displayed on the GUI.

```
config log gui-display
    Description: Configure how log messages are displayed on the GUI.
    set resolve-hosts [enable|disable]
    set resolve-apps [enable|disable]
    set fortiview-unscanned-apps [enable|disable]
end
```

config log gui-display

Parameter	Description	Type	Size	Default						
resolve-hosts	Enable/disable resolving IP addresses to hostname in log messages on the GUI using reverse DNS lookup.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable resolving IP addresses to hostnames.</td></tr><tr><td><i>disable</i></td><td>Disable resolving IP addresses to hostnames.</td></tr></table>	Option	Description	<i>enable</i>	Enable resolving IP addresses to hostnames.	<i>disable</i>	Disable resolving IP addresses to hostnames.			
Option	Description									
<i>enable</i>	Enable resolving IP addresses to hostnames.									
<i>disable</i>	Disable resolving IP addresses to hostnames.									
resolve-apps	Resolve unknown applications on the GUI using Fortinet's remote application database.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable unknown applications on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable unknown applications on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable unknown applications on the GUI.	<i>disable</i>	Disable unknown applications on the GUI.			
Option	Description									
<i>enable</i>	Enable unknown applications on the GUI.									
<i>disable</i>	Disable unknown applications on the GUI.									
fortiview-unscanned-apps	Enable/disable showing unscanned traffic in FortiView application charts.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable showing unscanned traffic.</td></tr><tr><td><i>disable</i></td><td>Disable showing unscanned traffic.</td></tr></table>	Option	Description	<i>enable</i>	Enable showing unscanned traffic.	<i>disable</i>	Disable showing unscanned traffic.			
Option	Description									
<i>enable</i>	Enable showing unscanned traffic.									
<i>disable</i>	Disable showing unscanned traffic.									

config log memory filter

Filters for memory buffer.

```
config log memory filter
    Description: Filters for memory buffer.
    set severity [emergency|alert|...]
```

```

set forward-traffic [enable|disable]
set local-traffic [enable|disable]
set multicast-traffic [enable|disable]
set sniffer-traffic [enable|disable]
set ztna-traffic [enable|disable]
set http-transaction [enable|disable]
set anomaly [enable|disable]
set voip [enable|disable]
config free-style
    Description: Free style filters.
    edit <id>
        set category [traffic|event|...]
        set filter {string}
        set filter-type [include|exclude]
    next
end
end

```

config log memory filter

Parameter	Description	Type	Size	Default
severity	Log every message above and including this severity level.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	OptionDescription			
	traffic	Traffic log.		
	event	Event log.		
	virus	Antivirus log.		
	webfilter	Web filter log.		
	attack	Attack log.		
	spam	Antispam log.		
	anomaly	Anomaly log.		
	voip	VoIP log.		
	dlp	DLP log.		
	app-ctrl	Application control log.		
	waf	Web application firewall log.		
	dns	DNS detail log.		
	ssh	SSH log.		
	ssl	SSL log.		
	file-filter	File filter log.		
icap	ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	OptionDescription			
	include	Include logs that match the filter.		
	exclude	Exclude logs that match the filter.		

config log memory global-setting

Global settings for memory logging.

```
config log memory global-setting
    Description: Global settings for memory logging.
    set max-size {integer}
    set full-first-warning-threshold {integer}
    set full-second-warning-threshold {integer}
    set full-final-warning-threshold {integer}
end
```

config log memory global-setting

Parameter	Description	Type	Size	Default
max-size	Maximum amount of memory that can be used for memory logging in bytes.	integer	Minimum value: 0 Maximum value: 4294967295	41308815
full-first-warning-threshold	Log full first warning threshold as a percent.	integer	Minimum value: 1 Maximum value: 98	75
full-second-warning-threshold	Log full second warning threshold as a percent.	integer	Minimum value: 2 Maximum value: 99	90
full-final-warning-threshold	Log full final warning threshold as a percent.	integer	Minimum value: 3 Maximum value: 100	95

config log memory setting

Settings for memory buffer.

```
config log memory setting
    Description: Settings for memory buffer.
    set status [enable|disable]
end
```

config log memory setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to the FortiProxy's memory.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging to memory.		
	<i>disable</i>	Disable logging to memory.		

config log null-device filter

Filters for null device logging.

```
config log null-device filter
    Description: Filters for null device logging.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log null-device filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

Parameter	Description	Type	Size	Default
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	Option	Description		
	traffic	Traffic log.		
	event	Event log.		
	virus	Antivirus log.		
	webfilter	Web filter log.		
	attack	Attack log.		
	spam	Antispam log.		
	anomaly	Anomaly log.		

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr></table>	Option	Description	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.			
	Option	Description																						
	<i>voip</i>	VoIP log.																						
	<i>dlp</i>	DLP log.																						
	<i>app-ctrl</i>	Application control log.																						
	<i>waf</i>	Web application firewall log.																						
	<i>dns</i>	DNS detail log.																						
	<i>ssh</i>	SSH log.																						
	<i>ssl</i>	SSL log.																						
	<i>file-filter</i>	File filter log.																						
<i>icap</i>	ICAP log.																							
filter	Free style filter string.	string	Maximum length: 1023																					
filter-type	Include/exclude logs that match the filter.	option	-	include																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																	
	Option	Description																						
	<i>include</i>	Include logs that match the filter.																						
<i>exclude</i>	Exclude logs that match the filter.																							

config log null-device setting

Settings for null device logging.

```
config log null-device setting
    Description: Settings for null device logging.
    set status [enable|disable]
end
```

config log null-device setting

Parameter	Description	Type	Size	Default
status	Enable/disable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).		
	<i>disable</i>	Disable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).		

config log setting

Configure general log settings.

```
config log setting
    Description: Configure general log settings.
    set resolve-ip [enable|disable]
    set resolve-port [enable|disable]
    set log-user-in-upper [enable|disable]
    set fwpolicy-implicit-log [enable|disable]
    set fwpolicy6-implicit-log [enable|disable]
    set log-invalid-packet [enable|disable]
    set local-in-allow [enable|disable]
    set local-in-deny-unicast [enable|disable]
    set local-in-deny-broadcast [enable|disable]
    set local-out [enable|disable]
    set local-out-ioc-detection [enable|disable]
    set daemon-log [enable|disable]
    set neighbor-event [enable|disable]
    set brief-traffic-format [enable|disable]
    set user-anonymize [enable|disable]
    set expolicy-implicit-log [enable|disable]
    set log-policy-comment [enable|disable]
    set faz-override [enable|disable]
    set syslog-override [enable|disable]
    set rest-api-set [enable|disable]
    set rest-api-get [enable|disable]
    set custom-log-fields <field-id1>, <field-id2>, ...
    set anonymization-hash {string}
end
```

config log setting

Parameter	Description	Type	Size	Default
resolve-ip	Enable/disable adding resolved domain names to traffic logs if possible.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable adding resolved domain names to traffic logs.		
	<i>disable</i>	Disable adding resolved domain names to traffic logs.		
resolve-port	Enable/disable adding resolved service names to traffic logs.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable adding resolved service names to traffic logs.		
	<i>disable</i>	Disable adding resolved service names to traffic logs.		
log-user-in-upper	Enable/disable logs with user-in-upper.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logs with user-in-upper.		
	<i>disable</i>	Disable logs with user-in-upper.		
fwpolicy-implicit-log	Enable/disable implicit firewall policy logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable implicit firewall policy logging.		
	<i>disable</i>	Disable implicit firewall policy logging.		
fwpolicy6-implicit-log	Enable/disable implicit firewall policy6 logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable implicit firewall policy6 logging.		
	<i>disable</i>	Disable implicit firewall policy6 logging.		
log-invalid-packet	Enable/disable invalid packet traffic logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable invalid packet traffic logging.		
	<i>disable</i>	Disable invalid packet traffic logging.		
local-in-allow	Enable/disable local-in-allow logging.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable local-in-allow logging.		
	<i>disable</i>	Disable local-in-allow logging.		
local-in-deny-unicast	Enable/disable local-in-deny-unicast logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable local-in-deny-unicast logging.		
	<i>disable</i>	Disable local-in-deny-unicast logging.		
local-in-deny-broadcast	Enable/disable local-in-deny-broadcast logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable local-in-deny-broadcast logging.		
	<i>disable</i>	Disable local-in-deny-broadcast logging.		
local-out	Enable/disable local-out logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local-out logging.		
	<i>disable</i>	Disable local-out logging.		
local-out-ioc-detection	Enable/disable local-out traffic IoC detection. Requires local-out to be enabled.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local-out traffic IoC detection. Requires local-out to be enabled.		
	<i>disable</i>	Disable local-out traffic IoC detection.		
daemon-log	Enable/disable daemon logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable daemon logging.		
	<i>disable</i>	Disable daemon logging.		
neighbor-event	Enable/disable neighbor event logging.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable neighbor event logging.		
	<i>disable</i>	Disable neighbor event logging.		
brief-traffic-format	Enable/disable brief format traffic logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable brief format traffic logging.		
	<i>disable</i>	Disable brief format traffic logging.		
user-anonymize	Enable/disable anonymizing user names in log messages.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable anonymizing user names in log messages.		
	<i>disable</i>	Disable anonymizing user names in log messages.		
expolicy-implicit-log	Enable/disable explicit proxy firewall implicit policy logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable explicit proxy firewall implicit policy logging.		
	<i>disable</i>	Disable explicit proxy firewall implicit policy logging.		
log-policy-comment	Enable/disable inserting policy comments into traffic logs.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable inserting policy comments into traffic logs.		
	<i>disable</i>	Disable inserting policy comments into traffic logs.		
faz-override	Enable/disable override FortiAnalyzer settings.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable override FortiAnalyzer settings.		
	<i>disable</i>	Disable override FortiAnalyzer settings.		
syslog-override	Enable/disable override Syslog settings.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable override Syslog settings.		
	<i>disable</i>	Disable override Syslog settings.		
rest-api-set	Enable/disable REST API POST/PUT/DELETE request logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable POST/PUT/DELETE REST API logging.		
	<i>disable</i>	Disable POST/PUT/DELETE REST API logging.		
rest-api-get	Enable/disable REST API GET request logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable GET REST API logging.		
	<i>disable</i>	Disable GET REST API logging.		
custom-log-fields <field-id>	Custom fields to append to all log messages. Custom log field.	string	Maximum length: 35	
anonymization- hash	User name anonymization hash salt.	string	Maximum length: 32	

config log syslogd2 filter

Filters for remote system server.

```
config log syslogd2 filter
    Description: Filters for remote system server.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    next
```


log

end
end

config log syslogd2 filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic

Parameter	Description	Type	Size	Default																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>traffic</i></td><td>Traffic log.</td></tr><tr><td><i>event</i></td><td>Event log.</td></tr><tr><td><i>virus</i></td><td>Antivirus log.</td></tr><tr><td><i>webfilter</i></td><td>Web filter log.</td></tr><tr><td><i>attack</i></td><td>Attack log.</td></tr><tr><td><i>spam</i></td><td>Antispam log.</td></tr><tr><td><i>anomaly</i></td><td>Anomaly log.</td></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr></table>	Option	Description	<i>traffic</i>	Traffic log.	<i>event</i>	Event log.	<i>virus</i>	Antivirus log.	<i>webfilter</i>	Web filter log.	<i>attack</i>	Attack log.	<i>spam</i>	Antispam log.	<i>anomaly</i>	Anomaly log.	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.			
	Option	Description																																				
	<i>traffic</i>	Traffic log.																																				
	<i>event</i>	Event log.																																				
	<i>virus</i>	Antivirus log.																																				
	<i>webfilter</i>	Web filter log.																																				
	<i>attack</i>	Attack log.																																				
	<i>spam</i>	Antispam log.																																				
	<i>anomaly</i>	Anomaly log.																																				
	<i>voip</i>	VoIP log.																																				
	<i>dlp</i>	DLP log.																																				
	<i>app-ctrl</i>	Application control log.																																				
	<i>waf</i>	Web application firewall log.																																				
	<i>dns</i>	DNS detail log.																																				
	<i>ssh</i>	SSH log.																																				
	<i>ssl</i>	SSL log.																																				
	<i>file-filter</i>	File filter log.																																				
<i>icap</i>	ICAP log.																																					
filter	Free style filter string.	string	Maximum length: 1023																																			
filter-type	Include/exclude logs that match the filter.	option	-	include																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																															
	Option	Description																																				
	<i>include</i>	Include logs that match the filter.																																				
<i>exclude</i>	Exclude logs that match the filter.																																					

config log syslogd2 override-filter

Override filters for remote system server.

```
config log syslogd2 override-filter
  Description: Override filters for remote system server.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
```

```

set sniffer-traffic [enable|disable]
set ztna-traffic [enable|disable]
set http-transaction [enable|disable]
set anomaly [enable|disable]
set voip [enable|disable]
config free-style
    Description: Free style filters.
    edit <id>
        set category [traffic|event|...]
        set filter {string}
        set filter-type [include|exclude]
    next
end
end

```

config log syslogd2 override-filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		

Parameter	Description	Type	Size	Default						
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multicast traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable multicast traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.			
Option	Description									
<i>enable</i>	Enable multicast traffic logging.									
<i>disable</i>	Disable multicast traffic logging.									
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.			
Option	Description									
<i>enable</i>	Enable sniffer traffic logging.									
<i>disable</i>	Disable sniffer traffic logging.									
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ztna traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable ztna traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable ztna traffic logging.	<i>disable</i>	Disable ztna traffic logging.			
Option	Description									
<i>enable</i>	Enable ztna traffic logging.									
<i>disable</i>	Disable ztna traffic logging.									
http-transaction	Enable/disable log http-transaction messages.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable http transaction logging.</td></tr><tr><td><i>disable</i></td><td>Disable http transaction logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable http transaction logging.	<i>disable</i>	Disable http transaction logging.			
Option	Description									
<i>enable</i>	Enable http transaction logging.									
<i>disable</i>	Disable http transaction logging.									
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
voip	Enable/disable VoIP logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VoIP logging.</td></tr><tr><td><i>disable</i></td><td>Disable VoIP logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.			
Option	Description									
<i>enable</i>	Enable VoIP logging.									
<i>disable</i>	Disable VoIP logging.									

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	OptionDescription			
	traffic	Traffic log.		
	event	Event log.		
	virus	Antivirus log.		
	webfilter	Web filter log.		
	attack	Attack log.		
	spam	Antispam log.		
	anomaly	Anomaly log.		
	voip	VoIP log.		
	dlp	DLP log.		
	app-ctrl	Application control log.		
	waf	Web application firewall log.		
	dns	DNS detail log.		
	ssh	SSH log.		
	ssl	SSL log.		
	file-filter	File filter log.		
icap	ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	OptionDescription			
	include	Include logs that match the filter.		
	exclude	Exclude logs that match the filter.		

config log syslogd2 override-setting

Override settings for remote syslog server.

```
config log syslogd2 override-setting
    Description: Override settings for remote syslog server.
    set status [enable|disable]
    set server {string}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set facility [kernel|user|...]
    set source-ip {string}
    set format [default|csv|...]
    set priority [default|low]
    set max-log-rate {integer}
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set name {string}
            set custom {string}
        next
    end
    set interface-select-method [auto|specify]
    set interface {string}
    config log-templates
        Description: Custom log templates.
        edit <id>
            set category [traffic|event|...]
            set empty-value-indicator {string}
            set template {string}
        next
    end
end
```

config log syslogd2 override-setting

Parameter	Description	Type	Size	Default
status	Enable/disable remote syslog logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Log to remote syslog server.		
	<i>disable</i>	Do not log to remote syslog server.		
server	Address of remote syslog server.	string	Maximum length: 127	

Parameter	Description	Type	Size	Default
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp
	Option	Description		
	<i>udp</i>	Enable syslogging over UDP.		
	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).		
	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).		
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
facility	Remote syslog facility.	option	-	local7
	Option	Description		
	<i>kernel</i>	Kernel messages.		
	<i>user</i>	Random user-level messages.		
	<i>mail</i>	Mail system.		
	<i>daemon</i>	System daemons.		
	<i>auth</i>	Security/authorization messages.		
	<i>syslog</i>	Messages generated internally by syslog.		
	<i>lpr</i>	Line printer subsystem.		
	<i>news</i>	Network news subsystem.		
	<i>uucp</i>	Network news subsystem.		
	<i>cron</i>	Clock daemon.		
	<i>authpriv</i>	Security/authorization messages (private).		
	<i>ftp</i>	FTP daemon.		
	<i>ntp</i>	NTP daemon.		
	<i>audit</i>	Log audit.		
	<i>alert</i>	Log alert.		
	<i>clock</i>	Clock daemon.		
	<i>local0</i>	Reserved for local use.		
	<i>local1</i>	Reserved for local use.		

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
	Option	Description																
	<i>local2</i>	Reserved for local use.																
	<i>local3</i>	Reserved for local use.																
	<i>local4</i>	Reserved for local use.																
	<i>local5</i>	Reserved for local use.																
	<i>local6</i>	Reserved for local use.																
<i>local7</i>	Reserved for local use.																	
source-ip	Source IP address of syslog.	string	Maximum length: 63															
format	Log format.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr><tr><td><i>json</i></td><td>JSON (JavaScript Object Notation) format.</td></tr><tr><td><i>custom</i></td><td>Custom format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.	<i>json</i>	JSON (JavaScript Object Notation) format.	<i>custom</i>	Custom format.			
	Option	Description																
	<i>default</i>	Syslog format.																
	<i>csv</i>	CSV (Comma Separated Values) format.																
	<i>cef</i>	CEF (Common Event Format) format.																
	<i>rfc5424</i>	Syslog RFC5424 format.																
	<i>json</i>	JSON (JavaScript Object Notation) format.																
<i>custom</i>	Custom format.																	
priority	Set log transmission priority.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Set Syslog transmission priority to default.</td></tr><tr><td><i>low</i></td><td>Set Syslog transmission priority to low.</td></tr></table>	Option	Description	<i>default</i>	Set Syslog transmission priority to default.	<i>low</i>	Set Syslog transmission priority to low.											
	Option	Description																
	<i>default</i>	Set Syslog transmission priority to default.																
<i>low</i>	Set Syslog transmission priority to low.																	
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0														
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>SSL communication with high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>SSL communication with high encryption algorithms.</td></tr></table>	Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.											
	Option	Description																
	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.																
<i>high</i>	SSL communication with high encryption algorithms.																	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>low</i>	SSL communication with low encryption algorithms.		
	<i>disable</i>	Disable SSL communication.		
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default
	Option	Description		
	<i>default</i>	Follow system global setting.		
	<i>SSLv3</i>	SSLv3.		
	<i>TLSv1</i>	TLSv1.		
	<i>TLSv1-1</i>	TLSv1.1.		
	<i>TLSv1-2</i>	TLSv1.2.		
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config custom-field-name

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name [A-Za-z0-9_].	string	Maximum length: 35	
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	

config log-templates

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	OptionDescription			
	traffic	Traffic log.		
	event	Event log.		
	virus	Antivirus log.		
	webfilter	Web filter log.		
	attack	Attack log.		
	spam	Antispam log.		
	anomaly	Anomaly log.		
	voip	VoIP log.		
	dlp	DLP log.		
	app-ctrl	Application control log.		
	waf	Web application firewall log.		
	dns	DNS detail log.		
	ssh	SSH log.		
	ssl	SSL log.		
	file-filter	File filter log.		
icap	ICAP log.			
empty-value-indicator	A character to indicate log field is empty.	string	Maximum length: 1	
template	Log template string.	string	Maximum length: 2047	

config log syslogd2 setting

Global settings for remote syslog server.

```

config log syslogd2 setting
    Description: Global settings for remote syslog server.
    set status [enable|disable]
    set server {string}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set facility [kernel|user|...]
    set source-ip {string}
    set format [default|csv|...]
    set priority [default|low]
    set max-log-rate {integer}
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set name {string}
            set custom {string}
        next
    end
    set interface-select-method [auto|specify]
    set interface {string}
    config log-templates
        Description: Custom log templates.
        edit <id>
            set category [traffic|event|...]
            set empty-value-indicator {string}
            set template {string}
        next
    end
end

```

config log syslogd2 setting

Parameter	Description	Type	Size	Default
status	Enable/disable remote syslog logging.	option	-	disable
	Option Description			
	<i>enable</i>	Log to remote syslog server.		
	<i>disable</i>	Do not log to remote syslog server.		
server	Address of remote syslog server.	string	Maximum length: 127	
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp
	Option Description			
	<i>udp</i>	Enable syslogging over UDP.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).		
	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).		
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
facility	Remote syslog facility.	option	-	local7
	Option	Description		
	<i>kernel</i>	Kernel messages.		
	<i>user</i>	Random user-level messages.		
	<i>mail</i>	Mail system.		
	<i>daemon</i>	System daemons.		
	<i>auth</i>	Security/authorization messages.		
	<i>syslog</i>	Messages generated internally by syslog.		
	<i>lpr</i>	Line printer subsystem.		
	<i>news</i>	Network news subsystem.		
	<i>uucp</i>	Network news subsystem.		
	<i>cron</i>	Clock daemon.		
	<i>authpriv</i>	Security/authorization messages (private).		
	<i>ftp</i>	FTP daemon.		
	<i>ntp</i>	NTP daemon.		
	<i>audit</i>	Log audit.		
	<i>alert</i>	Log alert.		
	<i>clock</i>	Clock daemon.		
	<i>local0</i>	Reserved for local use.		
	<i>local1</i>	Reserved for local use.		
	<i>local2</i>	Reserved for local use.		
<i>local3</i>	Reserved for local use.			

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.							
	Option	Description																
	<i>local4</i>	Reserved for local use.																
	<i>local5</i>	Reserved for local use.																
	<i>local6</i>	Reserved for local use.																
<i>local7</i>	Reserved for local use.																	
source-ip	Source IP address of syslog.	string	Maximum length: 63															
format	Log format.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr><tr><td><i>json</i></td><td>JSON (JavaScript Object Notation) format.</td></tr><tr><td><i>custom</i></td><td>Custom format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.	<i>json</i>	JSON (JavaScript Object Notation) format.	<i>custom</i>	Custom format.			
	Option	Description																
	<i>default</i>	Syslog format.																
	<i>csv</i>	CSV (Comma Separated Values) format.																
	<i>cef</i>	CEF (Common Event Format) format.																
	<i>rfc5424</i>	Syslog RFC5424 format.																
	<i>json</i>	JSON (JavaScript Object Notation) format.																
<i>custom</i>	Custom format.																	
priority	Set log transmission priority.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Set Syslog transmission priority to default.</td></tr><tr><td><i>low</i></td><td>Set Syslog transmission priority to low.</td></tr></table>	Option	Description	<i>default</i>	Set Syslog transmission priority to default.	<i>low</i>	Set Syslog transmission priority to low.											
	Option	Description																
	<i>default</i>	Set Syslog transmission priority to default.																
<i>low</i>	Set Syslog transmission priority to low.																	
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0														
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>SSL communication with high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>SSL communication with high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>SSL communication with low encryption algorithms.</td></tr><tr><td><i>disable</i></td><td>Disable SSL communication.</td></tr></table>	Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.	<i>low</i>	SSL communication with low encryption algorithms.	<i>disable</i>	Disable SSL communication.							
	Option	Description																
	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.																
	<i>high</i>	SSL communication with high encryption algorithms.																
	<i>low</i>	SSL communication with low encryption algorithms.																
<i>disable</i>	Disable SSL communication.																	

Parameter	Description	Type	Size	Default												
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.			
	Option	Description														
	default	Follow system global setting.														
	SSLv3	SSLv3.														
	TLSv1	TLSv1.														
	TLSv1-1	TLSv1.1.														
TLSv1-2	TLSv1.2.															
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35													
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	specify	Set outgoing interface manually.									
	Option	Description														
	auto	Set outgoing interface automatically.														
specify	Set outgoing interface manually.															
interface	Specify outgoing interface to reach server.	string	Maximum length: 15													

config custom-field-name

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name [A-Za-z0-9_].	string	Maximum length: 35	
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	

config log-templates

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	OptionDescription			
	traffic	Traffic log.		
	event	Event log.		
	virus	Antivirus log.		
	webfilter	Web filter log.		
	attack	Attack log.		
	spam	Antispam log.		
	anomaly	Anomaly log.		
	voip	VoIP log.		
	dlp	DLP log.		
	app-ctrl	Application control log.		
	waf	Web application firewall log.		
	dns	DNS detail log.		
	ssh	SSH log.		
	ssl	SSL log.		
	file-filter	File filter log.		
icap	ICAP log.			
empty-value-indicator	A character to indicate log field is empty.	string	Maximum length: 1	
template	Log template string.	string	Maximum length: 2047	

config log syslogd3 filter

Filters for remote system server.


```

config log syslogd3 filter
    Description: Filters for remote system server.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
config free-style
    Description: Free style filters.
    edit <id>
        set category [traffic|event|...]
        set filter {string}
        set filter-type [include|exclude]
    next
end
end

```

config log syslogd3 filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	OptionDescription			
	traffic	Traffic log.		
	event	Event log.		
	virus	Antivirus log.		
	webfilter	Web filter log.		
	attack	Attack log.		
	spam	Antispam log.		
	anomaly	Anomaly log.		
	voip	VoIP log.		
	dlp	DLP log.		
	app-ctrl	Application control log.		
	waf	Web application firewall log.		
	dns	DNS detail log.		
	ssh	SSH log.		
	ssl	SSL log.		
	file-filter	File filter log.		
icap	ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	OptionDescription			
	include	Include logs that match the filter.		
	exclude	Exclude logs that match the filter.		

config log syslogd3 override-filter

Override filters for remote system server.

```
config log syslogd3 override-filter
    Description: Override filters for remote system server.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log syslogd3 override-filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	emergency	Emergency level.		
	alert	Alert level.		
	critical	Critical level.		
	error	Error level.		
	warning	Warning level.		
	notification	Notification level.		
	information	Information level.		
	debug	Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option	Description		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		

config log syslogd3 override-setting

Override settings for remote syslog server.

```
config log syslogd3 override-setting
    Description: Override settings for remote syslog server.
    set status [enable|disable]
    set server {string}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set facility [kernel|user|...]
    set source-ip {string}
    set format [default|csv|...]
    set priority [default|low]
    set max-log-rate {integer}
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set name {string}
            set custom {string}
        next
    end
    set interface-select-method [auto|specify]
    set interface {string}
    config log-templates
        Description: Custom log templates.
        edit <id>
            set category [traffic|event|...]
            set empty-value-indicator {string}
```

```

        set template {string}
    next
end
end

```

config log syslogd3 override-setting

Parameter	Description	Type	Size	Default
status	Enable/disable remote syslog logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Log to remote syslog server.		
	<i>disable</i>	Do not log to remote syslog server.		
server	Address of remote syslog server.	string	Maximum length: 127	
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp
	Option	Description		
	<i>udp</i>	Enable syslogging over UDP.		
	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).		
	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).		
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
facility	Remote syslog facility.	option	-	local7
	Option	Description		
	<i>kernel</i>	Kernel messages.		
	<i>user</i>	Random user-level messages.		
	<i>mail</i>	Mail system.		
	<i>daemon</i>	System daemons.		
	<i>auth</i>	Security/authorization messages.		
	<i>syslog</i>	Messages generated internally by syslog.		
	<i>lpr</i>	Line printer subsystem.		

Parameter	Description	Type	Size	Default																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>news</i></td><td>Network news subsystem.</td></tr><tr><td><i>uucp</i></td><td>Network news subsystem.</td></tr><tr><td><i>cron</i></td><td>Clock daemon.</td></tr><tr><td><i>authpriv</i></td><td>Security/authorization messages (private).</td></tr><tr><td><i>ftp</i></td><td>FTP daemon.</td></tr><tr><td><i>ntp</i></td><td>NTP daemon.</td></tr><tr><td><i>audit</i></td><td>Log audit.</td></tr><tr><td><i>alert</i></td><td>Log alert.</td></tr><tr><td><i>clock</i></td><td>Clock daemon.</td></tr><tr><td><i>local0</i></td><td>Reserved for local use.</td></tr><tr><td><i>local1</i></td><td>Reserved for local use.</td></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
	Option	Description																																						
	<i>news</i>	Network news subsystem.																																						
	<i>uucp</i>	Network news subsystem.																																						
	<i>cron</i>	Clock daemon.																																						
	<i>authpriv</i>	Security/authorization messages (private).																																						
	<i>ftp</i>	FTP daemon.																																						
	<i>ntp</i>	NTP daemon.																																						
	<i>audit</i>	Log audit.																																						
	<i>alert</i>	Log alert.																																						
	<i>clock</i>	Clock daemon.																																						
	<i>local0</i>	Reserved for local use.																																						
	<i>local1</i>	Reserved for local use.																																						
	<i>local2</i>	Reserved for local use.																																						
	<i>local3</i>	Reserved for local use.																																						
	<i>local4</i>	Reserved for local use.																																						
	<i>local5</i>	Reserved for local use.																																						
	<i>local6</i>	Reserved for local use.																																						
<i>local7</i>	Reserved for local use.																																							
source-ip	Source IP address of syslog.	string	Maximum length: 63																																					
format	Log format.	option	-	default																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr><tr><td><i>json</i></td><td>JSON (JavaScript Object Notation) format.</td></tr><tr><td><i>custom</i></td><td>Custom format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.	<i>json</i>	JSON (JavaScript Object Notation) format.	<i>custom</i>	Custom format.																									
	Option	Description																																						
	<i>default</i>	Syslog format.																																						
	<i>csv</i>	CSV (Comma Separated Values) format.																																						
	<i>cef</i>	CEF (Common Event Format) format.																																						
	<i>rfc5424</i>	Syslog RFC5424 format.																																						
	<i>json</i>	JSON (JavaScript Object Notation) format.																																						
<i>custom</i>	Custom format.																																							
priority	Set log transmission priority.	option	-	default																																				

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>default</i>	Set Syslog transmission priority to default.		
	<i>low</i>	Set Syslog transmission priority to low.		
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable
	Option	Description		
	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.		
	<i>high</i>	SSL communication with high encryption algorithms.		
	<i>low</i>	SSL communication with low encryption algorithms.		
	<i>disable</i>	Disable SSL communication.		
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default
	Option	Description		
	<i>default</i>	Follow system global setting.		
	<i>SSLv3</i>	SSLv3.		
	<i>TLSv1</i>	TLSv1.		
	<i>TLSv1-1</i>	TLSv1.1.		
	<i>TLSv1-2</i>	TLSv1.2.		
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config custom-field-name

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name [A-Za-z0-9_].	string	Maximum length: 35	
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	

config log-templates

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	Option	Description		
	traffic	Traffic log.		
	event	Event log.		
	virus	Antivirus log.		
	webfilter	Web filter log.		
	attack	Attack log.		
	spam	Antispam log.		
	anomaly	Anomaly log.		
	voip	VoIP log.		
	dlp	DLP log.		
	app-ctrl	Application control log.		
	waf	Web application firewall log.		
	dns	DNS detail log.		
	ssh	SSH log.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
empty-value-indicator	A character to indicate log field is empty.	string	Maximum length: 1	
template	Log template string.	string	Maximum length: 2047	

config log syslogd3 setting

Global settings for remote syslog server.

```

config log syslogd3 setting
    Description: Global settings for remote syslog server.
    set status [enable|disable]
    set server {string}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set facility [kernel|user|...]
    set source-ip {string}
    set format [default|csv|...]
    set priority [default|low]
    set max-log-rate {integer}
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set name {string}
            set custom {string}
        next
    end
    set interface-select-method [auto|specify]
    set interface {string}
    config log-templates
        Description: Custom log templates.
        edit <id>
            set category [traffic|event|...]
            set empty-value-indicator {string}
            set template {string}
        next
    end
end
end

```

config log syslogd3 setting

Parameter	Description	Type	Size	Default																								
status	Enable/disable remote syslog logging.	option	-	disable																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Log to remote syslog server.</td></tr><tr><td><i>disable</i></td><td>Do not log to remote syslog server.</td></tr></table>				Option	Description	<i>enable</i>	Log to remote syslog server.	<i>disable</i>	Do not log to remote syslog server.																		
	Option	Description																										
	<i>enable</i>	Log to remote syslog server.																										
	<i>disable</i>	Do not log to remote syslog server.																										
server	Address of remote syslog server.	string	Maximum length: 127																									
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>udp</i></td><td>Enable syslogging over UDP.</td></tr><tr><td><i>legacy-reliable</i></td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td><i>reliable</i></td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>				Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).																
	Option	Description																										
	<i>udp</i>	Enable syslogging over UDP.																										
	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).																										
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).																											
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514																								
facility	Remote syslog facility.	option	-	local7																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>kernel</i></td><td>Kernel messages.</td></tr><tr><td><i>user</i></td><td>Random user-level messages.</td></tr><tr><td><i>mail</i></td><td>Mail system.</td></tr><tr><td><i>daemon</i></td><td>System daemons.</td></tr><tr><td><i>auth</i></td><td>Security/authorization messages.</td></tr><tr><td><i>syslog</i></td><td>Messages generated internally by syslog.</td></tr><tr><td><i>lpr</i></td><td>Line printer subsystem.</td></tr><tr><td><i>news</i></td><td>Network news subsystem.</td></tr><tr><td><i>uucp</i></td><td>Network news subsystem.</td></tr><tr><td><i>cron</i></td><td>Clock daemon.</td></tr><tr><td><i>authpriv</i></td><td>Security/authorization messages (private).</td></tr></table>				Option	Description	<i>kernel</i>	Kernel messages.	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslog.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).
	Option	Description																										
	<i>kernel</i>	Kernel messages.																										
	<i>user</i>	Random user-level messages.																										
	<i>mail</i>	Mail system.																										
	<i>daemon</i>	System daemons.																										
	<i>auth</i>	Security/authorization messages.																										
	<i>syslog</i>	Messages generated internally by syslog.																										
	<i>lpr</i>	Line printer subsystem.																										
	<i>news</i>	Network news subsystem.																										
	<i>uucp</i>	Network news subsystem.																										
	<i>cron</i>	Clock daemon.																										
<i>authpriv</i>	Security/authorization messages (private).																											

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ftp</i></td><td>FTP daemon.</td></tr><tr><td><i>ntp</i></td><td>NTP daemon.</td></tr><tr><td><i>audit</i></td><td>Log audit.</td></tr><tr><td><i>alert</i></td><td>Log alert.</td></tr><tr><td><i>clock</i></td><td>Clock daemon.</td></tr><tr><td><i>local0</i></td><td>Reserved for local use.</td></tr><tr><td><i>local1</i></td><td>Reserved for local use.</td></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
	Option	Description																														
	<i>ftp</i>	FTP daemon.																														
	<i>ntp</i>	NTP daemon.																														
	<i>audit</i>	Log audit.																														
	<i>alert</i>	Log alert.																														
	<i>clock</i>	Clock daemon.																														
	<i>local0</i>	Reserved for local use.																														
	<i>local1</i>	Reserved for local use.																														
	<i>local2</i>	Reserved for local use.																														
	<i>local3</i>	Reserved for local use.																														
	<i>local4</i>	Reserved for local use.																														
	<i>local5</i>	Reserved for local use.																														
	<i>local6</i>	Reserved for local use.																														
<i>local7</i>	Reserved for local use.																															
source-ip	Source IP address of syslog.	string	Maximum length: 63																													
format	Log format.	option	-	default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr><tr><td><i>json</i></td><td>JSON (JavaScript Object Notation) format.</td></tr><tr><td><i>custom</i></td><td>Custom format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.	<i>json</i>	JSON (JavaScript Object Notation) format.	<i>custom</i>	Custom format.																	
	Option	Description																														
	<i>default</i>	Syslog format.																														
	<i>csv</i>	CSV (Comma Separated Values) format.																														
	<i>cef</i>	CEF (Common Event Format) format.																														
	<i>rfc5424</i>	Syslog RFC5424 format.																														
	<i>json</i>	JSON (JavaScript Object Notation) format.																														
<i>custom</i>	Custom format.																															
priority	Set log transmission priority.	option	-	default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Set Syslog transmission priority to default.</td></tr><tr><td><i>low</i></td><td>Set Syslog transmission priority to low.</td></tr></table>	Option	Description	<i>default</i>	Set Syslog transmission priority to default.	<i>low</i>	Set Syslog transmission priority to low.																									
	Option	Description																														
	<i>default</i>	Set Syslog transmission priority to default.																														
<i>low</i>	Set Syslog transmission priority to low.																															

Parameter	Description	Type	Size	Default												
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0												
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>SSL communication with high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>SSL communication with high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>SSL communication with low encryption algorithms.</td></tr><tr><td><i>disable</i></td><td>Disable SSL communication.</td></tr></table>	Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.	<i>low</i>	SSL communication with low encryption algorithms.	<i>disable</i>	Disable SSL communication.					
Option	Description															
<i>high-medium</i>	SSL communication with high and medium encryption algorithms.															
<i>high</i>	SSL communication with high encryption algorithms.															
<i>low</i>	SSL communication with low encryption algorithms.															
<i>disable</i>	Disable SSL communication.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35													
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.									
Option	Description															
<i>auto</i>	Set outgoing interface automatically.															
<i>specify</i>	Set outgoing interface manually.															
interface	Specify outgoing interface to reach server.	string	Maximum length: 15													

config custom-field-name

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name [A-Za-z0-9_].	string	Maximum length: 35	
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	

config log-templates

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	Option	Description		
	traffic	Traffic log.		
	event	Event log.		
	virus	Antivirus log.		
	webfilter	Web filter log.		
	attack	Attack log.		
	spam	Antispam log.		
	anomaly	Anomaly log.		
	voip	VoIP log.		
	dlp	DLP log.		
	app-ctrl	Application control log.		
	waf	Web application firewall log.		
	dns	DNS detail log.		
	ssh	SSH log.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
empty-value-indicator	A character to indicate log field is empty.	string	Maximum length: 1	
template	Log template string.	string	Maximum length: 2047	

config log syslogd4 filter

Filters for remote system server.

```

config log syslogd4 filter
    Description: Filters for remote system server.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end

```

config log syslogd4 filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
	Option	Description																				
	<i>emergency</i>	Emergency level.																				
	<i>alert</i>	Alert level.																				
	<i>critical</i>	Critical level.																				
	<i>error</i>	Error level.																				
	<i>warning</i>	Warning level.																				
	<i>notification</i>	Notification level.																				
	<i>information</i>	Information level.																				
	<i>debug</i>	Debug level.																				
forward-traffic	Enable/disable forward traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.															
	Option	Description																				
	<i>enable</i>	Enable forward traffic logging.																				
	<i>disable</i>	Disable forward traffic logging.																				
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local in or out traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable local in or out traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.															
	Option	Description																				
	<i>enable</i>	Enable local in or out traffic logging.																				
	<i>disable</i>	Disable local in or out traffic logging.																				
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multicast traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable multicast traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.															
	Option	Description																				
	<i>enable</i>	Enable multicast traffic logging.																				
	<i>disable</i>	Disable multicast traffic logging.																				
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.															
	Option	Description																				
	<i>enable</i>	Enable sniffer traffic logging.																				
	<i>disable</i>	Disable sniffer traffic logging.																				
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable																		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>webfilter</i></td><td>Web filter log.</td></tr><tr><td><i>attack</i></td><td>Attack log.</td></tr><tr><td><i>spam</i></td><td>Antispam log.</td></tr><tr><td><i>anomaly</i></td><td>Anomaly log.</td></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr></table>	Option	Description	<i>webfilter</i>	Web filter log.	<i>attack</i>	Attack log.	<i>spam</i>	Antispam log.	<i>anomaly</i>	Anomaly log.	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.			
	Option	Description																														
	<i>webfilter</i>	Web filter log.																														
	<i>attack</i>	Attack log.																														
	<i>spam</i>	Antispam log.																														
	<i>anomaly</i>	Anomaly log.																														
	<i>voip</i>	VoIP log.																														
	<i>dlp</i>	DLP log.																														
	<i>app-ctrl</i>	Application control log.																														
	<i>waf</i>	Web application firewall log.																														
	<i>dns</i>	DNS detail log.																														
	<i>ssh</i>	SSH log.																														
	<i>ssl</i>	SSL log.																														
	<i>file-filter</i>	File filter log.																														
<i>icap</i>	ICAP log.																															
filter	Free style filter string.	string	Maximum length: 1023																													
filter-type	Include/exclude logs that match the filter.	option	-	include																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																									
	Option	Description																														
	<i>include</i>	Include logs that match the filter.																														
<i>exclude</i>	Exclude logs that match the filter.																															

config log syslogd4 override-filter

Override filters for remote system server.

```
config log syslogd4 override-filter
  Description: Override filters for remote system server.
  set severity [emergency|alert|...]
  set forward-traffic [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set sniffer-traffic [enable|disable]
  set ztna-traffic [enable|disable]
  set http-transaction [enable|disable]
  set anomaly [enable|disable]
  set voip [enable|disable]
```

```

config free-style
  Description: Free style filters.
  edit <id>
    set category [traffic|event|...]
    set filter {string}
    set filter-type [include|exclude]
  next
end
end

```

config log syslogd4 override-filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
<i>debug</i>	Debug level.			
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	OptionDescription			
	traffic	Traffic log.		
	event	Event log.		
	virus	Antivirus log.		
	webfilter	Web filter log.		
	attack	Attack log.		
	spam	Antispam log.		
	anomaly	Anomaly log.		
	voip	VoIP log.		
	dlp	DLP log.		
	app-ctrl	Application control log.		
	waf	Web application firewall log.		
	dns	DNS detail log.		
	ssh	SSH log.		
	ssl	SSL log.		
	file-filter	File filter log.		
icap	ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	OptionDescription			
	include	Include logs that match the filter.		
	exclude	Exclude logs that match the filter.		

config log syslogd4 override-setting

Override settings for remote syslog server.

```
config log syslogd4 override-setting
    Description: Override settings for remote syslog server.
    set status [enable|disable]
    set server {string}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set facility [kernel|user|...]
    set source-ip {string}
    set format [default|csv|...]
    set priority [default|low]
    set max-log-rate {integer}
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set name {string}
            set custom {string}
        next
    end
    set interface-select-method [auto|specify]
    set interface {string}
    config log-templates
        Description: Custom log templates.
        edit <id>
            set category [traffic|event|...]
            set empty-value-indicator {string}
            set template {string}
        next
    end
end
```

config log syslogd4 override-setting

Parameter	Description	Type	Size	Default
status	Enable/disable remote syslog logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Log to remote syslog server.		
	<i>disable</i>	Do not log to remote syslog server.		
server	Address of remote syslog server.	string	Maximum length: 127	

Parameter	Description	Type	Size	Default
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp
	Option	Description		
	udp	Enable syslogging over UDP.		
	legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).		
	reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).		
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
facility	Remote syslog facility.	option	-	local7
	Option	Description		
	kernel	Kernel messages.		
	user	Random user-level messages.		
	mail	Mail system.		
	daemon	System daemons.		
	auth	Security/authorization messages.		
	syslog	Messages generated internally by syslog.		
	lpr	Line printer subsystem.		
	news	Network news subsystem.		
	uucp	Network news subsystem.		
	cron	Clock daemon.		
	authpriv	Security/authorization messages (private).		
	ftp	FTP daemon.		
	ntp	NTP daemon.		
	audit	Log audit.		
	alert	Log alert.		
	clock	Clock daemon.		
	local0	Reserved for local use.		
	local1	Reserved for local use.		

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
	Option	Description																
	<i>local2</i>	Reserved for local use.																
	<i>local3</i>	Reserved for local use.																
	<i>local4</i>	Reserved for local use.																
	<i>local5</i>	Reserved for local use.																
	<i>local6</i>	Reserved for local use.																
	<i>local7</i>	Reserved for local use.																
source-ip	Source IP address of syslog.	string	Maximum length: 63															
format	Log format.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr><tr><td><i>json</i></td><td>JSON (JavaScript Object Notation) format.</td></tr><tr><td><i>custom</i></td><td>Custom format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.	<i>json</i>	JSON (JavaScript Object Notation) format.	<i>custom</i>	Custom format.			
	Option	Description																
	<i>default</i>	Syslog format.																
	<i>csv</i>	CSV (Comma Separated Values) format.																
	<i>cef</i>	CEF (Common Event Format) format.																
	<i>rfc5424</i>	Syslog RFC5424 format.																
	<i>json</i>	JSON (JavaScript Object Notation) format.																
<i>custom</i>	Custom format.																	
priority	Set log transmission priority.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Set Syslog transmission priority to default.</td></tr><tr><td><i>low</i></td><td>Set Syslog transmission priority to low.</td></tr></table>	Option	Description	<i>default</i>	Set Syslog transmission priority to default.	<i>low</i>	Set Syslog transmission priority to low.											
	Option	Description																
	<i>default</i>	Set Syslog transmission priority to default.																
<i>low</i>	Set Syslog transmission priority to low.																	
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0														
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>SSL communication with high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>SSL communication with high encryption algorithms.</td></tr></table>	Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.											
	Option	Description																
	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.																
<i>high</i>	SSL communication with high encryption algorithms.																	

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>low</i></td><td>SSL communication with low encryption algorithms.</td></tr><tr><td><i>disable</i></td><td>Disable SSL communication.</td></tr></table>	Option	Description	<i>low</i>	SSL communication with low encryption algorithms.	<i>disable</i>	Disable SSL communication.									
	Option	Description														
	<i>low</i>	SSL communication with low encryption algorithms.														
<i>disable</i>	Disable SSL communication.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
	Option	Description														
	<i>default</i>	Follow system global setting.														
	<i>SSLv3</i>	SSLv3.														
	<i>TLSv1</i>	TLSv1.														
	<i>TLSv1-1</i>	TLSv1.1.														
<i>TLSv1-2</i>	TLSv1.2.															
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35													
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.									
	Option	Description														
	<i>auto</i>	Set outgoing interface automatically.														
<i>specify</i>	Set outgoing interface manually.															
interface	Specify outgoing interface to reach server.	string	Maximum length: 15													

config custom-field-name

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name [A-Za-z0-9_].	string	Maximum length: 35	
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	

config log-templates

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	OptionDescription			
	traffic	Traffic log.		
	event	Event log.		
	virus	Antivirus log.		
	webfilter	Web filter log.		
	attack	Attack log.		
	spam	Antispam log.		
	anomaly	Anomaly log.		
	voip	VoIP log.		
	dlp	DLP log.		
	app-ctrl	Application control log.		
	waf	Web application firewall log.		
	dns	DNS detail log.		
	ssh	SSH log.		
	ssl	SSL log.		
	file-filter	File filter log.		
icap	ICAP log.			
empty-value-indicator	A character to indicate log field is empty.	string	Maximum length: 1	
template	Log template string.	string	Maximum length: 2047	

config log syslogd4 setting

Global settings for remote syslog server.

```

config log syslogd4 setting
    Description: Global settings for remote syslog server.
    set status [enable|disable]
    set server {string}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set facility [kernel|user|...]
    set source-ip {string}
    set format [default|csv|...]
    set priority [default|low]
    set max-log-rate {integer}
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set name {string}
            set custom {string}
        next
    end
    set interface-select-method [auto|specify]
    set interface {string}
    config log-templates
        Description: Custom log templates.
        edit <id>
            set category [traffic|event|...]
            set empty-value-indicator {string}
            set template {string}
        next
    end
end

```

config log syslogd4 setting

Parameter	Description	Type	Size	Default						
status	Enable/disable remote syslog logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Log to remote syslog server.</td></tr><tr><td><i>disable</i></td><td>Do not log to remote syslog server.</td></tr></table>	Option	Description	<i>enable</i>	Log to remote syslog server.	<i>disable</i>	Do not log to remote syslog server.			
Option	Description									
<i>enable</i>	Log to remote syslog server.									
<i>disable</i>	Do not log to remote syslog server.									
server	Address of remote syslog server.	string	Maximum length: 127							
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>udp</i></td><td>Enable syslogging over UDP.</td></tr></table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.					
Option	Description									
<i>udp</i>	Enable syslogging over UDP.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).		
	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).		
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
facility	Remote syslog facility.	option	-	local7
	Option	Description		
	<i>kernel</i>	Kernel messages.		
	<i>user</i>	Random user-level messages.		
	<i>mail</i>	Mail system.		
	<i>daemon</i>	System daemons.		
	<i>auth</i>	Security/authorization messages.		
	<i>syslog</i>	Messages generated internally by syslog.		
	<i>lpr</i>	Line printer subsystem.		
	<i>news</i>	Network news subsystem.		
	<i>uucp</i>	Network news subsystem.		
	<i>cron</i>	Clock daemon.		
	<i>authpriv</i>	Security/authorization messages (private).		
	<i>ftp</i>	FTP daemon.		
	<i>ntp</i>	NTP daemon.		
	<i>audit</i>	Log audit.		
	<i>alert</i>	Log alert.		
	<i>clock</i>	Clock daemon.		
	<i>local0</i>	Reserved for local use.		
	<i>local1</i>	Reserved for local use.		
	<i>local2</i>	Reserved for local use.		
<i>local3</i>	Reserved for local use.			

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.							
	Option	Description																
	<i>local4</i>	Reserved for local use.																
	<i>local5</i>	Reserved for local use.																
	<i>local6</i>	Reserved for local use.																
<i>local7</i>	Reserved for local use.																	
source-ip	Source IP address of syslog.	string	Maximum length: 63															
format	Log format.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr><tr><td><i>json</i></td><td>JSON (JavaScript Object Notation) format.</td></tr><tr><td><i>custom</i></td><td>Custom format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.	<i>json</i>	JSON (JavaScript Object Notation) format.	<i>custom</i>	Custom format.			
	Option	Description																
	<i>default</i>	Syslog format.																
	<i>csv</i>	CSV (Comma Separated Values) format.																
	<i>cef</i>	CEF (Common Event Format) format.																
	<i>rfc5424</i>	Syslog RFC5424 format.																
	<i>json</i>	JSON (JavaScript Object Notation) format.																
<i>custom</i>	Custom format.																	
priority	Set log transmission priority.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Set Syslog transmission priority to default.</td></tr><tr><td><i>low</i></td><td>Set Syslog transmission priority to low.</td></tr></table>	Option	Description	<i>default</i>	Set Syslog transmission priority to default.	<i>low</i>	Set Syslog transmission priority to low.											
	Option	Description																
	<i>default</i>	Set Syslog transmission priority to default.																
<i>low</i>	Set Syslog transmission priority to low.																	
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0														
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>SSL communication with high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>SSL communication with high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>SSL communication with low encryption algorithms.</td></tr><tr><td><i>disable</i></td><td>Disable SSL communication.</td></tr></table>	Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.	<i>low</i>	SSL communication with low encryption algorithms.	<i>disable</i>	Disable SSL communication.							
	Option	Description																
	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.																
	<i>high</i>	SSL communication with high encryption algorithms.																
	<i>low</i>	SSL communication with low encryption algorithms.																
<i>disable</i>	Disable SSL communication.																	

Parameter	Description	Type	Size	Default												
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.			
	Option	Description														
	default	Follow system global setting.														
	SSLv3	SSLv3.														
	TLSv1	TLSv1.														
	TLSv1-1	TLSv1.1.														
TLSv1-2	TLSv1.2.															
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35													
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	specify	Set outgoing interface manually.									
	Option	Description														
	auto	Set outgoing interface automatically.														
specify	Set outgoing interface manually.															
interface	Specify outgoing interface to reach server.	string	Maximum length: 15													

config custom-field-name

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name [A-Za-z0-9_].	string	Maximum length: 35	
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	

config log-templates

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	OptionDescription			
	traffic	Traffic log.		
	event	Event log.		
	virus	Antivirus log.		
	webfilter	Web filter log.		
	attack	Attack log.		
	spam	Antispam log.		
	anomaly	Anomaly log.		
	voip	VoIP log.		
	dlp	DLP log.		
	app-ctrl	Application control log.		
	waf	Web application firewall log.		
	dns	DNS detail log.		
	ssh	SSH log.		
	ssl	SSL log.		
	file-filter	File filter log.		
icap	ICAP log.			
empty-value-indicator	A character to indicate log field is empty.	string	Maximum length: 1	
template	Log template string.	string	Maximum length: 2047	

config log syslogd filter

Filters for remote system server.

```

config log syslogd filter
    Description: Filters for remote system server.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end

```

config log syslogd filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	OptionDescription			
	traffic	Traffic log.		
	event	Event log.		
	virus	Antivirus log.		
	webfilter	Web filter log.		
	attack	Attack log.		
	spam	Antispam log.		
	anomaly	Anomaly log.		
	voip	VoIP log.		
	dlp	DLP log.		
	app-ctrl	Application control log.		
	waf	Web application firewall log.		
	dns	DNS detail log.		
	ssh	SSH log.		
	ssl	SSL log.		
	file-filter	File filter log.		
icap	ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	OptionDescription			
	include	Include logs that match the filter.		
	exclude	Exclude logs that match the filter.		

config log syslogd override-filter

Override filters for remote system server.

```
config log syslogd override-filter
    Description: Override filters for remote system server.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end
```

config log syslogd override-filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option	Description		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		

config log syslogd override-setting

Override settings for remote syslog server.

```
config log syslogd override-setting
    Description: Override settings for remote syslog server.
    set status [enable|disable]
    set server {string}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set facility [kernel|user|...]
    set source-ip {string}
    set format [default|csv|...]
    set priority [default|low]
    set max-log-rate {integer}
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set name {string}
            set custom {string}
        next
    end
    set interface-select-method [auto|specify]
    set interface {string}
    config log-templates
        Description: Custom log templates.
        edit <id>
            set category [traffic|event|...]
            set empty-value-indicator {string}
```



```

        set template {string}
    next
end
end

```

config log syslogd override-setting

Parameter	Description	Type	Size	Default																
status	Enable/disable remote syslog logging.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Log to remote syslog server.</td></tr><tr><td><i>disable</i></td><td>Do not log to remote syslog server.</td></tr></table>				Option	Description	<i>enable</i>	Log to remote syslog server.	<i>disable</i>	Do not log to remote syslog server.										
	Option	Description																		
	<i>enable</i>	Log to remote syslog server.																		
	<i>disable</i>	Do not log to remote syslog server.																		
server	Address of remote syslog server.	string	Maximum length: 127																	
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>udp</i></td><td>Enable syslogging over UDP.</td></tr><tr><td><i>legacy-reliable</i></td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td><i>reliable</i></td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>				Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).								
	Option	Description																		
	<i>udp</i>	Enable syslogging over UDP.																		
	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).																		
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).																			
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514																
facility	Remote syslog facility.	option	-	local7																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>kernel</i></td><td>Kernel messages.</td></tr><tr><td><i>user</i></td><td>Random user-level messages.</td></tr><tr><td><i>mail</i></td><td>Mail system.</td></tr><tr><td><i>daemon</i></td><td>System daemons.</td></tr><tr><td><i>auth</i></td><td>Security/authorization messages.</td></tr><tr><td><i>syslog</i></td><td>Messages generated internally by syslog.</td></tr><tr><td><i>lpr</i></td><td>Line printer subsystem.</td></tr></table>				Option	Description	<i>kernel</i>	Kernel messages.	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslog.	<i>lpr</i>	Line printer subsystem.
	Option	Description																		
	<i>kernel</i>	Kernel messages.																		
	<i>user</i>	Random user-level messages.																		
	<i>mail</i>	Mail system.																		
	<i>daemon</i>	System daemons.																		
	<i>auth</i>	Security/authorization messages.																		
	<i>syslog</i>	Messages generated internally by syslog.																		
<i>lpr</i>	Line printer subsystem.																			

Parameter	Description	Type	Size	Default																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>news</i></td><td>Network news subsystem.</td></tr><tr><td><i>uucp</i></td><td>Network news subsystem.</td></tr><tr><td><i>cron</i></td><td>Clock daemon.</td></tr><tr><td><i>authpriv</i></td><td>Security/authorization messages (private).</td></tr><tr><td><i>ftp</i></td><td>FTP daemon.</td></tr><tr><td><i>ntp</i></td><td>NTP daemon.</td></tr><tr><td><i>audit</i></td><td>Log audit.</td></tr><tr><td><i>alert</i></td><td>Log alert.</td></tr><tr><td><i>clock</i></td><td>Clock daemon.</td></tr><tr><td><i>local0</i></td><td>Reserved for local use.</td></tr><tr><td><i>local1</i></td><td>Reserved for local use.</td></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
	Option	Description																																						
	<i>news</i>	Network news subsystem.																																						
	<i>uucp</i>	Network news subsystem.																																						
	<i>cron</i>	Clock daemon.																																						
	<i>authpriv</i>	Security/authorization messages (private).																																						
	<i>ftp</i>	FTP daemon.																																						
	<i>ntp</i>	NTP daemon.																																						
	<i>audit</i>	Log audit.																																						
	<i>alert</i>	Log alert.																																						
	<i>clock</i>	Clock daemon.																																						
	<i>local0</i>	Reserved for local use.																																						
	<i>local1</i>	Reserved for local use.																																						
	<i>local2</i>	Reserved for local use.																																						
	<i>local3</i>	Reserved for local use.																																						
	<i>local4</i>	Reserved for local use.																																						
	<i>local5</i>	Reserved for local use.																																						
	<i>local6</i>	Reserved for local use.																																						
<i>local7</i>	Reserved for local use.																																							
source-ip	Source IP address of syslog.	string	Maximum length: 63																																					
format	Log format.	option	-	default																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr><tr><td><i>json</i></td><td>JSON (JavaScript Object Notation) format.</td></tr><tr><td><i>custom</i></td><td>Custom format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.	<i>json</i>	JSON (JavaScript Object Notation) format.	<i>custom</i>	Custom format.																									
	Option	Description																																						
	<i>default</i>	Syslog format.																																						
	<i>csv</i>	CSV (Comma Separated Values) format.																																						
	<i>cef</i>	CEF (Common Event Format) format.																																						
	<i>rfc5424</i>	Syslog RFC5424 format.																																						
	<i>json</i>	JSON (JavaScript Object Notation) format.																																						
<i>custom</i>	Custom format.																																							
priority	Set log transmission priority.	option	-	default																																				

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>default</i>	Set Syslog transmission priority to default.		
	<i>low</i>	Set Syslog transmission priority to low.		
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable
	Option	Description		
	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.		
	<i>high</i>	SSL communication with high encryption algorithms.		
	<i>low</i>	SSL communication with low encryption algorithms.		
	<i>disable</i>	Disable SSL communication.		
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default
	Option	Description		
	<i>default</i>	Follow system global setting.		
	<i>SSLv3</i>	SSLv3.		
	<i>TLSv1</i>	TLSv1.		
	<i>TLSv1-1</i>	TLSv1.1.		
	<i>TLSv1-2</i>	TLSv1.2.		
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config custom-field-name

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name [A-Za-z0-9_].	string	Maximum length: 35	
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	

config log-templates

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	Option	Description		
	traffic	Traffic log.		
	event	Event log.		
	virus	Antivirus log.		
	webfilter	Web filter log.		
	attack	Attack log.		
	spam	Antispam log.		
	anomaly	Anomaly log.		
	voip	VoIP log.		
	dlp	DLP log.		
	app-ctrl	Application control log.		
	waf	Web application firewall log.		
	dns	DNS detail log.		
	ssh	SSH log.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
empty-value-indicator	A character to indicate log field is empty.	string	Maximum length: 1	
template	Log template string.	string	Maximum length: 2047	

config log syslogd setting

Global settings for remote syslog server.

```

config log syslogd setting
    Description: Global settings for remote syslog server.
    set status [enable|disable]
    set server {string}
    set mode [udp|legacy-reliable|...]
    set port {integer}
    set facility [kernel|user|...]
    set source-ip {string}
    set format [default|csv|...]
    set priority [default|low]
    set max-log-rate {integer}
    set enc-algorithm [high-medium|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set name {string}
            set custom {string}
        next
    end
    set interface-select-method [auto|specify]
    set interface {string}
    config log-templates
        Description: Custom log templates.
        edit <id>
            set category [traffic|event|...]
            set empty-value-indicator {string}
            set template {string}
        next
    end
end
end

```

config log syslogd setting

Parameter	Description	Type	Size	Default																								
status	Enable/disable remote syslog logging.	option	-	disable																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Log to remote syslog server.</td></tr><tr><td><i>disable</i></td><td>Do not log to remote syslog server.</td></tr></table>	Option	Description	<i>enable</i>	Log to remote syslog server.	<i>disable</i>	Do not log to remote syslog server.																					
Option	Description																											
<i>enable</i>	Log to remote syslog server.																											
<i>disable</i>	Do not log to remote syslog server.																											
server	Address of remote syslog server.	string	Maximum length: 127																									
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>udp</i></td><td>Enable syslogging over UDP.</td></tr><tr><td><i>legacy-reliable</i></td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td><i>reliable</i></td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>	Option	Description	<i>udp</i>	Enable syslogging over UDP.	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).																			
Option	Description																											
<i>udp</i>	Enable syslogging over UDP.																											
<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).																											
<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).																											
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514																								
facility	Remote syslog facility.	option	-	local7																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>kernel</i></td><td>Kernel messages.</td></tr><tr><td><i>user</i></td><td>Random user-level messages.</td></tr><tr><td><i>mail</i></td><td>Mail system.</td></tr><tr><td><i>daemon</i></td><td>System daemons.</td></tr><tr><td><i>auth</i></td><td>Security/authorization messages.</td></tr><tr><td><i>syslog</i></td><td>Messages generated internally by syslog.</td></tr><tr><td><i>lpr</i></td><td>Line printer subsystem.</td></tr><tr><td><i>news</i></td><td>Network news subsystem.</td></tr><tr><td><i>uucp</i></td><td>Network news subsystem.</td></tr><tr><td><i>cron</i></td><td>Clock daemon.</td></tr><tr><td><i>authpriv</i></td><td>Security/authorization messages (private).</td></tr></table>	Option	Description	<i>kernel</i>	Kernel messages.	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslog.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).			
Option	Description																											
<i>kernel</i>	Kernel messages.																											
<i>user</i>	Random user-level messages.																											
<i>mail</i>	Mail system.																											
<i>daemon</i>	System daemons.																											
<i>auth</i>	Security/authorization messages.																											
<i>syslog</i>	Messages generated internally by syslog.																											
<i>lpr</i>	Line printer subsystem.																											
<i>news</i>	Network news subsystem.																											
<i>uucp</i>	Network news subsystem.																											
<i>cron</i>	Clock daemon.																											
<i>authpriv</i>	Security/authorization messages (private).																											

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ftp</i></td><td>FTP daemon.</td></tr><tr><td><i>ntp</i></td><td>NTP daemon.</td></tr><tr><td><i>audit</i></td><td>Log audit.</td></tr><tr><td><i>alert</i></td><td>Log alert.</td></tr><tr><td><i>clock</i></td><td>Clock daemon.</td></tr><tr><td><i>local0</i></td><td>Reserved for local use.</td></tr><tr><td><i>local1</i></td><td>Reserved for local use.</td></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
	Option	Description																														
	<i>ftp</i>	FTP daemon.																														
	<i>ntp</i>	NTP daemon.																														
	<i>audit</i>	Log audit.																														
	<i>alert</i>	Log alert.																														
	<i>clock</i>	Clock daemon.																														
	<i>local0</i>	Reserved for local use.																														
	<i>local1</i>	Reserved for local use.																														
	<i>local2</i>	Reserved for local use.																														
	<i>local3</i>	Reserved for local use.																														
	<i>local4</i>	Reserved for local use.																														
	<i>local5</i>	Reserved for local use.																														
	<i>local6</i>	Reserved for local use.																														
<i>local7</i>	Reserved for local use.																															
source-ip	Source IP address of syslog.	string	Maximum length: 63																													
format	Log format.	option	-	default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr><tr><td><i>json</i></td><td>JSON (JavaScript Object Notation) format.</td></tr><tr><td><i>custom</i></td><td>Custom format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.	<i>json</i>	JSON (JavaScript Object Notation) format.	<i>custom</i>	Custom format.																	
	Option	Description																														
	<i>default</i>	Syslog format.																														
	<i>csv</i>	CSV (Comma Separated Values) format.																														
	<i>cef</i>	CEF (Common Event Format) format.																														
	<i>rfc5424</i>	Syslog RFC5424 format.																														
	<i>json</i>	JSON (JavaScript Object Notation) format.																														
<i>custom</i>	Custom format.																															
priority	Set log transmission priority.	option	-	default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Set Syslog transmission priority to default.</td></tr><tr><td><i>low</i></td><td>Set Syslog transmission priority to low.</td></tr></table>	Option	Description	<i>default</i>	Set Syslog transmission priority to default.	<i>low</i>	Set Syslog transmission priority to low.																									
	Option	Description																														
	<i>default</i>	Set Syslog transmission priority to default.																														
<i>low</i>	Set Syslog transmission priority to low.																															

Parameter	Description	Type	Size	Default												
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0												
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>SSL communication with high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>SSL communication with high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>SSL communication with low encryption algorithms.</td></tr><tr><td><i>disable</i></td><td>Disable SSL communication.</td></tr></table>	Option	Description	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.	<i>high</i>	SSL communication with high encryption algorithms.	<i>low</i>	SSL communication with low encryption algorithms.	<i>disable</i>	Disable SSL communication.					
	Option	Description														
	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.														
	<i>high</i>	SSL communication with high encryption algorithms.														
	<i>low</i>	SSL communication with low encryption algorithms.														
	<i>disable</i>	Disable SSL communication.														
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
	Option	Description														
	<i>default</i>	Follow system global setting.														
	<i>SSLv3</i>	SSLv3.														
	<i>TLSv1</i>	TLSv1.														
	<i>TLSv1-1</i>	TLSv1.1.														
<i>TLSv1-2</i>	TLSv1.2.															
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35													
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.									
	Option	Description														
	<i>auto</i>	Set outgoing interface automatically.														
<i>specify</i>	Set outgoing interface manually.															
interface	Specify outgoing interface to reach server.	string	Maximum length: 15													

config custom-field-name

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name [A-Za-z0-9_].	string	Maximum length: 35	
custom	Field custom name [A-Za-z0-9_].	string	Maximum length: 35	

config log-templates

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	Option	Description		
	traffic	Traffic log.		
	event	Event log.		
	virus	Antivirus log.		
	webfilter	Web filter log.		
	attack	Attack log.		
	spam	Antispam log.		
	anomaly	Anomaly log.		
	voip	VoIP log.		
	dlp	DLP log.		
	app-ctrl	Application control log.		
	waf	Web application firewall log.		
	dns	DNS detail log.		
	ssh	SSH log.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr></table>				Option	Description	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.
	Option	Description										
	<i>ssl</i>	SSL log.										
	<i>file-filter</i>	File filter log.										
	<i>icap</i>	ICAP log.										
empty-value-indicator	A character to indicate log field is empty.	string	Maximum length: 1									
template	Log template string.	string	Maximum length: 2047									

config log tacacs+accounting2 filter

Settings for TACACS+ accounting events filter.

```
config log tacacs+accounting2 filter
    Description: Settings for TACACS+ accounting events filter.
    set login-audit [enable|disable]
    set config-change-audit [enable|disable]
    set cli-cmd-audit [enable|disable]
end
```

config log tacacs+accounting2 filter

Parameter	Description	Type	Size	Default						
login-audit	Enable/disable TACACS+ accounting for login events audit.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ accounting for login events audit.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ accounting for login events audit.</td></tr></table>				Option	Description	<i>enable</i>	Enable TACACS+ accounting for login events audit.	<i>disable</i>	Disable TACACS+ accounting for login events audit.
Option	Description									
<i>enable</i>	Enable TACACS+ accounting for login events audit.									
<i>disable</i>	Disable TACACS+ accounting for login events audit.									
config-change-audit	Enable/disable TACACS+ accounting for configuration change events audit.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ accounting for configuration change events audit.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ accounting for configuration change events audit.</td></tr></table>				Option	Description	<i>enable</i>	Enable TACACS+ accounting for configuration change events audit.	<i>disable</i>	Disable TACACS+ accounting for configuration change events audit.
Option	Description									
<i>enable</i>	Enable TACACS+ accounting for configuration change events audit.									
<i>disable</i>	Disable TACACS+ accounting for configuration change events audit.									

Parameter	Description	Type	Size	Default
cli-cmd-audit	Enable/disable TACACS+ accounting for CLI commands audit.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable TACACS+ accounting for CLI commands audit.		
	<i>disable</i>	Disable TACACS+ accounting for CLI commands audit.		

config log tacacs+accounting2 setting

Settings for TACACS+ accounting.

```
config log tacacs+accounting2 setting
    Description: Settings for TACACS+ accounting.
    set status [enable|disable]
    set server {string}
    set server-key {password}
    set source-ip {string}
    set interface-select-method [auto|specify]
    set interface {string}
end
```

config log tacacs+accounting2 setting

Parameter	Description	Type	Size	Default
status	Enable/disable TACACS+ accounting.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable TACACS+ accounting.		
	<i>disable</i>	Disable TACACS+ accounting.		
server	Address of TACACS+ server.	string	Maximum length: 63	
server-key	Key to access the TACACS+ server.	password	Not Specified	
source-ip	Source IP address for communication to TACACS+ server.	string	Maximum length: 63	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config log tacacs+accounting3 filter

Settings for TACACS+ accounting events filter.

```
config log tacacs+accounting3 filter
    Description: Settings for TACACS+ accounting events filter.
    set login-audit [enable|disable]
    set config-change-audit [enable|disable]
    set cli-cmd-audit [enable|disable]
end
```

config log tacacs+accounting3 filter

Parameter	Description	Type	Size	Default
login-audit	Enable/disable TACACS+ accounting for login events audit.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable TACACS+ accounting for login events audit.		
	<i>disable</i>	Disable TACACS+ accounting for login events audit.		
config-change-audit	Enable/disable TACACS+ accounting for configuration change events audit.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable TACACS+ accounting for configuration change events audit.		
	<i>disable</i>	Disable TACACS+ accounting for configuration change events audit.		
cli-cmd-audit	Enable/disable TACACS+ accounting for CLI commands audit.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable TACACS+ accounting for CLI commands audit.		
	<i>disable</i>	Disable TACACS+ accounting for CLI commands audit.		

config log tacacs+accounting3 setting

Settings for TACACS+ accounting.

```
config log tacacs+accounting3 setting
    Description: Settings for TACACS+ accounting.
    set status [enable|disable]
    set server {string}
    set server-key {password}
    set source-ip {string}
    set interface-select-method [auto|specify]
    set interface {string}
end
```

config log tacacs+accounting3 setting

Parameter	Description	Type	Size	Default
status	Enable/disable TACACS+ accounting.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable TACACS+ accounting.		
	<i>disable</i>	Disable TACACS+ accounting.		
server	Address of TACACS+ server.	string	Maximum length: 63	
server-key	Key to access the TACACS+ server.	password	Not Specified	
source-ip	Source IP address for communication to TACACS+ server.	string	Maximum length: 63	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		

Parameter	Description	Type	Size	Default
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config log tacacs+accounting filter

Settings for TACACS+ accounting events filter.

```
config log tacacs+accounting filter
  Description: Settings for TACACS+ accounting events filter.
  set login-audit [enable|disable]
  set config-change-audit [enable|disable]
  set cli-cmd-audit [enable|disable]
end
```

config log tacacs+accounting filter

Parameter	Description	Type	Size	Default						
login-audit	Enable/disable TACACS+ accounting for login events audit.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ accounting for login events audit.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ accounting for login events audit.</td></tr></table>	Option	Description	<i>enable</i>	Enable TACACS+ accounting for login events audit.	<i>disable</i>	Disable TACACS+ accounting for login events audit.			
Option	Description									
<i>enable</i>	Enable TACACS+ accounting for login events audit.									
<i>disable</i>	Disable TACACS+ accounting for login events audit.									
config-change-audit	Enable/disable TACACS+ accounting for configuration change events audit.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ accounting for configuration change events audit.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ accounting for configuration change events audit.</td></tr></table>	Option	Description	<i>enable</i>	Enable TACACS+ accounting for configuration change events audit.	<i>disable</i>	Disable TACACS+ accounting for configuration change events audit.			
Option	Description									
<i>enable</i>	Enable TACACS+ accounting for configuration change events audit.									
<i>disable</i>	Disable TACACS+ accounting for configuration change events audit.									
cli-cmd-audit	Enable/disable TACACS+ accounting for CLI commands audit.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ accounting for CLI commands audit.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ accounting for CLI commands audit.</td></tr></table>	Option	Description	<i>enable</i>	Enable TACACS+ accounting for CLI commands audit.	<i>disable</i>	Disable TACACS+ accounting for CLI commands audit.			
Option	Description									
<i>enable</i>	Enable TACACS+ accounting for CLI commands audit.									
<i>disable</i>	Disable TACACS+ accounting for CLI commands audit.									

config log tacacs+accounting setting

Settings for TACACS+ accounting.

```
config log tacacs+accounting setting
    Description: Settings for TACACS+ accounting.
    set status [enable|disable]
    set server {string}
    set server-key {password}
    set source-ip {string}
    set interface-select-method [auto|specify]
    set interface {string}
end
```

config log tacacs+accounting setting

Parameter	Description	Type	Size	Default						
status	Enable/disable TACACS+ accounting.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ accounting.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ accounting.</td></tr></table>				Option	Description	<i>enable</i>	Enable TACACS+ accounting.	<i>disable</i>	Disable TACACS+ accounting.
	Option	Description								
	<i>enable</i>	Enable TACACS+ accounting.								
<i>disable</i>	Disable TACACS+ accounting.									
server	Address of TACACS+ server.	string	Maximum length: 63							
server-key	Key to access the TACACS+ server.	password	Not Specified							
source-ip	Source IP address for communication to TACACS+ server.	string	Maximum length: 63							
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.
	Option	Description								
	<i>auto</i>	Set outgoing interface automatically.								
<i>specify</i>	Set outgoing interface manually.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							

config log threat-weight

Configure threat weight settings.

```
config log threat-weight
  Description: Configure threat weight settings.
  set status [enable|disable]
  config level
    Description: Score mapping for threat weight levels.
    set low {integer}
    set medium {integer}
    set high {integer}
    set critical {integer}
  end
  set blocked-connection [disable|low|...]
  set failed-connection [disable|low|...]
  set url-block-detected [disable|low|...]
  set botnet-connection-detected [disable|low|...]
  config malware
    Description: Anti-virus malware threat weight settings.
    set virus-infected [disable|low|...]
    set fortindr [disable|low|...]
    set fortisandbox [disable|low|...]
    set file-blocked [disable|low|...]
    set command-blocked [disable|low|...]
    set oversized [disable|low|...]
    set virus-scan-error [disable|low|...]
    set switch-proto [disable|low|...]
    set mimefragmented [disable|low|...]
    set virus-file-type-executable [disable|low|...]
    set virus-outbreak-prevention [disable|low|...]
    set content-disarm [disable|low|...]
    set malware-list [disable|low|...]
    set ems-threat-feed [disable|low|...]
    set fsa-malicious [disable|low|...]
    set fsa-high-risk [disable|low|...]
    set fsa-medium-risk [disable|low|...]
  end
  config ips
    Description: IPS threat weight settings.
    set info-severity [disable|low|...]
    set low-severity [disable|low|...]
    set medium-severity [disable|low|...]
    set high-severity [disable|low|...]
    set critical-severity [disable|low|...]
  end
  config web
    Description: Web filtering threat weight settings.
    edit <id>
      set category {integer}
      set level [disable|low|...]
    next
  end
  config geolocation
    Description: Geolocation-based threat weight settings.
    edit <id>
      set country {string}
      set level [disable|low|...]
    next
  end
```



```

config application
    Description: Application-control threat weight settings.
    edit <id>
        set category {integer}
        set level [disable|low|...]
    next
end
end

```

config log threat-weight

Parameter	Description	Type	Size	Default
status	Enable/disable the threat weight feature.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable the threat weight feature.		
	<i>disable</i>	Disable the threat weight feature.		
blocked-connection	Threat weight score for blocked connections.	option	-	high
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for blocked connections.		
	<i>low</i>	Use the low level score for blocked connections.		
	<i>medium</i>	Use the medium level score for blocked connections.		
	<i>high</i>	Use the high level score for blocked connections.		
	<i>critical</i>	Use the critical level score for blocked connections.		
failed-connection	Threat weight score for failed connections.	option	-	low
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for failed connections.		
	<i>low</i>	Use the low level score for failed connections.		
	<i>medium</i>	Use the medium level score for failed connections.		
	<i>high</i>	Use the high level score for failed connections.		
	<i>critical</i>	Use the critical level score for failed connections.		
url-block-detected	Threat weight score for URL blocking.	option	-	high

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for URL blocking.</td></tr><tr><td><i>low</i></td><td>Use the low level score for URL blocking.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for URL blocking.</td></tr><tr><td><i>high</i></td><td>Use the high level score for URL blocking.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for URL blocking.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for URL blocking.	<i>low</i>	Use the low level score for URL blocking.	<i>medium</i>	Use the medium level score for URL blocking.	<i>high</i>	Use the high level score for URL blocking.	<i>critical</i>	Use the critical level score for URL blocking.			
	Option	Description														
	<i>disable</i>	Disable threat weight scoring for URL blocking.														
	<i>low</i>	Use the low level score for URL blocking.														
	<i>medium</i>	Use the medium level score for URL blocking.														
	<i>high</i>	Use the high level score for URL blocking.														
<i>critical</i>	Use the critical level score for URL blocking.															
botnet-connection-detected	Threat weight score for detected botnet connections.	option	-	critical												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for detected botnet connections.</td></tr><tr><td><i>low</i></td><td>Use the low level score for detected botnet connections.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for detected botnet connections.</td></tr><tr><td><i>high</i></td><td>Use the high level score for detected botnet connections.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for detected botnet connections.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for detected botnet connections.	<i>low</i>	Use the low level score for detected botnet connections.	<i>medium</i>	Use the medium level score for detected botnet connections.	<i>high</i>	Use the high level score for detected botnet connections.	<i>critical</i>	Use the critical level score for detected botnet connections.			
	Option	Description														
	<i>disable</i>	Disable threat weight scoring for detected botnet connections.														
	<i>low</i>	Use the low level score for detected botnet connections.														
	<i>medium</i>	Use the medium level score for detected botnet connections.														
	<i>high</i>	Use the high level score for detected botnet connections.														
<i>critical</i>	Use the critical level score for detected botnet connections.															

config level

Parameter	Description	Type	Size	Default
low	Low level score value.	integer	Minimum value: 1 Maximum value: 100	5
medium	Medium level score value.	integer	Minimum value: 1 Maximum value: 100	10
high	High level score value.	integer	Minimum value: 1 Maximum value: 100	30
critical	Critical level score value.	integer	Minimum value: 1 Maximum value: 100	50

config malware

Parameter	Description	Type	Size	Default
virus-infected	Threat weight score for virus (infected) detected.	option	-	critical
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for virus (infected) detected.		
	<i>low</i>	Use the low level score for virus (infected) detected.		
	<i>medium</i>	Use the medium level score for virus (infected) detected.		
	<i>high</i>	Use the high level score for virus (infected) detected.		
	<i>critical</i>	Use the critical level score for virus (infected) detected.		
fortindr	Threat weight score for FortiNDR-detected virus.	option	-	critical
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for virus detected by FortiNDR.		
	<i>low</i>	Use the low level score for virus detected by FortiNDR.		
	<i>medium</i>	Use the medium level score for virus detected by FortiNDR.		
	<i>high</i>	Use the high level score for virus detected by FortiNDR.		
	<i>critical</i>	Use the critical level score for virus detected by FortiNDR.		
fortisandbox	Threat weight score for FortiSandbox-detected virus.	option	-	critical
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for virus detected by FortiSandbox.		
	<i>low</i>	Use the low level score for virus detected by FortiSandbox.		
	<i>medium</i>	Use the medium level score for virus detected by FortiSandbox.		
	<i>high</i>	Use the high level score for virus detected by FortiSandbox.		
	<i>critical</i>	Use the critical level score for virus detected by FortiSandbox.		
file-blocked	Threat weight score for blocked file detected.	option	-	low
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for blocked file detected.		
	<i>low</i>	Use the low level score for blocked file detected.		
	<i>medium</i>	Use the medium level score for blocked file detected.		
	<i>high</i>	Use the high level score for blocked file detected.		
	<i>critical</i>	Use the critical level score for blocked file detected.		

Parameter	Description	Type	Size	Default
command-blocked	Threat weight score for blocked command detected.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for blocked command detected.		
	<i>low</i>	Use the low level score for blocked command detected.		
	<i>medium</i>	Use the medium level score for blocked command detected.		
	<i>high</i>	Use the high level score for blocked command detected.		
	<i>critical</i>	Use the critical level score for blocked command detected.		
oversized	Threat weight score for oversized file detected.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for oversized file detected.		
	<i>low</i>	Use the low level score for oversized file detected.		
	<i>medium</i>	Use the medium level score for oversized file detected.		
	<i>high</i>	Use the high level score for oversized file detected.		
	<i>critical</i>	Use the critical level score for oversized file detected.		
virus-scan-error	Threat weight score for virus (scan error) detected.	option	-	high
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for virus (scan error) detected.		
	<i>low</i>	Use the low level score for virus (scan error) detected.		
	<i>medium</i>	Use the medium level score for virus (scan error) detected.		
	<i>high</i>	Use the high level score for virus (scan error) detected.		
	<i>critical</i>	Use the critical level score for virus (scan error) detected.		
switch-proto	Threat weight score for switch proto detected.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for switch proto detected.		
	<i>low</i>	Use the low level score for switch proto detected.		
	<i>medium</i>	Use the medium level score for switch proto detected.		
	<i>high</i>	Use the high level score for switch proto detected.		
	<i>critical</i>	Use the critical level score for switch proto detected.		
mimefragmented	Threat weight score for mimefragmented detected.	option	-	disable

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for mimefragmented detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for mimefragmented detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for mimefragmented detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for mimefragmented detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for mimefragmented detected.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for mimefragmented detected.	<i>low</i>	Use the low level score for mimefragmented detected.	<i>medium</i>	Use the medium level score for mimefragmented detected.	<i>high</i>	Use the high level score for mimefragmented detected.	<i>critical</i>	Use the critical level score for mimefragmented detected.			
	Option	Description														
	<i>disable</i>	Disable threat weight scoring for mimefragmented detected.														
	<i>low</i>	Use the low level score for mimefragmented detected.														
	<i>medium</i>	Use the medium level score for mimefragmented detected.														
	<i>high</i>	Use the high level score for mimefragmented detected.														
	<i>critical</i>	Use the critical level score for mimefragmented detected.														
virus-file-type-executable	Threat weight score for virus (file type executable) detected.	option	-	medium												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for virus (filetype executable) detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for virus (filetype executable) detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for virus (filetype executable) detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for virus (filetype executable) detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for virus (filetype executable) detected.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for virus (filetype executable) detected.	<i>low</i>	Use the low level score for virus (filetype executable) detected.	<i>medium</i>	Use the medium level score for virus (filetype executable) detected.	<i>high</i>	Use the high level score for virus (filetype executable) detected.	<i>critical</i>	Use the critical level score for virus (filetype executable) detected.			
	Option	Description														
	<i>disable</i>	Disable threat weight scoring for virus (filetype executable) detected.														
	<i>low</i>	Use the low level score for virus (filetype executable) detected.														
	<i>medium</i>	Use the medium level score for virus (filetype executable) detected.														
	<i>high</i>	Use the high level score for virus (filetype executable) detected.														
	<i>critical</i>	Use the critical level score for virus (filetype executable) detected.														
virus-outbreak-prevention	Threat weight score for virus (outbreak prevention) event.	option	-	critical												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for virus (outbreak prevention) event.</td></tr><tr><td><i>low</i></td><td>Use the low level score for virus (outbreak prevention) event.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for virus (outbreak prevention) event.</td></tr><tr><td><i>high</i></td><td>Use the high level score for virus (outbreak prevention) event.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for virus (outbreak prevention) event.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for virus (outbreak prevention) event.	<i>low</i>	Use the low level score for virus (outbreak prevention) event.	<i>medium</i>	Use the medium level score for virus (outbreak prevention) event.	<i>high</i>	Use the high level score for virus (outbreak prevention) event.	<i>critical</i>	Use the critical level score for virus (outbreak prevention) event.			
	Option	Description														
	<i>disable</i>	Disable threat weight scoring for virus (outbreak prevention) event.														
	<i>low</i>	Use the low level score for virus (outbreak prevention) event.														
	<i>medium</i>	Use the medium level score for virus (outbreak prevention) event.														
	<i>high</i>	Use the high level score for virus (outbreak prevention) event.														
	<i>critical</i>	Use the critical level score for virus (outbreak prevention) event.														
content-disarm	Threat weight score for virus (content disarm) detected.	option	-	medium												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for virus (content disarm) detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for virus (content disarm) detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for virus (content disarm) detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for virus (content disarm) detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for virus (content disarm) detected.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for virus (content disarm) detected.	<i>low</i>	Use the low level score for virus (content disarm) detected.	<i>medium</i>	Use the medium level score for virus (content disarm) detected.	<i>high</i>	Use the high level score for virus (content disarm) detected.	<i>critical</i>	Use the critical level score for virus (content disarm) detected.			
	Option	Description														
	<i>disable</i>	Disable threat weight scoring for virus (content disarm) detected.														
	<i>low</i>	Use the low level score for virus (content disarm) detected.														
	<i>medium</i>	Use the medium level score for virus (content disarm) detected.														
	<i>high</i>	Use the high level score for virus (content disarm) detected.														
	<i>critical</i>	Use the critical level score for virus (content disarm) detected.														

Parameter	Description	Type	Size	Default												
malware-list	Threat weight score for virus (malware list) detected.	option	-	medium												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for virus (malware list) detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for virus (malware list) detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for virus (malware list) detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for virus (malware list) detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for virus (malware list) detected.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for virus (malware list) detected.	<i>low</i>	Use the low level score for virus (malware list) detected.	<i>medium</i>	Use the medium level score for virus (malware list) detected.	<i>high</i>	Use the high level score for virus (malware list) detected.	<i>critical</i>	Use the critical level score for virus (malware list) detected.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for virus (malware list) detected.															
<i>low</i>	Use the low level score for virus (malware list) detected.															
<i>medium</i>	Use the medium level score for virus (malware list) detected.															
<i>high</i>	Use the high level score for virus (malware list) detected.															
<i>critical</i>	Use the critical level score for virus (malware list) detected.															
ems-threat-feed	Threat weight score for virus (EMS threat feed) detected.	option	-	medium												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for virus (EMS threat feed) detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for virus (EMS threat feed) detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for virus (EMS threat feed) detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for virus (EMS threat feed) detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for virus (EMS threat feed) detected.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for virus (EMS threat feed) detected.	<i>low</i>	Use the low level score for virus (EMS threat feed) detected.	<i>medium</i>	Use the medium level score for virus (EMS threat feed) detected.	<i>high</i>	Use the high level score for virus (EMS threat feed) detected.	<i>critical</i>	Use the critical level score for virus (EMS threat feed) detected.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for virus (EMS threat feed) detected.															
<i>low</i>	Use the low level score for virus (EMS threat feed) detected.															
<i>medium</i>	Use the medium level score for virus (EMS threat feed) detected.															
<i>high</i>	Use the high level score for virus (EMS threat feed) detected.															
<i>critical</i>	Use the critical level score for virus (EMS threat feed) detected.															
fsa-malicious	Threat weight score for FortiSandbox malicious malware detected.	option	-	critical												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for FortiSandbox malicious malware detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for FortiSandbox malicious malware detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for FortiSandbox malicious malware detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for FortiSandbox malicious malware detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for FortiSandbox malicious malware detected.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for FortiSandbox malicious malware detected.	<i>low</i>	Use the low level score for FortiSandbox malicious malware detected.	<i>medium</i>	Use the medium level score for FortiSandbox malicious malware detected.	<i>high</i>	Use the high level score for FortiSandbox malicious malware detected.	<i>critical</i>	Use the critical level score for FortiSandbox malicious malware detected.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for FortiSandbox malicious malware detected.															
<i>low</i>	Use the low level score for FortiSandbox malicious malware detected.															
<i>medium</i>	Use the medium level score for FortiSandbox malicious malware detected.															
<i>high</i>	Use the high level score for FortiSandbox malicious malware detected.															
<i>critical</i>	Use the critical level score for FortiSandbox malicious malware detected.															
fsa-high-risk	Threat weight score for FortiSandbox high risk malware detected.	option	-	high												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for FortiSandbox high risk malware detected.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for FortiSandbox high risk malware detected.											
Option	Description															
<i>disable</i>	Disable threat weight scoring for FortiSandbox high risk malware detected.															

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>low</i></td><td>Use the low level score for FortiSandbox high risk malware detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for FortiSandbox high risk malware detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for FortiSandbox high risk malware detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for FortiSandbox high risk malware detected.</td></tr></table>	Option	Description	<i>low</i>	Use the low level score for FortiSandbox high risk malware detected.	<i>medium</i>	Use the medium level score for FortiSandbox high risk malware detected.	<i>high</i>	Use the high level score for FortiSandbox high risk malware detected.	<i>critical</i>	Use the critical level score for FortiSandbox high risk malware detected.					
	Option	Description														
	<i>low</i>	Use the low level score for FortiSandbox high risk malware detected.														
	<i>medium</i>	Use the medium level score for FortiSandbox high risk malware detected.														
	<i>high</i>	Use the high level score for FortiSandbox high risk malware detected.														
<i>critical</i>	Use the critical level score for FortiSandbox high risk malware detected.															
fsa-medium-risk	Threat weight score for FortiSandbox medium risk malware detected.	option	-	medium												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for FortiSandbox medium risk malware detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for FortiSandbox medium risk malware detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for FortiSandbox medium risk malware detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for FortiSandbox medium risk malware detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for FortiSandbox medium risk malware detected.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for FortiSandbox medium risk malware detected.	<i>low</i>	Use the low level score for FortiSandbox medium risk malware detected.	<i>medium</i>	Use the medium level score for FortiSandbox medium risk malware detected.	<i>high</i>	Use the high level score for FortiSandbox medium risk malware detected.	<i>critical</i>	Use the critical level score for FortiSandbox medium risk malware detected.			
	Option	Description														
	<i>disable</i>	Disable threat weight scoring for FortiSandbox medium risk malware detected.														
	<i>low</i>	Use the low level score for FortiSandbox medium risk malware detected.														
	<i>medium</i>	Use the medium level score for FortiSandbox medium risk malware detected.														
<i>high</i>	Use the high level score for FortiSandbox medium risk malware detected.															
<i>critical</i>	Use the critical level score for FortiSandbox medium risk malware detected.															

config ips

Parameter	Description	Type	Size	Default
info-severity	Threat weight score for IPS info severity events.	option	-	disable
	Option	Description		
	disable	Disable threat weight scoring for IPS info severity events.		
	low	Use the low level score for IPS info severity events.		
	medium	Use the medium level score for IPS info severity events.		
	high	Use the high level score for IPS info severity events.		
	critical	Use the critical level score for IPS info severity events.		
low-severity	Threat weight score for IPS low severity events.	option	-	low
	Option	Description		
	disable	Disable threat weight scoring for IPS low severity events.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>low</i>	Use the low level score for IPS low severity events.		
	<i>medium</i>	Use the medium level score for IPS low severity events.		
	<i>high</i>	Use the high level score for IPS low severity events.		
	<i>critical</i>	Use the critical level score for IPS low severity events.		
medium-severity	Threat weight score for IPS medium severity events.	option	-	medium
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for IPS medium severity events.		
	<i>low</i>	Use the low level score for IPS medium severity events.		
	<i>medium</i>	Use the medium level score for IPS medium severity events.		
	<i>high</i>	Use the high level score for IPS medium severity events.		
	<i>critical</i>	Use the critical level score for IPS medium severity events.		
high-severity	Threat weight score for IPS high severity events.	option	-	high
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for IPS high severity events.		
	<i>low</i>	Use the low level score for IPS high severity events.		
	<i>medium</i>	Use the medium level score for IPS high severity events.		
	<i>high</i>	Use the high level score for IPS high severity events.		
	<i>critical</i>	Use the critical level score for IPS high severity events.		
critical-severity	Threat weight score for IPS critical severity events.	option	-	critical
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for IPS critical severity events.		
	<i>low</i>	Use the low level score for IPS critical severity events.		
	<i>medium</i>	Use the medium level score for IPS critical severity events.		
	<i>high</i>	Use the high level score for IPS critical severity events.		
	<i>critical</i>	Use the critical level score for IPS critical severity events.		

config web

Parameter	Description	Type	Size	Default												
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0												
category	Threat weight score for web category filtering matches.	integer	Minimum value: 0 Maximum value: 255	0												
level	Threat weight score for web category filtering matches.	option	-	low												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable threat weight scoring for web category filtering matches.</td></tr><tr><td>low</td><td>Use the low level score for web category filtering matches.</td></tr><tr><td>medium</td><td>Use the medium level score for web category filtering matches.</td></tr><tr><td>high</td><td>Use the high level score for web category filtering matches.</td></tr><tr><td>critical</td><td>Use the critical level score for web category filtering matches.</td></tr></table>				Option	Description	disable	Disable threat weight scoring for web category filtering matches.	low	Use the low level score for web category filtering matches.	medium	Use the medium level score for web category filtering matches.	high	Use the high level score for web category filtering matches.	critical	Use the critical level score for web category filtering matches.
Option	Description															
disable	Disable threat weight scoring for web category filtering matches.															
low	Use the low level score for web category filtering matches.															
medium	Use the medium level score for web category filtering matches.															
high	Use the high level score for web category filtering matches.															
critical	Use the critical level score for web category filtering matches.															

config geolocation

Parameter	Description	Type	Size	Default												
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0												
country	Country code.	string	Maximum length: 2													
level	Threat weight score for Geolocation-based events.	option	-	low												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for Geolocation-based events.</td></tr><tr><td><i>low</i></td><td>Use the low level score for Geolocation-based events.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for Geolocation-based events.</td></tr><tr><td><i>high</i></td><td>Use the high level score for Geolocation-based events.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for Geolocation-based events.</td></tr></table>				Option	Description	<i>disable</i>	Disable threat weight scoring for Geolocation-based events.	<i>low</i>	Use the low level score for Geolocation-based events.	<i>medium</i>	Use the medium level score for Geolocation-based events.	<i>high</i>	Use the high level score for Geolocation-based events.	<i>critical</i>	Use the critical level score for Geolocation-based events.
Option	Description															
<i>disable</i>	Disable threat weight scoring for Geolocation-based events.															
<i>low</i>	Use the low level score for Geolocation-based events.															
<i>medium</i>	Use the medium level score for Geolocation-based events.															
<i>high</i>	Use the high level score for Geolocation-based events.															
<i>critical</i>	Use the critical level score for Geolocation-based events.															

config application

Parameter	Description	Type	Size	Default												
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0												
category	Application category.	integer	Minimum value: 0 Maximum value: 65535	0												
level	Threat weight score for Application events.	option	-	low												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for Application events.</td></tr><tr><td><i>low</i></td><td>Use the low level score for Application events.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for Application events.</td></tr><tr><td><i>high</i></td><td>Use the high level score for Application events.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for Application events.</td></tr></table>				Option	Description	<i>disable</i>	Disable threat weight scoring for Application events.	<i>low</i>	Use the low level score for Application events.	<i>medium</i>	Use the medium level score for Application events.	<i>high</i>	Use the high level score for Application events.	<i>critical</i>	Use the critical level score for Application events.
Option	Description															
<i>disable</i>	Disable threat weight scoring for Application events.															
<i>low</i>	Use the low level score for Application events.															
<i>medium</i>	Use the medium level score for Application events.															
<i>high</i>	Use the high level score for Application events.															
<i>critical</i>	Use the critical level score for Application events.															

config log webtrends filter

Filters for WebTrends.

```

config log webtrends filter
    Description: Filters for WebTrends.
    set severity [emergency|alert|...]
    set forward-traffic [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set sniffer-traffic [enable|disable]
    set ztna-traffic [enable|disable]
    set http-transaction [enable|disable]
    set anomaly [enable|disable]
    set voip [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
end

```

config log webtrends filter

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log to WebTrends.	option	-	information
	Option	Description		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		

Parameter	Description	Type	Size	Default
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		
http-transaction	Enable/disable log http-transaction messages.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable http transaction logging.		
	<i>disable</i>	Disable http transaction logging.		
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		

config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	Option	Description		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		

Parameter	Description	Type	Size	Default																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>virus</i></td><td>Antivirus log.</td></tr><tr><td><i>webfilter</i></td><td>Web filter log.</td></tr><tr><td><i>attack</i></td><td>Attack log.</td></tr><tr><td><i>spam</i></td><td>Antispam log.</td></tr><tr><td><i>anomaly</i></td><td>Anomaly log.</td></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr></table>	Option	Description	<i>virus</i>	Antivirus log.	<i>webfilter</i>	Web filter log.	<i>attack</i>	Attack log.	<i>spam</i>	Antispam log.	<i>anomaly</i>	Anomaly log.	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.			
	Option	Description																																
	<i>virus</i>	Antivirus log.																																
	<i>webfilter</i>	Web filter log.																																
	<i>attack</i>	Attack log.																																
	<i>spam</i>	Antispam log.																																
	<i>anomaly</i>	Anomaly log.																																
	<i>voip</i>	VoIP log.																																
	<i>dlp</i>	DLP log.																																
	<i>app-ctrl</i>	Application control log.																																
	<i>waf</i>	Web application firewall log.																																
	<i>dns</i>	DNS detail log.																																
	<i>ssh</i>	SSH log.																																
	<i>ssl</i>	SSL log.																																
	<i>file-filter</i>	File filter log.																																
<i>icap</i>	ICAP log.																																	
filter	Free style filter string.	string	Maximum length: 1023																															
filter-type	Include/exclude logs that match the filter.	option	-	include																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																											
	Option	Description																																
	<i>include</i>	Include logs that match the filter.																																
<i>exclude</i>	Exclude logs that match the filter.																																	

config log webtrends setting

Settings for WebTrends.

```
config log webtrends setting
    Description: Settings for WebTrends.
    set status [enable|disable]
    set server {string}
end
```

config log webtrends setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to WebTrends.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging to WebTrends.		
	<i>disable</i>	Disble logging to WebTrends.		
server	Address of the remote WebTrends server.	string	Maximum length: 63	

mgmt-data

This section includes syntax for the following commands:

- [config mgmt-data status on page 615](#)

config mgmt-data status

Status for mgmt-data.

```
config mgmt-data status
    Description: Status for mgmt-data.
end
```

report

This section includes syntax for the following commands:

- [config report layout on page 616](#)
- [config report setting on page 624](#)
- [config report sql status on page 625](#)

config report layout

Report layout configuration.

```
config report layout
  Description: Report layout configuration.
  edit <name>
    set title {string}
    set subtitle {string}
    set description {string}
    set style-theme {string}
    set options {option1}, {option2}, ...
    set format {option1}, {option2}, ...
    set schedule-type [demand|daily|...]
    set day [sunday|monday|...]
    set time {user}
    set cutoff-option [run-time|custom]
    set cutoff-time {user}
    set email-send [enable|disable]
    set email-recipients {string}
    set max-pdf-report {integer}
  config page
    Description: Configure report page.
    set paper [a4|letter]
    set column-break-before {option1}, {option2}, ...
    set page-break-before {option1}, {option2}, ...
    set options {option1}, {option2}, ...
  config header
    Description: Configure report page header.
    set style {string}
  config header-item
    Description: Configure report header item.
    edit <id>
      set description {string}
      set type [text|image]
      set style {string}
      set content {string}
      set img-src {string}
    next
  end
end
```



```

config footer
  Description: Configure report page footer.
  set style {string}
  config footer-item
    Description: Configure report footer item.
    edit <id>
      set description {string}
      set type [text|image]
      set style {string}
      set content {string}
      set img-src {string}
    next
  end
end
end
config body-item
  Description: Configure report body item.
  edit <id>
    set description {string}
    set type [text|image|...]
    set style {string}
    set top-n {integer}
    config parameters
      Description: Parameters.
      edit <id>
        set name {string}
        set value {string}
      next
    end
    set text-component [text|heading1|...]
    set content {string}
    set img-src {string}
    set chart {string}
    set chart-options {option1}, {option2}, ...
    set misc-component [hline|page-break|...]
    set title {string}
  next
end
next
end
end

```

config report layout

Parameter	Description	Type	Size	Default
name	Report layout name.	string	Maximum length: 35	
title	Report title.	string	Maximum length: 127	
subtitle	Report subtitle.	string	Maximum length: 127	

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 127	
style-theme	Report style theme.	string	Maximum length: 35	
options	Report layout options.	option	-	include-table-of-content auto-numbering- heading view- chart-as- heading
	Option	Description		
	<i>include-table-of-content</i>	Include table of content in the report.		
	<i>auto-numbering-heading</i>	Prepend heading with auto numbering.		
	<i>view-chart-as-heading</i>	Auto add heading for each chart.		
	<i>show-html-navbar-before-heading</i>	Show HTML navigation bar before each heading.		
	<i>dummy-option</i>	Use this option if you need none of the above options.		
format	Report format.	option	-	pdf
	Option	Description		
	<i>pdf</i>	PDF.		
schedule-type	Report schedule type.	option	-	daily
	Option	Description		
	<i>demand</i>	Run on demand.		
	<i>daily</i>	Schedule daily.		
	<i>weekly</i>	Schedule weekly.		
day	Schedule days of week to generate report.	option	-	sunday
	Option	Description		
	<i>sunday</i>	Sunday.		

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>monday</i></td><td>Monday.</td></tr><tr><td><i>tuesday</i></td><td>Tuesday.</td></tr><tr><td><i>wednesday</i></td><td>Wednesday.</td></tr><tr><td><i>thursday</i></td><td>Thursday.</td></tr><tr><td><i>friday</i></td><td>Friday.</td></tr><tr><td><i>saturday</i></td><td>Saturday.</td></tr></table>	Option	Description	<i>monday</i>	Monday.	<i>tuesday</i>	Tuesday.	<i>wednesday</i>	Wednesday.	<i>thursday</i>	Thursday.	<i>friday</i>	Friday.	<i>saturday</i>	Saturday.			
	Option	Description																
	<i>monday</i>	Monday.																
	<i>tuesday</i>	Tuesday.																
	<i>wednesday</i>	Wednesday.																
	<i>thursday</i>	Thursday.																
	<i>friday</i>	Friday.																
<i>saturday</i>	Saturday.																	
time	Schedule time to generate report (format = hh:mm).	user	Not Specified															
cutoff-option	Cutoff-option is either run-time or custom.	option	-	run-time														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>run-time</i></td><td>Run time.</td></tr><tr><td><i>custom</i></td><td>Custom.</td></tr></table>	Option	Description	<i>run-time</i>	Run time.	<i>custom</i>	Custom.											
	Option	Description																
	<i>run-time</i>	Run time.																
<i>custom</i>	Custom.																	
cutoff-time	Custom cutoff time to generate report (format = hh:mm).	user	Not Specified															
email-send	Enable/disable sending emails after reports are generated.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending emails after generating reports.</td></tr><tr><td><i>disable</i></td><td>Disable sending emails after generating reports.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending emails after generating reports.	<i>disable</i>	Disable sending emails after generating reports.											
	Option	Description																
	<i>enable</i>	Enable sending emails after generating reports.																
<i>disable</i>	Disable sending emails after generating reports.																	
email-recipients	Email recipients for generated reports.	string	Maximum length: 511															
max-pdf-report	Maximum number of PDF reports to keep at one time (oldest report is overwritten).	integer	Minimum value: 1 Maximum value: 365	31														

config page

Parameter	Description	Type	Size	Default
paper	Report page paper.	option	-	a4

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>a4</i>	A4 paper.		
	<i>letter</i>	Letter paper.		
column-break-before	Report page auto column break before heading.	option	-	
	Option	Description		
	<i>heading1</i>	Column break before heading 1.		
	<i>heading2</i>	Column break before heading 2.		
	<i>heading3</i>	Column break before heading 3.		
page-break-before	Report page auto page break before heading.	option	-	
	Option	Description		
	<i>heading1</i>	Page break before heading 1.		
	<i>heading2</i>	Page break before heading 2.		
	<i>heading3</i>	Page break before heading 3.		
options	Report page options.	option	-	
	Option	Description		
	<i>header-on-first-page</i>	Show header on first page.		
	<i>footer-on-first-page</i>	Show footer on first page.		

config header

Parameter	Description	Type	Size	Default
style	Report header style.	string	Maximum length: 71	

config header-item

Parameter	Description	Type	Size	Default						
id	Report item ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
description	Description.	string	Maximum length: 63							
type	Report item type.	option	-	text						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>text</i></td><td>Text.</td></tr><tr><td><i>image</i></td><td>Image.</td></tr></table>				Option	Description	<i>text</i>	Text.	<i>image</i>	Image.
	Option	Description								
	<i>text</i>	Text.								
<i>image</i>	Image.									
style	Report item style.	string	Maximum length: 71							
content	Report item text content.	string	Maximum length: 511							
img-src	Report item image file name.	string	Maximum length: 127							

config footer

Parameter	Description	Type	Size	Default
style	Report footer style.	string	Maximum length: 71	

config footer-item

Parameter	Description	Type	Size	Default
id	Report item ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
description	Description.	string	Maximum length: 63	
type	Report item type.	option	-	text

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>text</i>	Text.		
	<i>image</i>	Image.		
style	Report item style.	string	Maximum length: 71	
content	Report item text content.	string	Maximum length: 511	
img-src	Report item image file name.	string	Maximum length: 127	

config body-item

Parameter	Description	Type	Size	Default
id	Report item ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
description	Description.	string	Maximum length: 63	
type	Report item type.	option	-	text
	Option	Description		
	<i>text</i>	Text.		
	<i>image</i>	Image.		
	<i>chart</i>	Chart.		
	<i>misc</i>	Miscellaneous.		
style	Report item style.	string	Maximum length: 71	
top-n	Value of top.	integer	Minimum value: 0 Maximum value: 4294967295	0
text-component	Report item text component.	option	-	text

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>text</i>	Normal text.		
	<i>heading1</i>	Heading 1.		
	<i>heading2</i>	Heading 2.		
	<i>heading3</i>	Heading 3.		
content	Report item text content.	string	Maximum length: 511	
img-src	Report item image file name.	string	Maximum length: 127	
chart	Report item chart name.	string	Maximum length: 71	
chart-options	Report chart options.	option	-	include-no-data hide-title show-caption
	Option	Description		
	<i>include-no-data</i>	Include chart with no data.		
	<i>hide-title</i>	Hide chart title.		
	<i>show-caption</i>	Show chart caption.		
misc-component	Report item miscellaneous component.	option	-	hline
	Option	Description		
	<i>hline</i>	Horizontal line.		
	<i>page-break</i>	Page break.		
	<i>column-break</i>	Column break.		
	<i>section-start</i>	Section start.		
title	Report section title.	string	Maximum length: 511	

config parameters

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Field name that match field of parameters defined in dataset.	string	Maximum length: 127	
value	Value to replace corresponding field of parameters defined in dataset.	string	Maximum length: 1023	

config report setting

Report setting configuration.

```
config report setting
    Description: Report setting configuration.
    set pdf-report [enable|disable]
    set fortiview [enable|disable]
    set report-source {option1}, {option2}, ...
    set web-browsing-threshold {integer}
    set top-n {integer}
end
```

config report setting

Parameter	Description	Type	Size	Default						
pdf-report	Enable/disable PDF report.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable PDF report.</td></tr><tr><td><i>disable</i></td><td>Disable PDF report.</td></tr></table>	Option	Description	<i>enable</i>	Enable PDF report.	<i>disable</i>	Disable PDF report.			
Option	Description									
<i>enable</i>	Enable PDF report.									
<i>disable</i>	Disable PDF report.									
fortiview	Enable/disable historical FortiView.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable historical FortiView.</td></tr><tr><td><i>disable</i></td><td>Disable historical FortiView.</td></tr></table>	Option	Description	<i>enable</i>	Enable historical FortiView.	<i>disable</i>	Disable historical FortiView.			
Option	Description									
<i>enable</i>	Enable historical FortiView.									
<i>disable</i>	Disable historical FortiView.									

Parameter	Description	Type	Size	Default								
report-source	Report log source.	option	-	forward-traffic								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>forward-traffic</i></td><td>Report includes forward traffic logs.</td></tr><tr><td><i>sniffer-traffic</i></td><td>Report includes sniffer traffic logs.</td></tr><tr><td><i>local-deny-traffic</i></td><td>Report includes local deny traffic logs.</td></tr></table>				Option	Description	<i>forward-traffic</i>	Report includes forward traffic logs.	<i>sniffer-traffic</i>	Report includes sniffer traffic logs.	<i>local-deny-traffic</i>	Report includes local deny traffic logs.
	Option	Description										
	<i>forward-traffic</i>	Report includes forward traffic logs.										
	<i>sniffer-traffic</i>	Report includes sniffer traffic logs.										
	<i>local-deny-traffic</i>	Report includes local deny traffic logs.										
web-browsing-threshold	Web browsing time calculation threshold.	integer	Minimum value: 3 Maximum value: 15	3								
top-n	Number of items to populate.	integer	Minimum value: 1000 Maximum value: 20000	1000								

config report sql status

Show report database status.

```
config report sql status
    Description: Show report database status.
end
```

router

This section includes syntax for the following commands:

- [config router policy on page 626](#)
- [config router static on page 628](#)
- [config router static6 on page 630](#)

config router policy

Configure IPv4 routing policies.

```
config router policy
  Description: Configure IPv4 routing policies.
  edit <seq-num>
    set input-device <name1>, <name2>, ...
    set src <subnet1>, <subnet2>, ...
    set dst <subnet1>, <subnet2>, ...
    set action [deny|permit]
    set protocol {integer}
    set start-port {integer}
    set end-port {integer}
    set start-source-port {integer}
    set end-source-port {integer}
    set gateway {ipv4-address}
    set output-device {string}
    set status [enable|disable]
    set comments {var-string}
    set internet-service-id <id1>, <id2>, ...
    set internet-service-custom <name1>, <name2>, ...
  next
end
```

config router policy

Parameter	Description	Type	Size	Default
seq-num	Sequence number.	integer	Minimum value: 1 Maximum value: 2048	0
input-device <name>	Incoming interface name. Interface name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default						
src <subnet>	Source IP and mask (x.x.x.x/x). IP and mask.	string	Maximum length: 79							
dst <subnet>	Destination IP and mask (x.x.x.x/x). IP and mask.	string	Maximum length: 79							
action	Action of the policy route.	option	-	permit						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>deny</td><td>Do not search policy route table.</td></tr><tr><td>permit</td><td>Use this policy route for forwarding.</td></tr></table>				Option	Description	deny	Do not search policy route table.	permit	Use this policy route for forwarding.
Option	Description									
deny	Do not search policy route table.									
permit	Use this policy route for forwarding.									
protocol	Protocol number.	integer	Minimum value: 0 Maximum value: 255	0						
start-port	Start destination port number.	integer	Minimum value: 0 Maximum value: 65535	1						
end-port	End destination port number.	integer	Minimum value: 0 Maximum value: 65535	65534						
start-source-port	Start source port number.	integer	Minimum value: 0 Maximum value: 65535	1						
end-source-port	End source port number.	integer	Minimum value: 0 Maximum value: 65535	65534						
gateway	IP address of the gateway.	ipv4- address	Not Specified	0.0.0.0						
output-device	Outgoing interface name.	string	Maximum length: 35							
status	Enable/disable this policy route.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable this policy route.</td></tr><tr><td>disable</td><td>Disable this policy route.</td></tr></table>				Option	Description	enable	Enable this policy route.	disable	Disable this policy route.
Option	Description									
enable	Enable this policy route.									
disable	Disable this policy route.									

Parameter	Description	Type	Size	Default
comments	Optional comments.	var-string	Maximum length: 255	
internet-service-id <id>	Destination Internet Service ID. Destination Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295	
internet-service-custom <name>	Custom Destination Internet Service name. Custom Destination Internet Service name.	string	Maximum length: 79	

config router static

Configure IPv4 static routing tables.

```

config router static
    Description: Configure IPv4 static routing tables.
    edit <seq-num>
        set status [enable|disable]
        set dst {ipv4-classnet}
        set src {ipv4-classnet}
        set gateway {ipv4-address}
        set weight {integer}
        set priority {integer}
        set device {string}
        set comment {var-string}
        set blackhole [enable|disable]
        set sdwan-zone <name1>, <name2>, ...
        set dstaddr {string}
        set link-monitor-exempt [enable|disable]
        set tag {integer}
    next
end

```

config router static

Parameter	Description	Type	Size	Default
seq-num	Sequence number.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
status	Enable/disable this static route.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable static route.		
	<i>disable</i>	Disable static route.		
dst	Destination IP and mask for this route.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
src	Source prefix for this route.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
gateway	Gateway IP for this route.	ipv4-address	Not Specified	0.0.0.0
weight	Administrative weight.	integer	Minimum value: 0 Maximum value: 255	0
priority	Administrative priority.	integer	Minimum value: 1 Maximum value: 65535	1
device	Gateway out interface or tunnel.	string	Maximum length: 35	
comment	Optional comments.	var-string	Maximum length: 255	
blackhole	Enable/disable black hole.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable black hole.		
	<i>disable</i>	Disable black hole.		
sdwan-zone <name>	Choose SD-WAN Zone. SD-WAN zone name.	string	Maximum length: 79	
dstaddr	Name of firewall address or address group.	string	Maximum length: 79	
link-monitor-exempt	Enable/disable withdrawal of this static route when link monitor or health check is down.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Keep this static route when link monitor or health check is down.		
	<i>disable</i>	Withdraw this static route when link monitor or health check is down. (default)		
tag	Route tag.	integer	Minimum value: 0 Maximum value: 4294967295	0

config router static6

Configure IPv6 static routing tables.

```

config router static6
    Description: Configure IPv6 static routing tables.
    edit <seq-num>
        set status [enable|disable]
        set dst {ipv6-network}
        set gateway {ipv6-address}
        set device {string}
        set devindex {integer}
        set weight {integer}
        set priority {integer}
        set comment {var-string}
        set blackhole [enable|disable]
        set sdwan-zone <name1>, <name2>, ...
        set dstaddr {string}
        set link-monitor-exempt [enable|disable]
    next
end

```

config router static6

Parameter	Description	Type	Size	Default
seq-num	Sequence number.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Enable/disable this static route.	option	-	enable

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable static route.</td></tr><tr><td><i>disable</i></td><td>Disable static route.</td></tr></table>	Option	Description	<i>enable</i>	Enable static route.	<i>disable</i>	Disable static route.			
	Option	Description								
	<i>enable</i>	Enable static route.								
<i>disable</i>	Disable static route.									
dst	Destination IPv6 prefix.	ipv6-network	Not Specified	::/0						
gateway	IPv6 address of the gateway.	ipv6-address	Not Specified	::						
device	Gateway out interface or tunnel.	string	Maximum length: 35							
devindex	Device index.	integer	Minimum value: 0 Maximum value: 4294967295	0						
weight	Administrative weight.	integer	Minimum value: 0 Maximum value: 255	0						
priority	Administrative priority.	integer	Minimum value: 1 Maximum value: 65535	1024						
comment	Optional comments.	var-string	Maximum length: 255							
blackhole	Enable/disable black hole.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable black hole.</td></tr><tr><td><i>disable</i></td><td>Disable black hole.</td></tr></table>	Option	Description	<i>enable</i>	Enable black hole.	<i>disable</i>	Disable black hole.			
	Option	Description								
	<i>enable</i>	Enable black hole.								
<i>disable</i>	Disable black hole.									
sdwan-zone <name>	Choose SD-WAN Zone. SD-WAN zone name.	string	Maximum length: 79							
dstaddr	Name of firewall address or address group.	string	Maximum length: 79							
link-monitor-exempt	Enable/disable withdrawal of this static route when link monitor or health check is down.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Keep this static route when link monitor or health check is down.		
	<i>disable</i>	Withdraw this static route when link monitor or health check is down. (default)		

rule

This section includes syntax for the following commands:

- [config rule fmwp on page 633](#)

config rule fmwp

Show FMWP rules.

```
config rule fmwp
  Description: Show FMWP rules.
  edit <name>
    set log [disable|enable]
    set log-packet [disable|enable]
    set action [pass|block]
    set group {string}
    set severity {user}
    set location {user}
    set os {user}
    set application {user}
    set service {user}
    set rule-id {integer}
    set rev {integer}
    set date {integer}
    config metadata
      Description: Meta data.
      edit <id>
        set metaid {integer}
        set valueid {integer}
      next
    end
  next
end
```

config rule fmwp

Parameter	Description	Type	Size	Default
name	Rule name.	string	Maximum length: 63	
log	Enable/disable logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable logging.		
	<i>enable</i>	Enable logging.		
log-packet	Enable/disable packet logging.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable packet logging.		
	<i>enable</i>	Enable packet logging.		
action	Action.	option	-	pass
	Option	Description		
	<i>pass</i>	Pass or allow matching traffic.		
	<i>block</i>	Block or drop matching traffic.		
group	Group.	string	Maximum length: 63	
severity	Severity.	user	Not Specified	
location	Vulnerable location.	user	Not Specified	
os	Vulnerable operation systems.	user	Not Specified	
application	Vulnerable applications.	user	Not Specified	
service	Vulnerable service.	user	Not Specified	
rule-id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
rev	Revision.	integer	Minimum value: 0 Maximum value: 4294967295	0
date	Date.	integer	Minimum value: 0 Maximum value: 4294967295	0

config metadata

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
metaid	Meta ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
valueid	Value ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

ssh-filter

This section includes syntax for the following commands:

- [config ssh-filter profile on page 636](#)

config ssh-filter profile

Configure SSH filter profile.

```
config ssh-filter profile
  Description: Configure SSH filter profile.
  edit <name>
    set block {option1}, {option2}, ...
    set log {option1}, {option2}, ...
    set default-command-log [enable|disable]
    config shell-commands
      Description: SSH command filter.
      edit <id>
        set type [simple|regex]
        set pattern {string}
        set action [block|allow]
        set log [enable|disable]
        set alert [enable|disable]
        set severity [low|medium|...]
      next
    end
  next
end
```

config ssh-filter profile

Parameter	Description	Type	Size	Default								
name	SSH filter profile name.	string	Maximum length: 35									
block	SSH blocking options.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>x11</td><td>X server forwarding.</td></tr><tr><td>shell</td><td>SSH shell.</td></tr><tr><td>exec</td><td>SSH execution.</td></tr></table>				Option	Description	x11	X server forwarding.	shell	SSH shell.	exec	SSH execution.
Option	Description											
x11	X server forwarding.											
shell	SSH shell.											
exec	SSH execution.											

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>port-forward</i></td><td>Port forwarding.</td></tr><tr><td><i>tun-forward</i></td><td>Tunnel forwarding.</td></tr><tr><td><i>sftp</i></td><td>SFTP.</td></tr><tr><td><i>scp</i></td><td>SCP.</td></tr><tr><td><i>unknown</i></td><td>Unknown channel.</td></tr></table>	Option	Description	<i>port-forward</i>	Port forwarding.	<i>tun-forward</i>	Tunnel forwarding.	<i>sftp</i>	SFTP.	<i>scp</i>	SCP.	<i>unknown</i>	Unknown channel.									
	Option	Description																				
	<i>port-forward</i>	Port forwarding.																				
	<i>tun-forward</i>	Tunnel forwarding.																				
	<i>sftp</i>	SFTP.																				
	<i>scp</i>	SCP.																				
	<i>unknown</i>	Unknown channel.																				
log	SSH logging options.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>x11</i></td><td>X server forwarding.</td></tr><tr><td><i>shell</i></td><td>SSH shell.</td></tr><tr><td><i>exec</i></td><td>SSH execution.</td></tr><tr><td><i>port-forward</i></td><td>Port forwarding.</td></tr><tr><td><i>tun-forward</i></td><td>Tunnel forwarding.</td></tr><tr><td><i>sftp</i></td><td>SFTP.</td></tr><tr><td><i>scp</i></td><td>SCP.</td></tr><tr><td><i>unknown</i></td><td>Unknown channel.</td></tr></table>	Option	Description	<i>x11</i>	X server forwarding.	<i>shell</i>	SSH shell.	<i>exec</i>	SSH execution.	<i>port-forward</i>	Port forwarding.	<i>tun-forward</i>	Tunnel forwarding.	<i>sftp</i>	SFTP.	<i>scp</i>	SCP.	<i>unknown</i>	Unknown channel.			
	Option	Description																				
	<i>x11</i>	X server forwarding.																				
	<i>shell</i>	SSH shell.																				
	<i>exec</i>	SSH execution.																				
	<i>port-forward</i>	Port forwarding.																				
	<i>tun-forward</i>	Tunnel forwarding.																				
	<i>sftp</i>	SFTP.																				
	<i>scp</i>	SCP.																				
<i>unknown</i>	Unknown channel.																					
default-command-log	Enable/disable logging unmatched shell commands.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable log unmatched shell commands.</td></tr><tr><td><i>disable</i></td><td>Disable log unmatched shell commands.</td></tr></table>	Option	Description	<i>enable</i>	Enable log unmatched shell commands.	<i>disable</i>	Disable log unmatched shell commands.															
	Option	Description																				
	<i>enable</i>	Enable log unmatched shell commands.																				
<i>disable</i>	Disable log unmatched shell commands.																					

config shell-commands

Parameter	Description	Type	Size	Default
id	Id.	integer	Minimum value: 0 Maximum value: 4294967295	0
type	Matching type.	option	-	simple

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>simple</i>	Match single command.		
	<i>regex</i>	Match command line using regular expression.		
pattern	SSH shell command pattern.	string	Maximum length: 128	
action	Action to take for SSH shell command matches.	option	-	block
	Option	Description		
	<i>block</i>	Block the SSH shell command.		
	<i>allow</i>	Allow the SSH shell command.		
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging.		
	<i>disable</i>	Disable logging.		
alert	Enable/disable alert.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable alert.		
	<i>disable</i>	Disable alert.		
severity	Log severity.	option	-	medium
	Option	Description		
	<i>low</i>	Severity low.		
	<i>medium</i>	Severity medium.		
	<i>high</i>	Severity high.		
	<i>critical</i>	Severity critical.		

system

This section includes syntax for the following commands:

- [config system accprofile on page 642](#)
- [config system acme on page 652](#)
- [config system admin on page 653](#)
- [config system affinity-interrupt on page 660](#)
- [config system affinity-packet-redistribution on page 661](#)
- [config system alarm on page 662](#)
- [config system alias on page 665](#)
- [config system api-user on page 665](#)
- [config system arp-table on page 667](#)
- [config system arp on page 668](#)
- [config system auto-install on page 668](#)
- [config system auto-script on page 669](#)
- [config system auto-update status on page 670](#)
- [config system auto-update versions on page 671](#)
- [config system automation-action on page 671](#)
- [config system automation-destination on page 676](#)
- [config system automation-stitch on page 677](#)
- [config system automation-trigger on page 678](#)
- [config system autoupdate schedule on page 683](#)
- [config system autoupdate tunneling on page 684](#)
- [config system central-management on page 685](#)
- [config system central-mgmt on page 689](#)
- [config system checksum status on page 690](#)
- [config system cmdb on page 690](#)
- [config system console on page 690](#)
- [config system csf on page 691](#)
- [config system custom-language on page 697](#)
- [config system ddns on page 697](#)
- [config system device-upgrade on page 700](#)
- [config system dhcp6 server on page 703](#)
- [config system dhcp server on page 706](#)
- [config system dns-database on page 721](#)
- [config system dns-server on page 724](#)
- [config system dns on page 725](#)
- [config system dscp-based-priority on page 728](#)
- [config system email-server on page 729](#)
- [config system external-resource on page 731](#)

- [config system fabric-vpn on page 734](#)
- [config system federated-upgrade on page 738](#)
- [config system fips-cc on page 741](#)
- [config system fortianalyzer-connectivity on page 742](#)
- [config system fortiguard-log-service on page 742](#)
- [config system fortiguard-service on page 742](#)
- [config system fortiguard on page 743](#)
- [config system fortindr on page 753](#)
- [config system fortisandbox on page 754](#)
- [config system fsso-polling on page 755](#)
- [config system ftm-push on page 756](#)
- [config system geoip-country on page 757](#)
- [config system geoip-override on page 758](#)
- [config system global on page 759](#)
- [config system gre-tunnel on page 804](#)
- [config system ha-lic on page 806](#)
- [config system ha-monitor on page 807](#)
- [config system ha-nonsync-csum on page 808](#)
- [config system ha on page 808](#)
- [config system info admin ssh on page 818](#)
- [config system info admin status on page 818](#)
- [config system interface on page 818](#)
- [config system ip-conflict status on page 851](#)
- [config system ipam on page 851](#)
- [config system ips-urlfilter-dns on page 853](#)
- [config system ips-urlfilter-dns6 on page 854](#)
- [config system ips on page 855](#)
- [config system ipv6-neighbor-cache on page 855](#)
- [config system link-monitor on page 856](#)
- [config system management-tunnel on page 861](#)
- [config system mgmt-csum on page 863](#)
- [config system nethsm on page 863](#)
- [config system network-visibility on page 866](#)
- [config system ntp on page 868](#)
- [config system object-tagging on page 871](#)
- [config system password-policy-guest-admin on page 872](#)
- [config system password-policy on page 874](#)
- [config system performance status on page 876](#)
- [config system performance top on page 877](#)
- [config system probe-response on page 877](#)
- [config system proxy-arp on page 878](#)
- [config system ptp on page 879](#)
- [config system replacemsg-group on page 881](#)

- [config system replacemsg-image on page 893](#)
- [config system replacemsg admin on page 894](#)
- [config system replacemsg alertmail on page 895](#)
- [config system replacemsg auth on page 896](#)
- [config system replacemsg automation on page 897](#)
- [config system replacemsg custom-message on page 898](#)
- [config system replacemsg fortiguard-wf on page 899](#)
- [config system replacemsg ftp on page 899](#)
- [config system replacemsg http on page 900](#)
- [config system replacemsg icap on page 901](#)
- [config system replacemsg mail on page 902](#)
- [config system replacemsg nac-quar on page 903](#)
- [config system replacemsg spam on page 904](#)
- [config system replacemsg sslvpn on page 905](#)
- [config system replacemsg traffic-quota on page 906](#)
- [config system replacemsg utm on page 907](#)
- [config system replacemsg webproxy on page 907](#)
- [config system resource-limits on page 908](#)
- [config system saml on page 910](#)
- [config system sdn-connector on page 914](#)
- [config system session-ttl on page 923](#)
- [config system session on page 924](#)
- [config system session6 on page 924](#)
- [config system settings on page 924](#)
- [config system sms-server on page 938](#)
- [config system snmp community on page 939](#)
- [config system snmp mib-view on page 945](#)
- [config system snmp sysinfo on page 946](#)
- [config system snmp user on page 947](#)
- [config system source-ip status on page 953](#)
- [config system span-port on page 953](#)
- [config system speed-test-schedule on page 954](#)
- [config system speed-test-server on page 956](#)
- [config system speed-test-setting on page 957](#)
- [config system sso-admin on page 958](#)
- [config system sso-forticloud-admin on page 958](#)
- [config system sso-fortigate-cloud-admin on page 959](#)
- [config system startup-error-log on page 959](#)
- [config system status on page 960](#)
- [config system storage on page 960](#)
- [config system vdom-dns on page 961](#)
- [config system vdom-exception on page 963](#)
- [config system vdom-link on page 966](#)

- [config system vdom-property on page 966](#)
- [config system vdom-radius-server on page 968](#)
- [config system vdom on page 968](#)
- [config system vne-tunnel on page 969](#)
- [config system vxlan on page 970](#)
- [config system wccp on page 972](#)
- [config system zone on page 975](#)

config system accprofile

Configure access profiles for system administrators.

```
config system accprofile
  Description: Configure access profiles for system administrators.
  edit <name>
    set scope [vdom|global]
    set comments {var-string}
    set secfabgrp [none|read|...]
    set ftviewgrp [none|read|...]
    set authgrp [none|read|...]
    set sysgrp [none|read|...]
    set netgrp [none|read|...]
    set loggrp [none|read|...]
    set fwgrp [none|read|...]
    set vpngrp [none|read|...]
    set utmgrp [none|read|...]
    set wanoptgrp [none|read|...]
    config netgrp-permission
      Description: Custom network permission.
      set cfg [none|read|...]
      set packet-capture [none|read|...]
      set route-cfg [none|read|...]
    end
    config sysgrp-permission
      Description: Custom system permission.
      set admin [none|read|...]
      set upd [none|read|...]
      set cfg [none|read|...]
      set mnt [none|read|...]
    end
    config fwgrp-permission
      Description: Custom firewall permission.
      set policy [none|read|...]
      set address [none|read|...]
      set service [none|read|...]
      set schedule [none|read|...]
      set others [none|read|...]
    end
    config loggrp-permission
      Description: Custom Log & Report permission.
      set config [none|read|...]
```

```

        set data-access [none|read|...]
        set report-access [none|read|...]
        set threat-weight [none|read|...]
    end
    config utmgrp-permission
        Description: Custom Security Profile permissions.
        set antivirus [none|read|...]
        set ips [none|read|...]
        set webfilter [none|read|...]
        set emailfilter [none|read|...]
        set data-leak-prevention [none|read|...]
        set file-filter [none|read|...]
        set application-control [none|read|...]
        set icap [none|read|...]
        set voip [none|read|...]
        set waf [none|read|...]
        set dnsfilter [none|read|...]
        set endpoint-control [none|read|...]
        set videofilter [none|read|...]
    end
    set admintimeout-override [enable|disable]
    set admintimeout {integer}
    set system-diagnostics [enable|disable]
    set system-execute-ssh [enable|disable]
    set system-execute-telnet [enable|disable]
next
end

```

config system accprofile

Parameter	Description	Type	Size	Default
name	Profile name.	string	Maximum length: 35	
scope	Scope of admin access: global or specific VDOM(s).	option	-	vdom
	Option	Description		
	<i>vdom</i>	VDOM access.		
	<i>global</i>	Global access.		
comments	Comment.	var-string	Maximum length: 255	
secfabgrp	Security Fabric.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

Parameter	Description	Type	Size	Default										
ftviewgrp	FortiView.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.					
Option	Description													
<i>none</i>	No access.													
<i>read</i>	Read access.													
<i>read-write</i>	Read/write access.													
authgrp	Administrator access to Users and Devices.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.					
Option	Description													
<i>none</i>	No access.													
<i>read</i>	Read access.													
<i>read-write</i>	Read/write access.													
sysgrp	System Configuration.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr><tr><td><i>custom</i></td><td>Customized access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.	<i>custom</i>	Customized access.			
Option	Description													
<i>none</i>	No access.													
<i>read</i>	Read access.													
<i>read-write</i>	Read/write access.													
<i>custom</i>	Customized access.													
netgrp	Network Configuration.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr><tr><td><i>custom</i></td><td>Customized access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.	<i>custom</i>	Customized access.			
Option	Description													
<i>none</i>	No access.													
<i>read</i>	Read access.													
<i>read-write</i>	Read/write access.													
<i>custom</i>	Customized access.													
loggrp	Administrator access to Logging and Reporting including viewing log messages.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr><tr><td><i>custom</i></td><td>Customized access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.	<i>custom</i>	Customized access.			
Option	Description													
<i>none</i>	No access.													
<i>read</i>	Read access.													
<i>read-write</i>	Read/write access.													
<i>custom</i>	Customized access.													

Parameter	Description	Type	Size	Default										
fwgrp	Administrator access to the Firewall configuration.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr><tr><td><i>custom</i></td><td>Customized access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.	<i>custom</i>	Customized access.			
Option	Description													
<i>none</i>	No access.													
<i>read</i>	Read access.													
<i>read-write</i>	Read/write access.													
<i>custom</i>	Customized access.													
vpngrp	Administrator access to IPsec, SSL, PPTP, and L2TP VPN.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.					
Option	Description													
<i>none</i>	No access.													
<i>read</i>	Read access.													
<i>read-write</i>	Read/write access.													
utmgrp	Administrator access to Security Profiles.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr><tr><td><i>custom</i></td><td>Customized access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.	<i>custom</i>	Customized access.			
Option	Description													
<i>none</i>	No access.													
<i>read</i>	Read access.													
<i>read-write</i>	Read/write access.													
<i>custom</i>	Customized access.													
wanoptgrp	Administrator access to WAN Opt & Cache.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.					
Option	Description													
<i>none</i>	No access.													
<i>read</i>	Read access.													
<i>read-write</i>	Read/write access.													
admintimeout-override	Enable/disable overriding the global administrator idle timeout.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable overriding the global administrator idle timeout.</td></tr><tr><td><i>disable</i></td><td>Disable overriding the global administrator idle timeout.</td></tr></table>	Option	Description	<i>enable</i>	Enable overriding the global administrator idle timeout.	<i>disable</i>	Disable overriding the global administrator idle timeout.							
Option	Description													
<i>enable</i>	Enable overriding the global administrator idle timeout.													
<i>disable</i>	Disable overriding the global administrator idle timeout.													

Parameter	Description	Type	Size	Default						
admintimeout	Administrator timeout for this access profile.	integer	Minimum value: 1 Maximum value: 480	10						
system-diagnostics	Enable/disable permission to run system diagnostic commands.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable permission to run system diagnostic commands.</td></tr><tr><td><i>disable</i></td><td>Disable permission to run system diagnostic commands.</td></tr></table>	Option	Description	<i>enable</i>	Enable permission to run system diagnostic commands.	<i>disable</i>	Disable permission to run system diagnostic commands.			
Option	Description									
<i>enable</i>	Enable permission to run system diagnostic commands.									
<i>disable</i>	Disable permission to run system diagnostic commands.									
system-execute-ssh	Enable/disable permission to execute SSH commands.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable permission to execute SSH commands.</td></tr><tr><td><i>disable</i></td><td>Disable permission to execute SSH commands.</td></tr></table>	Option	Description	<i>enable</i>	Enable permission to execute SSH commands.	<i>disable</i>	Disable permission to execute SSH commands.			
Option	Description									
<i>enable</i>	Enable permission to execute SSH commands.									
<i>disable</i>	Disable permission to execute SSH commands.									
system-execute-telnet	Enable/disable permission to execute TELNET commands.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable permission to execute TELNET commands.</td></tr><tr><td><i>disable</i></td><td>Disable permission to execute TELNET commands.</td></tr></table>	Option	Description	<i>enable</i>	Enable permission to execute TELNET commands.	<i>disable</i>	Disable permission to execute TELNET commands.			
Option	Description									
<i>enable</i>	Enable permission to execute TELNET commands.									
<i>disable</i>	Disable permission to execute TELNET commands.									

config netgrp-permission

Parameter	Description	Type	Size	Default								
cfg	Network Configuration.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
	Option	Description										
	<i>none</i>	No access.										
	<i>read</i>	Read access.										
<i>read-write</i>	Read/write access.											
packet-capture	Packet Capture Configuration.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr></table>	Option	Description	<i>none</i>	No access.							
	Option	Description										
<i>none</i>	No access.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
route-cfg	Router Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

config sysgrp-permission

Parameter	Description	Type	Size	Default
admin	Administrator Users.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
upd	FortiGuard Updates.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
cfg	System Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
mnt	Maintenance.	option	-	none

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

config fwgrp-permission

Parameter	Description	Type	Size	Default
policy	Policy Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
address	Address Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
service	Service Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
schedule	Schedule Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
others	Other Firewall Configuration.	option	-	none

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

config loggrp-permission

Parameter	Description	Type	Size	Default
config	Log & Report configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
data-access	Log & Report Data Access.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
report-access	Log & Report Report Access.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
threat-weight	Log & Report Threat Weight.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

config utmgrp-permission

Parameter	Description	Type	Size	Default
antivirus	Antivirus profiles and settings.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
ips	IPS profiles and settings.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
webfilter	Web Filter profiles and settings.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
emailfilter	Email Filter and settings.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
data-leak-prevention	DLP profiles and settings.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
file-filter	File-filter profiles and settings.	option	-	none

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
application-control	Application Control profiles and settings.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
icap	ICAP profiles and settings.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
voip	VoIP profiles and settings.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
waf	Web Application Firewall profiles and settings.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
dnsfilter	DNS Filter profiles and settings.	option	-	none
	Option	Description		
	<i>none</i>	No access.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
endpoint-control	FortiClient Profiles.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
videofilter	Video filter profiles and settings.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

config system acme

Configure ACME client.

```

config system acme
    Description: Configure ACME client.
    set interface <interface-name1>, <interface-name2>, ...
    set source-ip {ipv4-address}
    set source-ip6 {ipv6-address}
    config accounts
        Description: ACME accounts list.
        edit <id>
            set status {string}
            set url {string}
            set ca_url {string}
            set email {string}
            set privatekey {string}
        next
    end
end

```

config system acme

Parameter	Description	Type	Size	Default
interface <interface-name>	Interface(s) on which the ACME client will listen for challenges. Interface name.	string	Maximum length: 79	
source-ip	Source IPv4 address used to connect to the ACME server.	ipv4-address	Not Specified	0.0.0.0
source-ip6	Source IPv6 address used to connect to the ACME server.	ipv6-address	Not Specified	::

config accounts

Parameter	Description	Type	Size	Default
id	Account id.	string	Maximum length: 255	
status	Account status.	string	Maximum length: 127	
url	Account url.	string	Maximum length: 511	
ca_url	Account ca_url.	string	Maximum length: 255	
email	Account email.	string	Maximum length: 255	
privatekey	Account Private Key.	string	Maximum length: 8191	

config system admin

Configure admin users.

```
config system admin
  Description: Configure admin users.
  edit <name>
    set wildcard [enable|disable]
    set remote-auth [enable|disable]
    set remote-group {string}
    set password {password-2}
    set peer-auth [enable|disable]
    set peer-group {string}
    set trusthost1 {ipv4-classnet}
    set trusthost2 {ipv4-classnet}
```

```
set trusthost3 {ipv4-classnet}
set trusthost4 {ipv4-classnet}
set trusthost5 {ipv4-classnet}
set trusthost6 {ipv4-classnet}
set trusthost7 {ipv4-classnet}
set trusthost8 {ipv4-classnet}
set trusthost9 {ipv4-classnet}
set trusthost10 {ipv4-classnet}
set ip6-trusthost1 {ipv6-prefix}
set ip6-trusthost2 {ipv6-prefix}
set ip6-trusthost3 {ipv6-prefix}
set ip6-trusthost4 {ipv6-prefix}
set ip6-trusthost5 {ipv6-prefix}
set ip6-trusthost6 {ipv6-prefix}
set ip6-trusthost7 {ipv6-prefix}
set ip6-trusthost8 {ipv6-prefix}
set ip6-trusthost9 {ipv6-prefix}
set ip6-trusthost10 {ipv6-prefix}
set accprofile {string}
set allow-remove-admin-session [enable|disable]
set comments {var-string}
set vdom <name1>, <name2>, ...
set ssh-public-key1 {user}
set ssh-public-key2 {user}
set ssh-public-key3 {user}
set ssh-certificate {string}
set schedule {string}
set accprofile-override [enable|disable]
set vdom-override [enable|disable]
set password-expire {user}
set force-password-change [enable|disable]
set two-factor [disable|fortitoken|...]
set two-factor-authentication [fortitoken|email|...]
set two-factor-notification [email|sms]
set fortitoken {string}
set email-to {string}
set sms-server [fortiguard|custom]
set sms-custom-server {string}
set sms-phone {string}
set guest-auth [disable|enable]
set guest-usergroups <name1>, <name2>, ...
set guest-lang {string}
config trusthosts
    Description: Table of trusthosts.
    edit <id>
        set type [ipv4|ipv6]
        set ipv4 {ipv4-classnet}
        set ipv6 {ipv6-prefix}
    next
end
next
end
```

config system admin

Parameter	Description	Type	Size	Default
name	User name.	string	Maximum length: 64	
wildcard	Enable/disable wildcard RADIUS authentication.	option	-	disable
	Option Description			
	<i>enable</i>	Enable username wildcard.		
	<i>disable</i>	Disable username wildcard.		
remote-auth	Enable/disable authentication using a remote RADIUS, LDAP, or TACACS+ server.	option	-	disable
	Option Description			
	<i>enable</i>	Enable remote authentication.		
	<i>disable</i>	Disable remote authentication.		
remote-group	User group name used for remote auth.	string	Maximum length: 35	
password	Admin user password.	password-2	Not Specified	
peer-auth	Set to enable peer certificate authentication (for HTTPS admin access).	option	-	disable
	Option Description			
	<i>enable</i>	Enable peer.		
	<i>disable</i>	Disable peer.		
peer-group	Name of peer group defined under config user group which has PKI members. Used for peer certificate authentication (for HTTPS admin access).	string	Maximum length: 35	
trusthost1	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost2	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

Parameter	Description	Type	Size	Default
trusthost3	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost4	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost5	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost6	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost7	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost8	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost9	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost10	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
ip6-trusthost1	Any IPv6 address from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost2	Any IPv6 address from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost3	Any IPv6 address from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0

Parameter	Description	Type	Size	Default						
ip6-trusthost4	Any IPv6 address from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0						
ip6-trusthost5	Any IPv6 address from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0						
ip6-trusthost6	Any IPv6 address from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0						
ip6-trusthost7	Any IPv6 address from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0						
ip6-trusthost8	Any IPv6 address from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0						
ip6-trusthost9	Any IPv6 address from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0						
ip6-trusthost10	Any IPv6 address from which the administrator can connect to the FortiProxy unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0						
accprofile	Access profile for this administrator. Access profiles control administrator access to FortiProxy features.	string	Maximum length: 35							
allow-remove-admin-session	Enable/disable allow admin session to be removed by privileged admin users.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable allow-remove option.</td></tr><tr><td><i>disable</i></td><td>Disable allow-remove option.</td></tr></table>				Option	Description	<i>enable</i>	Enable allow-remove option.	<i>disable</i>	Disable allow-remove option.
Option	Description									
<i>enable</i>	Enable allow-remove option.									
<i>disable</i>	Disable allow-remove option.									
comments	Comment.	var-string	Maximum length: 255							
vdom <name>	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79							
ssh-public-key1	Public key of an SSH client. The client is authenticated without being asked for credentials. Create the public-private key pair in the SSH client application.	user	Not Specified							

Parameter	Description	Type	Size	Default
ssh-public-key2	Public key of an SSH client. The client is authenticated without being asked for credentials. Create the public-private key pair in the SSH client application.	user	Not Specified	
ssh-public-key3	Public key of an SSH client. The client is authenticated without being asked for credentials. Create the public-private key pair in the SSH client application.	user	Not Specified	
ssh-certificate	Select the certificate to be used by the FortiProxy for authentication with an SSH client.	string	Maximum length: 35	
schedule	Firewall schedule used to restrict when the administrator can log in. No schedule means no restrictions.	string	Maximum length: 35	
accprofile-override	Enable to use the name of an access profile provided by the remote authentication server to control the FortiProxy features that this administrator can access.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable access profile override.	
	<i>disable</i>		Disable access profile override.	
vdom-override	Enable to use the names of VDOMs provided by the remote authentication server to control the VDOMs that this administrator can access.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable VDOM override.	
	<i>disable</i>		Disable VDOM override.	
password-expire	Password expire time.	user	Not Specified	
force-password-change	Enable/disable force password change on next login.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable force password change on next login.	
	<i>disable</i>		Disable force password change on next login.	
two-factor	Enable/disable two-factor authentication.	option	-	disable

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable two-factor authentication.</td></tr><tr><td><i>fortitoken</i></td><td>Use FortiToken or FortiToken mobile two-factor authentication.</td></tr><tr><td><i>fortitoken-cloud</i></td><td>FortiToken Cloud Service.</td></tr><tr><td><i>email</i></td><td>Send a two-factor authentication code to the configured email-to email address.</td></tr><tr><td><i>sms</i></td><td>Send a two-factor authentication code to the configured sms-server and sms-phone.</td></tr></table>	Option	Description	<i>disable</i>	Disable two-factor authentication.	<i>fortitoken</i>	Use FortiToken or FortiToken mobile two-factor authentication.	<i>fortitoken-cloud</i>	FortiToken Cloud Service.	<i>email</i>	Send a two-factor authentication code to the configured email-to email address.	<i>sms</i>	Send a two-factor authentication code to the configured sms-server and sms-phone.			
	Option	Description														
	<i>disable</i>	Disable two-factor authentication.														
	<i>fortitoken</i>	Use FortiToken or FortiToken mobile two-factor authentication.														
	<i>fortitoken-cloud</i>	FortiToken Cloud Service.														
	<i>email</i>	Send a two-factor authentication code to the configured email-to email address.														
<i>sms</i>	Send a two-factor authentication code to the configured sms-server and sms-phone.															
two-factor-authentication	Authentication method by FortiToken Cloud.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortitoken</i></td><td>FortiToken authentication.</td></tr><tr><td><i>email</i></td><td>Email one time password.</td></tr><tr><td><i>sms</i></td><td>SMS one time password.</td></tr></table>	Option	Description	<i>fortitoken</i>	FortiToken authentication.	<i>email</i>	Email one time password.	<i>sms</i>	SMS one time password.							
	Option	Description														
	<i>fortitoken</i>	FortiToken authentication.														
	<i>email</i>	Email one time password.														
<i>sms</i>	SMS one time password.															
two-factor-notification	Notification method for user activation by FortiToken Cloud.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>email</i></td><td>Email notification for activation code.</td></tr><tr><td><i>sms</i></td><td>SMS notification for activation code.</td></tr></table>	Option	Description	<i>email</i>	Email notification for activation code.	<i>sms</i>	SMS notification for activation code.									
	Option	Description														
	<i>email</i>	Email notification for activation code.														
<i>sms</i>	SMS notification for activation code.															
fortitoken	This administrator's FortiToken serial number.	string	Maximum length: 16													
email-to	This administrator's email address.	string	Maximum length: 63													
sms-server	Send SMS messages using the FortiGuard SMS server or a custom server.	option	-	fortiguard												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortiguard</i></td><td>Send SMS by FortiGuard.</td></tr><tr><td><i>custom</i></td><td>Send SMS by custom server.</td></tr></table>	Option	Description	<i>fortiguard</i>	Send SMS by FortiGuard.	<i>custom</i>	Send SMS by custom server.									
	Option	Description														
	<i>fortiguard</i>	Send SMS by FortiGuard.														
<i>custom</i>	Send SMS by custom server.															
sms-custom-server	Custom SMS server to send SMS messages to.	string	Maximum length: 35													
sms-phone	Phone number on which the administrator receives SMS messages.	string	Maximum length: 15													

Parameter	Description	Type	Size	Default
guest-auth	Enable/disable guest authentication.	option	-	disable
	Option	Description		
	disable	Disable guest authentication.		
	enable	Enable guest authentication.		
guest-usergroups	Select guest user groups.	string	Maximum length: 79	
<name>	Select guest user groups.			
guest-lang	Guest management portal language.	string	Maximum length: 35	

config trusthosts

Parameter	Description	Type	Size	Default
type	Trusthost type.	option	-	ipv4
	Option	Description		
	ipv4	IPv4 trusthost.		
	ipv6	IPv6 trusthost.		
ipv4	IPv4 trusthost.	ipv4- classnet	Not Specified	0.0.0.0 0.0.0.0
ipv6	IPv6 trusthost.	ipv6-prefix	Not Specified	::/0

config system affinity-interrupt

Configure interrupt affinity.

```

config system affinity-interrupt
    Description: Configure interrupt affinity.
    edit <id>
        set interrupt {string}
        set affinity-cpumask {string}
        set default-affinity-cpumask {string}
    next
end

```

config system affinity-interrupt

Parameter	Description	Type	Size	Default
id	ID of the interrupt affinity setting.	integer	Minimum value: 0 Maximum value: 4294967295	0
interrupt	Interrupt name.	string	Maximum length: 127	
affinity-cpumask	Affinity setting (64-bit hexadecimal value in the format of 0xxxxxxxxxxxxxxxxx).	string	Maximum length: 127	
default-affinity-cpumask	Default affinity setting (64-bit hexadecimal value in the format of 0xxxxxxxxxxxxxxxxx).	string	Maximum length: 127	

config system affinity-packet-redistribution

Configure packet redistribution.

```
config system affinity-packet-redistribution
  Description: Configure packet redistribution.
  edit <id>
    set interface {string}
    set rxqid {integer}
    set affinity-cpumask {string}
  next
end
```

config system affinity-packet-redistribution

Parameter	Description	Type	Size	Default
id	ID of the packet redistribution setting.	integer	Minimum value: 0 Maximum value: 4294967295	0
interface	Physical interface name on which to perform packet redistribution.	string	Maximum length: 127	

Parameter	Description	Type	Size	Default
rxqid	ID of the receive queue (when the interface has multiple queues) on which to perform packet redistribution.	integer	Minimum value: 0 Maximum value: 255	0
affinity-cpumask	Affinity setting for VM throughput (64-bit hexadecimal value in the format of 0xxxxxxxxxxxxxxxxx).	string	Maximum length: 127	

config system alarm

Configure alarm.

```

config system alarm
  Description: Configure alarm.
  set status [enable|disable]
  set audible [enable|disable]
  config groups
    Description: Alarm groups.
    edit <id>
      set period {integer}
      set admin-auth-failure-threshold {integer}
      set admin-auth-lockout-threshold {integer}
      set user-auth-failure-threshold {integer}
      set user-auth-lockout-threshold {integer}
      set replay-attempt-threshold {integer}
      set self-test-failure-threshold {integer}
      set log-full-warning-threshold {integer}
      set encryption-failure-threshold {integer}
      set decryption-failure-threshold {integer}
      config fw-policy-violations
        Description: Firewall policy violations.
        edit <id>
          set threshold {integer}
          set src-ip {ipv4-address}
          set dst-ip {ipv4-address}
          set src-port {integer}
          set dst-port {integer}
        next
      end
      set fw-policy-id {integer}
      set fw-policy-id-threshold {integer}
    next
  end
end

```

config system alarm

Parameter	Description	Type	Size	Default
status	Enable/disable alarm.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable alarm.		
	<i>disable</i>	Disable alarm.		
audible	Enable/disable audible alarm.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable audible alarm.		
	<i>disable</i>	Disable audible alarm.		

config groups

Parameter	Description	Type	Size	Default
id	Group ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
period	Time period in seconds (0 = from start up).	integer	Minimum value: 0 Maximum value: 4294967295	0
admin-auth-failure-threshold	Admin authentication failure threshold.	integer	Minimum value: 0 Maximum value: 1024	0
admin-auth-lockout-threshold	Admin authentication lockout threshold.	integer	Minimum value: 0 Maximum value: 1024	0
user-auth-failure-threshold	User authentication failure threshold.	integer	Minimum value: 0 Maximum value: 1024	0

Parameter	Description	Type	Size	Default
user-auth-lockout-threshold	User authentication lockout threshold.	integer	Minimum value: 0 Maximum value: 1024	0
replay-attempt-threshold	Replay attempt threshold.	integer	Minimum value: 0 Maximum value: 1024	0
self-test-failure-threshold	Self-test failure threshold.	integer	Minimum value: 0 Maximum value: 1	0
log-full-warning-threshold	Log full warning threshold.	integer	Minimum value: 0 Maximum value: 1024	0
encryption-failure-threshold	Encryption failure threshold.	integer	Minimum value: 0 Maximum value: 1024	0
decryption-failure-threshold	Decryption failure threshold.	integer	Minimum value: 0 Maximum value: 1024	0
fw-policy-id	Firewall policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
fw-policy-id-threshold	Firewall policy ID threshold.	integer	Minimum value: 0 Maximum value: 1024	0

config fw-policy-violations

Parameter	Description	Type	Size	Default
id	Firewall policy violations ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
threshold	Firewall policy violation threshold.	integer	Minimum value: 0 Maximum value: 1024	0
src-ip	Source IP (0=all).	ipv4-address	Not Specified	0.0.0.0
dst-ip	Destination IP (0=all).	ipv4-address	Not Specified	0.0.0.0
src-port	Source port (0=all).	integer	Minimum value: 0 Maximum value: 65535	0
dst-port	Destination port (0=all).	integer	Minimum value: 0 Maximum value: 65535	0

config system alias

Configure alias command.

```
config system alias
  Description: Configure alias command.
  edit <name>
    set command {var-string}
  next
end
```

config system alias

Parameter	Description	Type	Size	Default
name	Alias command name.	string	Maximum length: 35	
command	Command list to execute.	var-string	Maximum length: 255	

config system api-user

Configure API users.

```

config system api-user
  Description: Configure API users.
  edit <name>
    set comments {var-string}
    set api-key {password-2}
    set accprofile {string}
    set vdom <name1>, <name2>, ...
    set schedule {string}
    set cors-allow-origin {string}
    set peer-auth [enable|disable]
    set peer-group {string}
  config trusthost
    Description: Trusthost.
    edit <id>
      set type [ipv4-trusthost|ipv6-trusthost]
      set ipv4-trusthost {ipv4-classnet}
      set ipv6-trusthost {ipv6-prefix}
    next
  end
next
end

```

config system api-user

Parameter	Description	Type	Size	Default
name	User name.	string	Maximum length: 35	
comments	Comment.	var-string	Maximum length: 255	
api-key	Admin user password.	password-2	Not Specified	
accprofile	Admin user access profile.	string	Maximum length: 35	
vdom <name>	Virtual domains. Virtual domain name.	string	Maximum length: 79	
schedule	Schedule name.	string	Maximum length: 35	
cors-allow-origin	Value for Access-Control-Allow-Origin on API responses. Avoid using '*' if possible.	string	Maximum length: 269	
peer-auth	Enable/disable peer authentication.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable peer.	
		<i>disable</i>	Disable peer.	

Parameter	Description	Type	Size	Default
peer-group	Peer group name.	string	Maximum length: 35	

config trusthost

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
type	Trusthost type.	option	-	ipv4-trusthost						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4-trusthost</td><td>IPv4 trusthost.</td></tr><tr><td>ipv6-trusthost</td><td>IPv6 trusthost.</td></tr></table>				Option	Description	ipv4-trusthost	IPv4 trusthost.	ipv6-trusthost	IPv6 trusthost.
	Option	Description								
	ipv4-trusthost	IPv4 trusthost.								
ipv6-trusthost	IPv6 trusthost.									
ipv4-trusthost	IPv4 trusted host address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0						
ipv6-trusthost	IPv6 trusted host address.	ipv6-prefix	Not Specified	::/0						

config system arp-table

Configure ARP table.

```
config system arp-table
  Description: Configure ARP table.
  edit <id>
    set interface {string}
    set ip {ipv4-address}
    set mac {mac-address}
  next
end
```

config system arp-table

Parameter	Description	Type	Size	Default
id	Unique integer ID of the entry.	integer	Minimum value: 0 Maximum value: 4294967295	0
interface	Interface name.	string	Maximum length: 15	
ip	IP address.	ipv4-address	Not Specified	0.0.0.0
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00

config system arp

IPv4 ARP table.

```
config system arp
    Description: IPv4 ARP table.
end
```

config system auto-install

Configure USB auto installation.

```
config system auto-install
    Description: Configure USB auto installation.
    set auto-install-config [enable|disable]
    set auto-install-image [enable|disable]
    set default-config-file {string}
    set default-image-file {string}
end
```

config system auto-install

Parameter	Description	Type	Size	Default
auto-install-config	Enable/disable auto install the config in USB disk.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable config.		
	<i>disable</i>	Disable config.		
auto-install-image	Enable/disable auto install the image in USB disk.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable config.		
	<i>disable</i>	Disable config.		
default-config-file	Default config file name in USB disk.	string	Maximum length: 127	fpx_system.conf
default-image-file	Default image file name in USB disk.	string	Maximum length: 127	image.out

config system auto-script

Configure auto script.

```

config system auto-script
    Description: Configure auto script.
    edit <name>
        set interval {integer}
        set repeat {integer}
        set start [manual|auto]
        set script {var-string}
        set password {password}
        set output-size {integer}
        set timeout {integer}
    next
end

```

config system auto-script

Parameter	Description	Type	Size	Default
name	Auto script name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
interval	Repeat interval in seconds.	integer	Minimum value: 0 Maximum value: 31557600	0
repeat	Number of times to repeat this script (0 = infinite).	integer	Minimum value: 0 Maximum value: 65535	1
start	Script starting mode.	option	-	manual
	Option	Description		
	manual	Starting manually.		
	auto	Starting automatically.		
script	List of FortiProxy CLI commands to repeat.	var-string	Maximum length: 1023	
password	Script password to replace %%PASSWD%% tag in the script. Use cases include replacing a password tag for sftp/ftp server password.	password	Not Specified	
output-size	Number of megabytes to limit script output to.	integer	Minimum value: 10 Maximum value: 1024	10
timeout	Maximum running time for this script in seconds (0 = no timeout).	integer	Minimum value: 0 Maximum value: 300	0

config system auto-update status

Status of automatic updates.

```
config system auto-update status
    Description: Status of automatic updates.
end
```

config system auto-update versions

Update object versions.

```
config system auto-update versions
    Description: Update object versions.
end
```

config system automation-action

Action for automation stitches.

```
config system automation-action
    Description: Action for automation stitches.
    edit <name>
        set description {var-string}
        set action-type [email|fortiexplorer-notification|...]
        set system-action [reboot|shutdown|...]
        set tls-certificate {string}
        set email-to <name1>, <name2>, ...
        set email-from {var-string}
        set email-subject {var-string}
        set minimum-interval {integer}
        set aws-api-key {password}
        set azure-function-authorization [anonymous|function|...]
        set azure-api-key {password}
        set alicloud-function-authorization [anonymous|function]
        set alicloud-access-key-id {string}
        set alicloud-access-key-secret {password}
        set message-type [text|json]
        set message {string}
        set replacement-message [enable|disable]
        set replacemsg-group {string}
        set protocol [http|https]
        set method [post|put|...]
        set uri {var-string}
        set http-body {var-string}
        set port {integer}
        config http-headers
            Description: Request headers.
            edit <id>
                set key {var-string}
                set value {var-string}
            next
        end
        set verify-host-cert [enable|disable]
        set script {var-string}
        set output-size {integer}
        set timeout {integer}
        set password {password}
        set execute-security-fabric [enable|disable]
        set accprofile {string}
```

```

    set security-tag {string}
    set sdn-connector <name1>, <name2>, ...
next
end

```

config system automation-action

Parameter	Description	Type	Size	Default																																				
name	Name.	string	Maximum length: 64																																					
description	Description.	var-string	Maximum length: 255																																					
action-type	Action type.	option	-	alert																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>email</td><td>Send notification email.</td></tr><tr><td>fortiexplorer-notification</td><td>Send push notification to FortiExplorer.</td></tr><tr><td>alert</td><td>Generate FortiProxy dashboard alert.</td></tr><tr><td>disable-ssid</td><td>Disable interface.</td></tr><tr><td>system-actions</td><td>Perform immediate system operations on this FortiGate unit.</td></tr><tr><td>quarantine</td><td>Quarantine host.</td></tr><tr><td>quarantine-forticlient</td><td>Quarantine FortiClient by EMS.</td></tr><tr><td>quarantine-nsx</td><td>Quarantine NSX instance.</td></tr><tr><td>quarantine-fortinac</td><td>Quarantine host by FortiNAC.</td></tr><tr><td>ban-ip</td><td>Ban IP address.</td></tr><tr><td>aws-lambda</td><td>Send log data to integrated AWS service.</td></tr><tr><td>azure-function</td><td>Send log data to an Azure function.</td></tr><tr><td>google-cloud-function</td><td>Send log data to a Google Cloud function.</td></tr><tr><td>alicloud-function</td><td>Send log data to an AliCloud function.</td></tr><tr><td>webhook</td><td>Send an HTTP request.</td></tr><tr><td>cli-script</td><td>Run CLI script.</td></tr><tr><td>slack-notification</td><td>Send a notification message to a Slack incoming webhook.</td></tr></table>				Option	Description	email	Send notification email.	fortiexplorer-notification	Send push notification to FortiExplorer.	alert	Generate FortiProxy dashboard alert.	disable-ssid	Disable interface.	system-actions	Perform immediate system operations on this FortiGate unit.	quarantine	Quarantine host.	quarantine-forticlient	Quarantine FortiClient by EMS.	quarantine-nsx	Quarantine NSX instance.	quarantine-fortinac	Quarantine host by FortiNAC.	ban-ip	Ban IP address.	aws-lambda	Send log data to integrated AWS service.	azure-function	Send log data to an Azure function.	google-cloud-function	Send log data to a Google Cloud function.	alicloud-function	Send log data to an AliCloud function.	webhook	Send an HTTP request.	cli-script	Run CLI script.	slack-notification	Send a notification message to a Slack incoming webhook.
Option	Description																																							
email	Send notification email.																																							
fortiexplorer-notification	Send push notification to FortiExplorer.																																							
alert	Generate FortiProxy dashboard alert.																																							
disable-ssid	Disable interface.																																							
system-actions	Perform immediate system operations on this FortiGate unit.																																							
quarantine	Quarantine host.																																							
quarantine-forticlient	Quarantine FortiClient by EMS.																																							
quarantine-nsx	Quarantine NSX instance.																																							
quarantine-fortinac	Quarantine host by FortiNAC.																																							
ban-ip	Ban IP address.																																							
aws-lambda	Send log data to integrated AWS service.																																							
azure-function	Send log data to an Azure function.																																							
google-cloud-function	Send log data to a Google Cloud function.																																							
alicloud-function	Send log data to an AliCloud function.																																							
webhook	Send an HTTP request.																																							
cli-script	Run CLI script.																																							
slack-notification	Send a notification message to a Slack incoming webhook.																																							

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>microsoft-teams-notification</i></td><td>Send a notification message to a Microsoft Teams incoming webhook.</td></tr></table>	Option	Description	<i>microsoft-teams-notification</i>	Send a notification message to a Microsoft Teams incoming webhook.							
	Option	Description										
	<i>microsoft-teams-notification</i>	Send a notification message to a Microsoft Teams incoming webhook.										
system-action	System action type.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>reboot</i></td><td>Reboot this FortiGate unit.</td></tr><tr><td><i>shutdown</i></td><td>Shutdown this FortiGate unit.</td></tr><tr><td><i>backup-config</i></td><td>Backup current configuration to the disk revisions.</td></tr></table>	Option	Description	<i>reboot</i>	Reboot this FortiGate unit.	<i>shutdown</i>	Shutdown this FortiGate unit.	<i>backup-config</i>	Backup current configuration to the disk revisions.			
	Option	Description										
	<i>reboot</i>	Reboot this FortiGate unit.										
	<i>shutdown</i>	Shutdown this FortiGate unit.										
<i>backup-config</i>	Backup current configuration to the disk revisions.											
tls-certificate	Custom TLS certificate for API request.	string	Maximum length: 35									
email-to <name>	Email addresses. Email address.	string	Maximum length: 255									
email-from	Email sender name.	var-string	Maximum length: 127									
email-subject	Email subject.	var-string	Maximum length: 511									
minimum-interval	Limit execution to no more than once in this interval (in seconds).	integer	Minimum value: 0 Maximum value: 2592000	0								
aws-api-key	AWS API Gateway API key.	password	Not Specified									
azure-function-authorization	Azure function authorization level.	option	-	anonymous								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>anonymous</i></td><td>Anonymous authorization level (No authorization required).</td></tr><tr><td><i>function</i></td><td>Function authorization level (Function or Host Key required).</td></tr><tr><td><i>admin</i></td><td>Admin authorization level (Master Host Key required).</td></tr></table>	Option	Description	<i>anonymous</i>	Anonymous authorization level (No authorization required).	<i>function</i>	Function authorization level (Function or Host Key required).	<i>admin</i>	Admin authorization level (Master Host Key required).			
	Option	Description										
	<i>anonymous</i>	Anonymous authorization level (No authorization required).										
	<i>function</i>	Function authorization level (Function or Host Key required).										
<i>admin</i>	Admin authorization level (Master Host Key required).											
azure-api-key	Azure function API key.	password	Not Specified									
alicloud-function-authorization	AliCloud function authorization type.	option	-	anonymous								

Parameter	Description	Type	Size	Default
	Option Description			
	<i>anonymous</i>	Anonymous authorization (No authorization required).		
	<i>function</i>	Function authorization (Authorization required).		
alicloud-access-key-id	AliCloud AccessKey ID.	string	Maximum length: 35	
alicloud-access-key-secret	AliCloud AccessKey secret.	password	Not Specified	
message-type	Message type.	option	-	text
	Option Description			
	<i>text</i>	Plaintext.		
	<i>json</i>	Custom JSON.		
message	Message content.	string	Maximum length: 4095	%%log%%
replacement-message	Enable/disable replacement message.	option	-	disable
	Option Description			
	<i>enable</i>	Enable replacement message.		
	<i>disable</i>	Disable replacement message.		
replacemsg-group	Replacement message group.	string	Maximum length: 35	
protocol	Request protocol.	option	-	http
	Option Description			
	<i>http</i>	HTTP.		
	<i>https</i>	HTTPS.		
method	Request method (POST, PUT, GET, PATCH or DELETE).	option	-	post
	Option Description			
	<i>post</i>	POST.		
	<i>put</i>	PUT.		
	<i>get</i>	GET.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>patch</i>	PATCH.		
	<i>delete</i>	DELETE.		
uri	Request API URI.	var-string	Maximum length: 1023	
http-body	Request body (if necessary). Should be serialized json string.	var-string	Maximum length: 4095	
port	Protocol port.	integer	Minimum value: 1 Maximum value: 65535	0
verify-host-cert	Enable/disable verification of the remote host certificate.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable verification of the remote host certificate.		
	<i>disable</i>	Disable verification of the remote host certificate.		
script	CLI script.	var-string	Maximum length: 1023	
output-size	Number of megabytes to limit script output to.	integer	Minimum value: 1 Maximum value: 1024	10
timeout	Maximum running time for this script in seconds (0 = no timeout).	integer	Minimum value: 0 Maximum value: 300	0
password	Script password to replace %%PASSWD%% tag in the script. Use cases include replacing a password tag for sftp/ftp server password.	password	Not Specified	
execute-security-fabric	Enable/disable execution of CLI script on all or only one FortiGate unit in the Security Fabric.	option	-	disable
	Option	Description		
	<i>enable</i>	CLI script executes on all FortiGate units in the Security Fabric.		
	<i>disable</i>	CLI script executes only on the FortiGate unit that the stitch is triggered.		

Parameter	Description	Type	Size	Default
accprofile	Access profile for CLI script action to access FortiProxy features.	string	Maximum length: 35	
security-tag	NSX security tag.	string	Maximum length: 255	
sdn-connector <name>	NSX SDN connector names. SDN connector name.	string	Maximum length: 79	

config http-headers

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
key	Request header key.	var-string	Maximum length: 1023	
value	Request header value.	var-string	Maximum length: 4095	

config system automation-destination

Automation destinations.

```

config system automation-destination
    Description: Automation destinations.
    edit <name>
        set type [fortiproxy|ha-cluster]
        set destination <name1>, <name2>, ...
        set ha-group-id {integer}
    next
end

```

config system automation-destination

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
type	Destination type.	option	-	fortiproxy

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>fortiproxy</i>	FortiProxy set as destination.		
	<i>ha-cluster</i>	HA cluster set as destination.		
destination <name>	Destinations. Destination.	string	Maximum length: 31	
ha-group-id	Cluster group ID set for this destination.	integer	Minimum value: 0 Maximum value: 255	0

config system automation-stitch

Automation stitches.

```

config system automation-stitch
  Description: Automation stitches.
  edit <name>
    set description {var-string}
    set status [enable|disable]
    set trigger {string}
    config actions
      Description: Configure stitch actions.
      edit <id>
        set action {string}
        set delay {integer}
        set required [enable|disable]
      next
    end
    set destination <name1>, <name2>, ...
  next
end

```

config system automation-stitch

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
description	Description.	var-string	Maximum length: 255	
status	Enable/disable this stitch.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable stitch.		
	<i>disable</i>	Disable stitch.		
trigger	Trigger name.	string	Maximum length: 35	
destination <name>	Serial number/HA group-name of destination devices. Destination name.	string	Maximum length: 79	

config actions

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
action	Action name.	string	Maximum length: 64	
delay	Delay before execution (in seconds).	integer	Minimum value: 0 Maximum value: 3600	0
required	Required in action chain.	option	-	disable
	Option	Description		
	<i>enable</i>	Required in action chain.		
	<i>disable</i>	Not required in action chain.		

config system automation-trigger

Trigger for automation stitches.

```
config system automation-trigger
  Description: Trigger for automation stitches.
  edit <name>
    set description {var-string}
    set trigger-type [event-based|scheduled]
    set event-type [ioc|event-log|...]
    set vdom <name1>, <name2>, ...
```

```

set license-type [forticare-support|fortiguard-webfilter|...]
set report-type [posture|coverage|...]
set logid <id1>, <id2>, ...
set trigger-frequency [hourly|daily|...]
set trigger-weekday [sunday|monday|...]
set trigger-day {integer}
set trigger-hour {integer}
set trigger-minute {integer}
set trigger-datetime {datetime}
config fields
    Description: Customized trigger field settings.
    edit <id>
        set name {string}
        set value {var-string}
    next
end
set faz-event-name {var-string}
set faz-event-severity {var-string}
set faz-event-tags {var-string}
set serial {var-string}
set fabric-event-name {var-string}
set fabric-event-severity {var-string}
next
end

```

config system automation-trigger

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
description	Description.	var-string	Maximum length: 255	
trigger-type	Trigger type.	option	-	event-based
	Option	Description		
	event-based	Event based trigger.		
	scheduled	Scheduled trigger.		
event-type	Event type.	option	-	ioc
	Option	Description		
	ioc	Indicator of compromise detected.		
	event-log	Use log ID as trigger.		
	reboot	Device reboot.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>low-memory</i>	Conserve mode due to low memory.		
	<i>high-cpu</i>	High CPU usage.		
	<i>license-near-expiry</i>	License near expiration date.		
	<i>local-cert-near-expiry</i>	The local certificate near expiration date.		
	<i>ha-failover</i>	HA failover.		
	<i>config-change</i>	Configuration change.		
	<i>security-rating-summary</i>	Security rating summary.		
	<i>virus-ips-db-updated</i>	Virus and IPS database updated.		
	<i>faz-event</i>	FortiAnalyzer event.		
	<i>incoming-webhook</i>	Incoming webhook call.		
	<i>fabric-event</i>	Fabric connector event.		
	<i>ips-logs</i>	IPS logs.		
	<i>anomaly-logs</i>	Anomaly logs.		
	<i>virus-logs</i>	Virus logs.		
	<i>ssh-logs</i>	SSH logs.		
	<i>webfilter-violation</i>	Webfilter violation.		
<i>traffic-violation</i>	Traffic violation.			
vdom <name>	Virtual domain(s) that this trigger is valid for. Virtual domain name.	string	Maximum length: 79	
license-type	License type.	option	-	forticare-support
	Option	Description		
	<i>forticare-support</i>	FortiCare support license.		
	<i>fortiguard-webfilter</i>	FortiGuard web filter license.		

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortiguard-antispam</i></td><td>FortiGuard antispam license.</td></tr><tr><td><i>fortiguard-antivirus</i></td><td>FortiGuard AntiVirus license.</td></tr><tr><td><i>fortiguard-ips</i></td><td>FortiGuard IPS license.</td></tr><tr><td><i>fortiguard-management</i></td><td>FortiGuard management service license.</td></tr><tr><td><i>forticloud</i></td><td>FortiCloud license.</td></tr><tr><td><i>any</i></td><td>Any license.</td></tr></table>	Option	Description	<i>fortiguard-antispam</i>	FortiGuard antispam license.	<i>fortiguard-antivirus</i>	FortiGuard AntiVirus license.	<i>fortiguard-ips</i>	FortiGuard IPS license.	<i>fortiguard-management</i>	FortiGuard management service license.	<i>forticloud</i>	FortiCloud license.	<i>any</i>	Any license.			
	Option	Description																
	<i>fortiguard-antispam</i>	FortiGuard antispam license.																
	<i>fortiguard-antivirus</i>	FortiGuard AntiVirus license.																
	<i>fortiguard-ips</i>	FortiGuard IPS license.																
	<i>fortiguard-management</i>	FortiGuard management service license.																
	<i>forticloud</i>	FortiCloud license.																
<i>any</i>	Any license.																	
report-type	Security Rating report.	option	-	posture														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>posture</i></td><td>Posture report.</td></tr><tr><td><i>coverage</i></td><td>Coverage report.</td></tr><tr><td><i>optimization</i></td><td>Optimization report</td></tr><tr><td><i>any</i></td><td>Any report.</td></tr></table>	Option	Description	<i>posture</i>	Posture report.	<i>coverage</i>	Coverage report.	<i>optimization</i>	Optimization report	<i>any</i>	Any report.							
	Option	Description																
	<i>posture</i>	Posture report.																
	<i>coverage</i>	Coverage report.																
	<i>optimization</i>	Optimization report																
<i>any</i>	Any report.																	
logid <id>	Log IDs to trigger event. Log ID.	integer	Minimum value: 1 Maximum value: 65535															
trigger-frequency	Scheduled trigger frequency.	option	-	daily														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hourly</i></td><td>Run hourly.</td></tr><tr><td><i>daily</i></td><td>Run daily.</td></tr><tr><td><i>weekly</i></td><td>Run weekly.</td></tr><tr><td><i>monthly</i></td><td>Run monthly.</td></tr><tr><td><i>once</i></td><td>Run once at specified date time.</td></tr></table>	Option	Description	<i>hourly</i>	Run hourly.	<i>daily</i>	Run daily.	<i>weekly</i>	Run weekly.	<i>monthly</i>	Run monthly.	<i>once</i>	Run once at specified date time.					
	Option	Description																
	<i>hourly</i>	Run hourly.																
	<i>daily</i>	Run daily.																
	<i>weekly</i>	Run weekly.																
	<i>monthly</i>	Run monthly.																
<i>once</i>	Run once at specified date time.																	
trigger-weekday	Day of week for trigger.	option	-															

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>sunday</i>	Sunday.		
	<i>monday</i>	Monday.		
	<i>tuesday</i>	Tuesday.		
	<i>wednesday</i>	Wednesday.		
	<i>thursday</i>	Thursday.		
	<i>friday</i>	Friday.		
	<i>saturday</i>	Saturday.		
trigger-day	Day within a month to trigger.	integer	Minimum value: 1 Maximum value: 31	1
trigger-hour	Hour of the day on which to trigger.	integer	Minimum value: 0 Maximum value: 23	0
trigger-minute	Minute of the hour on which to trigger.	integer	Minimum value: 0 Maximum value: 59	0
trigger-datetime	Trigger date and time (YYYY-MM-DD HH:MM:SS).	datetime	Not Specified	0000-00-00 00:00:00
faz-event-name	FortiAnalyzer event handler name.	var-string	Maximum length: 255	
faz-event-severity	FortiAnalyzer event severity.	var-string	Maximum length: 255	
faz-event-tags	FortiAnalyzer event tags.	var-string	Maximum length: 255	
serial	Fabric connector serial number.	var-string	Maximum length: 255	
fabric-event-name	Fabric connector event handler name.	var-string	Maximum length: 255	
fabric-event-severity	Fabric connector event severity.	var-string	Maximum length: 255	

config fields

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name.	string	Maximum length: 35	
value	Value.	var-string	Maximum length: 63	

config system autoupdate schedule

Configure update schedule.

```
config system autoupdate schedule
    Description: Configure update schedule.
    set status [enable|disable]
    set frequency [every|daily|...]
    set time {user}
    set day [Sunday|Monday|...]
end
```

config system autoupdate schedule

Parameter	Description	Type	Size	Default
status	Enable/disable scheduled updates.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
frequency	Update frequency.	option	-	automatic
	Option	Description		
	<i>every</i>	Time interval.		
	<i>daily</i>	Every day.		
	<i>weekly</i>	Every week.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>automatic</i>	Update automatically within every one hour period.		
time	Update time.	user	Not Specified	
day	Update day.	option	-	Monday
	Option	Description		
	<i>Sunday</i>	Update every Sunday.		
	<i>Monday</i>	Update every Monday.		
	<i>Tuesday</i>	Update every Tuesday.		
	<i>Wednesday</i>	Update every Wednesday.		
	<i>Thursday</i>	Update every Thursday.		
	<i>Friday</i>	Update every Friday.		
	<i>Saturday</i>	Update every Saturday.		

config system autoupdate tunneling

Configure web proxy tunneling for the FDN.

```
config system autoupdate tunneling
    Description: Configure web proxy tunneling for the FDN.
    set status [enable|disable]
    set address {string}
    set port {integer}
    set username {string}
    set password {password}
end
```

config system autoupdate tunneling

Parameter	Description	Type	Size	Default
status	Enable/disable web proxy tunneling.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default
address	Web proxy IP address or FQDN.	string	Maximum length: 63	
port	Web proxy port.	integer	Minimum value: 0 Maximum value: 65535	0
username	Web proxy username.	string	Maximum length: 49	
password	Web proxy password.	password	Not Specified	

config system central-management

Configure central management.

```

config system central-management
    Description: Configure central management.
    set mode [normal|backup]
    set type [fortimanager|fortiguard|...]
    set fortigate-cloud-sso-default-profile {string}
    set schedule-config-restore [enable|disable]
    set schedule-script-restore [enable|disable]
    set allow-push-configuration [enable|disable]
    set allow-push-firmware [enable|disable]
    set allow-remote-firmware-upgrade [enable|disable]
    set allow-monitor [enable|disable]
    set serial-number {user}
    set fmg {user}
    set fmg-source-ip {ipv4-address}
    set fmg-source-ip6 {ipv6-address}
    set local-cert {string}
    set ca-cert {user}
    set vdom {string}
    config server-list
        Description: Additional servers that the FortiProxy can use for updates (for AV, IPS,
updates) and ratings (for web filter and antispam ratings) servers.
        edit <id>
            set server-type {option1}, {option2}, ...
            set addr-type [ipv4|ipv6|...]
            set server-address {ipv4-address}
            set server-address6 {ipv6-address}
            set fqdn {string}
        next
    end
    set fmg-update-port [8890|443]
    set include-default-servers [enable|disable]
    set enc-algorithm [default|high|...]

```

```

set interface-select-method [auto|specify]
set interface {string}
end

```

config system central-management

Parameter	Description	Type	Size	Default								
mode	Central management mode.	option	-	normal								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>normal</i></td><td>Manage and configure this FortiProxy from FortiManager.</td></tr><tr><td><i>backup</i></td><td>Manage and configure this FortiProxy locally and back up its configuration to FortiManager.</td></tr></table>	Option	Description	<i>normal</i>	Manage and configure this FortiProxy from FortiManager.	<i>backup</i>	Manage and configure this FortiProxy locally and back up its configuration to FortiManager.					
Option	Description											
<i>normal</i>	Manage and configure this FortiProxy from FortiManager.											
<i>backup</i>	Manage and configure this FortiProxy locally and back up its configuration to FortiManager.											
type	Central management type.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortimanager</i></td><td>FortiManager.</td></tr><tr><td><i>fortiguard</i></td><td>Central management of this FortiProxy using FortiCloud.</td></tr><tr><td><i>none</i></td><td>No central management.</td></tr></table>	Option	Description	<i>fortimanager</i>	FortiManager.	<i>fortiguard</i>	Central management of this FortiProxy using FortiCloud.	<i>none</i>	No central management.			
Option	Description											
<i>fortimanager</i>	FortiManager.											
<i>fortiguard</i>	Central management of this FortiProxy using FortiCloud.											
<i>none</i>	No central management.											
fortigate-cloud-sso-default-profile	Override access profile.	string	Maximum length: 35									
schedule-config-restore	Enable/disable allowing the central management server to restore the configuration of this FortiProxy.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable scheduled configuration restore.</td></tr><tr><td><i>disable</i></td><td>Disable scheduled configuration restore.</td></tr></table>	Option	Description	<i>enable</i>	Enable scheduled configuration restore.	<i>disable</i>	Disable scheduled configuration restore.					
Option	Description											
<i>enable</i>	Enable scheduled configuration restore.											
<i>disable</i>	Disable scheduled configuration restore.											
schedule-script-restore	Enable/disable allowing the central management server to restore the scripts stored on this FortiProxy.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable scheduled script restore.</td></tr><tr><td><i>disable</i></td><td>Disable scheduled script restore.</td></tr></table>	Option	Description	<i>enable</i>	Enable scheduled script restore.	<i>disable</i>	Disable scheduled script restore.					
Option	Description											
<i>enable</i>	Enable scheduled script restore.											
<i>disable</i>	Disable scheduled script restore.											
allow-push-configuration	Enable/disable allowing the central management server to push configuration changes to this FortiProxy.	option	-	enable								

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable push configuration.		
	<i>disable</i>	Disable push configuration.		
allow-push-firmware	Enable/disable allowing the central management server to push firmware updates to this FortiProxy.	option	-	enable
	Option Description			
	<i>enable</i>	Enable push firmware.		
	<i>disable</i>	Disable push firmware.		
allow-remote-firmware-upgrade	Enable/disable remotely upgrading the firmware on this FortiProxy from the central management server.	option	-	enable
	Option Description			
	<i>enable</i>	Enable remote firmware upgrade.		
	<i>disable</i>	Disable remote firmware upgrade.		
allow-monitor	Enable/disable allowing the central management server to remotely monitor this FortiProxy unit.	option	-	enable
	Option Description			
	<i>enable</i>	Enable remote monitoring of device.		
	<i>disable</i>	Disable remote monitoring of device.		
serial-number	Serial number.	user	Not Specified	
fmg	IP address or FQDN of the FortiManager.	user	Not Specified	
fmg-source-ip	IPv4 source address that this FortiProxy uses when communicating with FortiManager.	ipv4-address	Not Specified	0.0.0.0
fmg-source-ip6	IPv6 source address that this FortiProxy uses when communicating with FortiManager.	ipv6-address	Not Specified	::
local-cert	Certificate to be used by FGFM protocol.	string	Maximum length: 35	
ca-cert	CA certificate to be used by FGFM protocol.	user	Not Specified	

Parameter	Description	Type	Size	Default								
vdom	Virtual domain (VDOM) name to use when communicating with FortiManager.	string	Maximum length: 31	root								
fmg-update-port	Port used to communicate with FortiManager that is acting as a FortiGuard update server.	option	-	8890								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>8890</td><td>Use port 8890 to communicate with FortiManager that is acting as a FortiGuard update server.</td></tr><tr><td>443</td><td>Use port 443 to communicate with FortiManager that is acting as a FortiGuard update server.</td></tr></table>				Option	Description	8890	Use port 8890 to communicate with FortiManager that is acting as a FortiGuard update server.	443	Use port 443 to communicate with FortiManager that is acting as a FortiGuard update server.		
	Option	Description										
	8890	Use port 8890 to communicate with FortiManager that is acting as a FortiGuard update server.										
443	Use port 443 to communicate with FortiManager that is acting as a FortiGuard update server.											
include-default-servers	Enable/disable inclusion of public FortiGuard servers in the override server list.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable inclusion of public FortiGuard servers in the override server list.</td></tr><tr><td>disable</td><td>Disable inclusion of public FortiGuard servers in the override server list.</td></tr></table>				Option	Description	enable	Enable inclusion of public FortiGuard servers in the override server list.	disable	Disable inclusion of public FortiGuard servers in the override server list.		
	Option	Description										
	enable	Enable inclusion of public FortiGuard servers in the override server list.										
disable	Disable inclusion of public FortiGuard servers in the override server list.											
enc-algorithm	Encryption strength for communications between the FortiProxy and central management.	option	-	high								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>High strength algorithms and medium-strength 128-bit key length algorithms.</td></tr><tr><td>high</td><td>128-bit and larger key length algorithms.</td></tr><tr><td>low</td><td>64-bit or 56-bit key length algorithms without export restrictions.</td></tr></table>				Option	Description	default	High strength algorithms and medium-strength 128-bit key length algorithms.	high	128-bit and larger key length algorithms.	low	64-bit or 56-bit key length algorithms without export restrictions.
	Option	Description										
	default	High strength algorithms and medium-strength 128-bit key length algorithms.										
	high	128-bit and larger key length algorithms.										
low	64-bit or 56-bit key length algorithms without export restrictions.											
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	auto	Set outgoing interface automatically.	specify	Set outgoing interface manually.		
	Option	Description										
	auto	Set outgoing interface automatically.										
specify	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

config server-list

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
server-type	FortiGuard service type.	option	-	
	Option Description			
	update	AV, IPS, and AV-query update server.		
	rating	Web filter and anti-spam rating server.		
	iot-query	IoT query server.		
	iot-collect	IoT device collection server.		
addr-type	Indicate whether the FortiProxy communicates with the override server using an IPv4 address, an IPv6 address or a FQDN.	option	-	ipv4
	Option Description			
	ipv4	IPv4 address.		
	ipv6	IPv6 address.		
	fqdn	FQDN.		
server-address	IPv4 address of override server.	ipv4-address	Not Specified	0.0.0.0
server-address6	IPv6 address of override server.	ipv6-address	Not Specified	::
fqdn	FQDN address of override server.	string	Maximum length: 255	

config system central-mgmt

Configuration of Central Management Service.

```
config system central-mgmt
    Description: Configuration of Central Management Service.
end
```

config system checksum status

System checksum.

```
config system checksum status
    Description: System checksum.
end
```

config system cmdb

System CMDB information.

```
config system cmdb
    Description: System CMDB information.
end
```

config system console

Configure console.

```
config system console
    Description: Configure console.
    set baudrate [9600|19200|...]
    set output [standard|more]
    set login [enable|disable]
end
```

config system console

Parameter	Description	Type	Size	Default
baudrate	Console baud rate.	option	-	9600
	Option			Description
	9600			9600
	19200			19200
	38400			38400
	57600			57600
	115200			115200
output	Console output mode.	option	-	more

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>standard</i>	Standard output.		
	<i>more</i>	More page output.		
login	Enable/disable serial console and FortiExplorer.	option	-	enable
	Option	Description		
	<i>enable</i>	Console login enable.		
	<i>disable</i>	Console login disable.		

config system csf

Add this FortiProxy to a Security Fabric or set up a new Security Fabric on this FortiProxy.

```
config system csf
```

Description: Add this FortiProxy to a Security Fabric or set up a new Security Fabric on this FortiProxy.

```
set status [enable|disable]
set upstream {string}
set source-ip {ipv4-address}
set upstream-interface-select-method [auto|specify]
set upstream-interface {string}
set upstream-port {integer}
set group-name {string}
set group-password {password}
set accept-auth-by-cert [disable|enable]
set log-unification [disable|enable]
set authorization-request-type [serial|certificate]
set certificate {string}
set fabric-workers {integer}
set downstream-access [enable|disable]
set license-sharing [enable|disable]
set preferred-seats {integer}
set legacy-authentication [disable|enable]
set downstream-accprofile {string}
set configuration-sync [default|local]
set fabric-object-unification [default|local]
set saml-configuration-sync [default|local]
config trusted-list
```

Description: Pre-authorized and blocked security fabric nodes.

```
edit <name>
```

```
set authorization-type [serial|certificate]
set serial {string}
set certificate {var-string}
set action [accept|deny]
set ha-members {string}
set downstream-authorization [enable|disable]
```

```

        set preferred-seats {integer}
        set index {integer}
    next
end
config fabric-connector
    Description: Fabric connector configuration.
    edit <serial>
        set accprofile {string}
        set configuration-write-access [enable|disable]
    next
end
set forticloud-account-enforcement [enable|disable]
set file-mgmt [enable|disable]
set file-quota {integer}
set file-quota-warning {integer}
end

```

config system csf

Parameter	Description	Type	Size	Default
status	Enable/disable Security Fabric.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Security Fabric.		
	<i>disable</i>	Disable Security Fabric.		
upstream	IP/FQDN of the FortiProxy upstream from this FortiProxy in the Security Fabric.	string	Maximum length: 255	
source-ip	Source IP address for communication with the upstream FortiGate.	ipv4-address	Not Specified	0.0.0.0
upstream-interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
upstream-interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
upstream-port	The port number to use to communicate with the FortiProxy upstream from this FortiProxy in the Security Fabric.	integer	Minimum value: 1 Maximum value: 65535	8013

Parameter	Description	Type	Size	Default						
group-name	Security Fabric group name. All FortiProxys in a Security Fabric must have the same group name.	string	Maximum length: 35							
group-password	Security Fabric group password. All FortiProxys in a Security Fabric must have the same group password.	password	Not Specified							
accept-auth-by-cert	Accept connections with unknown certificates and ask admin for approval.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not accept SSL connections with unknown certificates.</td></tr><tr><td><i>enable</i></td><td>Accept SSL connections without automatic certificate verification.</td></tr></table>	Option	Description	<i>disable</i>	Do not accept SSL connections with unknown certificates.	<i>enable</i>	Accept SSL connections without automatic certificate verification.			
Option	Description									
<i>disable</i>	Do not accept SSL connections with unknown certificates.									
<i>enable</i>	Accept SSL connections without automatic certificate verification.									
log-unification	Enable/disable broadcast of discovery messages for log unification.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable broadcast of discovery messages for log unification.</td></tr><tr><td><i>enable</i></td><td>Enable broadcast of discovery messages for log unification.</td></tr></table>	Option	Description	<i>disable</i>	Disable broadcast of discovery messages for log unification.	<i>enable</i>	Enable broadcast of discovery messages for log unification.			
Option	Description									
<i>disable</i>	Disable broadcast of discovery messages for log unification.									
<i>enable</i>	Enable broadcast of discovery messages for log unification.									
authorization-request-type	Authorization request type.	option	-	serial						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>serial</i></td><td>Request verification by serial number.</td></tr><tr><td><i>certificate</i></td><td>Request verification by certificate.</td></tr></table>	Option	Description	<i>serial</i>	Request verification by serial number.	<i>certificate</i>	Request verification by certificate.			
Option	Description									
<i>serial</i>	Request verification by serial number.									
<i>certificate</i>	Request verification by certificate.									
certificate	Certificate.	string	Maximum length: 35							
fabric-workers	Number of worker processes for Security Fabric daemon.	integer	Minimum value: 1 Maximum value: 4	2						
downstream-access	Enable/disable downstream device access to this device's configuration and data.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable downstream device access to this device's configuration and data.</td></tr><tr><td><i>disable</i></td><td>Disable downstream device access to this device's configuration and data.</td></tr></table>	Option	Description	<i>enable</i>	Enable downstream device access to this device's configuration and data.	<i>disable</i>	Disable downstream device access to this device's configuration and data.			
Option	Description									
<i>enable</i>	Enable downstream device access to this device's configuration and data.									
<i>disable</i>	Disable downstream device access to this device's configuration and data.									

Parameter	Description	Type	Size	Default						
license-sharing	Enable/disable license sharing between FortiProxy devices.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable license sharing.</td></tr><tr><td><i>disable</i></td><td>Disable license sharing.</td></tr></table>	Option	Description	<i>enable</i>	Enable license sharing.	<i>disable</i>	Disable license sharing.			
Option	Description									
<i>enable</i>	Enable license sharing.									
<i>disable</i>	Disable license sharing.									
preferred-seats	The number of seats this FortiProxy device as CSF root should be allocated with. The number of gurrantted seats is capped by minimum of the number of local purchased seats and the number of preferred seats. And the rest of preferred seats will be allocated from shared pool at higher priority.	integer	Minimum value: 0 Maximum value: 4294967295	0						
legacy-authentication	Enable/disable legacy authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not accept legacy authentication requests.</td></tr><tr><td><i>enable</i></td><td>Accept legacy authentication requests.</td></tr></table>	Option	Description	<i>disable</i>	Do not accept legacy authentication requests.	<i>enable</i>	Accept legacy authentication requests.			
Option	Description									
<i>disable</i>	Do not accept legacy authentication requests.									
<i>enable</i>	Accept legacy authentication requests.									
downstream-accprofile	Default access profile for requests from downstream devices.	string	Maximum length: 35							
configuration-sync	Configuration sync mode.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Synchronize configuration for IPAM, FortiAnalyzer, FortiSandbox, and Central Management to root node.</td></tr><tr><td><i>local</i></td><td>Do not synchronize configuration with root node.</td></tr></table>	Option	Description	<i>default</i>	Synchronize configuration for IPAM, FortiAnalyzer, FortiSandbox, and Central Management to root node.	<i>local</i>	Do not synchronize configuration with root node.			
Option	Description									
<i>default</i>	Synchronize configuration for IPAM, FortiAnalyzer, FortiSandbox, and Central Management to root node.									
<i>local</i>	Do not synchronize configuration with root node.									
fabric-object-unification	Fabric CMDB Object Unification.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Global CMDB objects will be synchronized in Security Fabric.</td></tr><tr><td><i>local</i></td><td>Global CMDB objects will not be synchronized to and from this device.</td></tr></table>	Option	Description	<i>default</i>	Global CMDB objects will be synchronized in Security Fabric.	<i>local</i>	Global CMDB objects will not be synchronized to and from this device.			
Option	Description									
<i>default</i>	Global CMDB objects will be synchronized in Security Fabric.									
<i>local</i>	Global CMDB objects will not be synchronized to and from this device.									
saml-configuration-sync	SAML setting configuration synchronization.	option	-	default						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>default</i>	SAML setting for fabric members is created by fabric root.		
	<i>local</i>	Do not apply SAML configuration generated by root.		
forticloud-account-enforcement	Fabric FortiCloud account unification.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable FortiCloud account ID matching for Security Fabric.		
	<i>disable</i>	Disable FortiCloud account ID matching for Security Fabric.		
file-mgmt	Enable/disable Security Fabric daemon file management.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable daemon file management.		
	<i>disable</i>	Disable daemon file management.		
file-quota	Maximum amount of memory that can be used by the daemon files (in bytes).	integer	Minimum value: 0 Maximum value: 4294967295	268435456
file-quota-warning	Warn when the set percentage of quota has been used.	integer	Minimum value: 1 Maximum value: 99	90

config trusted-list

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
authorization-type	Authorization type.	option	-	serial
	Option	Description		
	<i>serial</i>	Verify downstream by serial number.		
	<i>certificate</i>	Verify downstream by certificate.		

Parameter	Description	Type	Size	Default						
serial	Serial.	string	Maximum length: 19							
certificate	Certificate.	var-string	Maximum length: 32767							
action	Security fabric authorization action.	option	-	accept						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accept</i></td><td>Accept authorization request.</td></tr><tr><td><i>deny</i></td><td>Deny authorization request.</td></tr></table>				Option	Description	<i>accept</i>	Accept authorization request.	<i>deny</i>	Deny authorization request.
	Option	Description								
	<i>accept</i>	Accept authorization request.								
<i>deny</i>	Deny authorization request.									
ha-members	HA members.	string	Maximum length: 19							
downstream-authorization	Trust authorizations by this node's administrator.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable downstream authorization.</td></tr><tr><td><i>disable</i></td><td>Disable downstream authorization.</td></tr></table>				Option	Description	<i>enable</i>	Enable downstream authorization.	<i>disable</i>	Disable downstream authorization.
	Option	Description								
	<i>enable</i>	Enable downstream authorization.								
<i>disable</i>	Disable downstream authorization.									
preferred-seats	The number of seats this FortiProxy device should be allocated with. The number of gurranttred seats is capped by minimum of the number of local purchased seats and the number of preferred seats. And the rest of preferred seats will be allocated from shared pool at higher priority.	integer	Minimum value: 0 Maximum value: 4294967295	0						
index	Index of the downstream in tree.	integer	Minimum value: 1 Maximum value: 1024	0						

config fabric-connector

Parameter	Description	Type	Size	Default
serial	Serial.	string	Maximum length: 19	
accprofile	Override access profile.	string	Maximum length: 35	
configuration-write-access	Enable/disable downstream device write access to configuration.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable downstream device write access to configuration.		
	<i>disable</i>	Disable downstream device write access to configuration.		

config system custom-language

Configure custom languages.

```
config system custom-language
    Description: Configure custom languages.
    edit <name>
        set filename {string}
        set comments {var-string}
    next
end
```

config system custom-language

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
filename	Custom language file path.	string	Maximum length: 63	
comments	Comment.	var-string	Maximum length: 255	

config system ddns

Configure DDNS.

```
config system ddns
    Description: Configure DDNS.
    edit <ddnsid>
        set ddns-server [dyndns.org|dyns.net|...]
        set server-type [ipv4|ipv6]
        set ddns-server-addr <addr1>, <addr2>, ...
        set ddns-zone {string}
        set ddns-ttl {integer}
        set ddns-auth [disable|tsig]
        set ddns-keyname {string}
```

```

set ddns-key {password_aes256}
set ddns-domain {string}
set ddns-username {string}
set ddns-sn {string}
set ddns-password {password}
set use-public-ip [disable|enable]
set addr-type [ipv4|ipv6]
set update-interval {integer}
set clear-text [disable|enable]
set ssl-certificate {string}
set bound-ip {string}
set monitor-interface <interface-name1>, <interface-name2>, ...
next
end

```

config system ddns

Parameter	Description	Type	Size	Default																								
ddnsid	DDNS ID.	integer	Minimum value: 0 Maximum value: 4294967295	0																								
ddns-server	Select a DDNS service provider.	option	-																									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dyndns.org</i></td><td>members.dyndns.org and dnsalias.com</td></tr><tr><td><i>dyns.net</i></td><td>www.dyns.net</td></tr><tr><td><i>tzo.com</i></td><td>rh.tzo.com</td></tr><tr><td><i>vavic.com</i></td><td>Peanut Hull</td></tr><tr><td><i>dipdns.net</i></td><td>dipdnsserver.dipdns.com</td></tr><tr><td><i>now.net.cn</i></td><td>ip.todayisp.com</td></tr><tr><td><i>dhs.org</i></td><td>members.dhs.org</td></tr><tr><td><i>easydns.com</i></td><td>members.easydns.com</td></tr><tr><td><i>genericDDNS</i></td><td>Generic DDNS based on RFC2136.</td></tr><tr><td><i>FortiGuardDDNS</i></td><td>FortiGuard DDNS service.</td></tr><tr><td><i>noip.com</i></td><td>dynupdate.no-ip.com</td></tr></table>	Option	Description	<i>dyndns.org</i>	members.dyndns.org and dnsalias.com	<i>dyns.net</i>	www.dyns.net	<i>tzo.com</i>	rh.tzo.com	<i>vavic.com</i>	Peanut Hull	<i>dipdns.net</i>	dipdnsserver.dipdns.com	<i>now.net.cn</i>	ip.todayisp.com	<i>dhs.org</i>	members.dhs.org	<i>easydns.com</i>	members.easydns.com	<i>genericDDNS</i>	Generic DDNS based on RFC2136.	<i>FortiGuardDDNS</i>	FortiGuard DDNS service.	<i>noip.com</i>	dynupdate.no-ip.com			
	Option	Description																										
	<i>dyndns.org</i>	members.dyndns.org and dnsalias.com																										
	<i>dyns.net</i>	www.dyns.net																										
	<i>tzo.com</i>	rh.tzo.com																										
	<i>vavic.com</i>	Peanut Hull																										
	<i>dipdns.net</i>	dipdnsserver.dipdns.com																										
	<i>now.net.cn</i>	ip.todayisp.com																										
	<i>dhs.org</i>	members.dhs.org																										
	<i>easydns.com</i>	members.easydns.com																										
	<i>genericDDNS</i>	Generic DDNS based on RFC2136.																										
	<i>FortiGuardDDNS</i>	FortiGuard DDNS service.																										
<i>noip.com</i>	dynupdate.no-ip.com																											
server-type	Address type of the DDNS server.	option	-	ipv4																								

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4</td><td>Use IPv4 addressing.</td></tr><tr><td>ipv6</td><td>Use IPv6 addressing.</td></tr></table>				Option	Description	ipv4	Use IPv4 addressing.	ipv6	Use IPv6 addressing.
	Option	Description								
	ipv4	Use IPv4 addressing.								
ipv6	Use IPv6 addressing.									
ddns-server-addr <addr>	Generic DDNS server IP/FQDN list. IP address or FQDN of the server.	string	Maximum length: 256							
ddns-zone	Zone of your domain name (for example, DDNS.com).	string	Maximum length: 64							
ddns-ttl	Time-to-live for DDNS packets.	integer	Minimum value: 60 Maximum value: 86400	300						
ddns-auth	Enable/disable TSIG authentication for your DDNS server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable DDNS authentication.</td></tr><tr><td>tsig</td><td>Enable TSIG authentication based on RFC2845.</td></tr></table>				Option	Description	disable	Disable DDNS authentication.	tsig	Enable TSIG authentication based on RFC2845.
	Option	Description								
	disable	Disable DDNS authentication.								
tsig	Enable TSIG authentication based on RFC2845.									
ddns-keyname	DDNS update key name.	string	Maximum length: 64							
ddns-key	DDNS update key (base 64 encoding).	password_ aes256	Not Specified							
ddns-domain	Your fully qualified domain name. For example, yourname.ddns.com.	string	Maximum length: 64							
ddns-username	DDNS user name.	string	Maximum length: 64							
ddns-sn	DDNS Serial Number.	string	Maximum length: 64							
ddns-password	DDNS password.	password	Not Specified							
use-public-ip	Enable/disable use of public IP address.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable use of public IP address.</td></tr><tr><td>enable</td><td>Enable use of public IP address.</td></tr></table>				Option	Description	disable	Disable use of public IP address.	enable	Enable use of public IP address.
	Option	Description								
	disable	Disable use of public IP address.								
enable	Enable use of public IP address.									
addr-type	Address type of interface address in DDNS update.	option	-	ipv4						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ipv4</i></td><td>Use IPv4 address of the interface.</td></tr><tr><td><i>ipv6</i></td><td>Use IPv6 address of the interface.</td></tr></table>				Option	Description	<i>ipv4</i>	Use IPv4 address of the interface.	<i>ipv6</i>	Use IPv6 address of the interface.
	Option	Description								
	<i>ipv4</i>	Use IPv4 address of the interface.								
<i>ipv6</i>	Use IPv6 address of the interface.									
update-interval	DDNS update interval.	integer	Minimum value: 60 Maximum value: 2592000	0						
clear-text	Enable/disable use of clear text connections.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use of clear text connections.</td></tr><tr><td><i>enable</i></td><td>Enable use of clear text connections.</td></tr></table>				Option	Description	<i>disable</i>	Disable use of clear text connections.	<i>enable</i>	Enable use of clear text connections.
	Option	Description								
	<i>disable</i>	Disable use of clear text connections.								
<i>enable</i>	Enable use of clear text connections.									
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory						
bound-ip	Bound IP address.	string	Maximum length: 46							
monitor-interface	Monitored interface.	string	Maximum length: 79							
<interface-name>	Interface name.									

config system device-upgrade

Independent upgrades for managed devices.

```

config system device-upgrade
    Description: Independent upgrades for managed devices.
    edit <serial>
        set timing [immediate|scheduled]
        set maximum-minutes {integer}
        set time {user}
        set setup-time {user}
        set upgrade-path {user}
        set device-type [fortiswitch|fortiap|...]
        set status [disabled|initialized|...]
        set failure-reason [none|internal|...]
    next
end

```

config system device-upgrade

Parameter	Description	Type	Size	Default														
serial	Serial number of the node to include.	string	Maximum length: 79															
timing	Run immediately or at a scheduled time.	option	-	immediate														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>immediate</i></td><td>Begin the upgrade immediately.</td></tr><tr><td><i>scheduled</i></td><td>Begin the upgrade at a configured time.</td></tr></table>				Option	Description	<i>immediate</i>	Begin the upgrade immediately.	<i>scheduled</i>	Begin the upgrade at a configured time.								
Option	Description																	
<i>immediate</i>	Begin the upgrade immediately.																	
<i>scheduled</i>	Begin the upgrade at a configured time.																	
maximum-minutes	Maximum number of minutes to allow for immediate upgrade preparation.	integer	Minimum value: 5 Maximum value: 10080	15														
time	Scheduled upgrade execution time in UTC (hh:mm yyyy/mm/dd UTC).	user	Not Specified															
setup-time	Upgrade preparation start time in UTC (hh:mm yyyy/mm/dd UTC).	user	Not Specified															
upgrade-path	Fortinet OS image versions to upgrade through in major-minor-patch format, such as 7-0-4.	user	Not Specified															
device-type	Fortinet device type.	option	-	fortiswitch														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortiswitch</i></td><td>This device is a FortiSwitch.</td></tr><tr><td><i>fortiap</i></td><td>This device is a FortiAP.</td></tr><tr><td><i>fortiextender</i></td><td>This device is a FortiExtender.</td></tr></table>				Option	Description	<i>fortiswitch</i>	This device is a FortiSwitch.	<i>fortiap</i>	This device is a FortiAP.	<i>fortiextender</i>	This device is a FortiExtender.						
Option	Description																	
<i>fortiswitch</i>	This device is a FortiSwitch.																	
<i>fortiap</i>	This device is a FortiAP.																	
<i>fortiextender</i>	This device is a FortiExtender.																	
status	Current status of the upgrade.	option	-	disabled														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disabled</i></td><td>No federated upgrade has been configured.</td></tr><tr><td><i>initialized</i></td><td>The upgrade has been configured.</td></tr><tr><td><i>downloading</i></td><td>The image is downloading in preparation for the upgrade.</td></tr><tr><td><i>device-disconnected</i></td><td>The image downloads are complete, but one or more devices have disconnected.</td></tr><tr><td><i>ready</i></td><td>The image download finished and the upgrade is pending.</td></tr><tr><td><i>coordinating</i></td><td>The upgrade is coordinating with other running upgrades.</td></tr></table>				Option	Description	<i>disabled</i>	No federated upgrade has been configured.	<i>initialized</i>	The upgrade has been configured.	<i>downloading</i>	The image is downloading in preparation for the upgrade.	<i>device-disconnected</i>	The image downloads are complete, but one or more devices have disconnected.	<i>ready</i>	The image download finished and the upgrade is pending.	<i>coordinating</i>	The upgrade is coordinating with other running upgrades.
Option	Description																	
<i>disabled</i>	No federated upgrade has been configured.																	
<i>initialized</i>	The upgrade has been configured.																	
<i>downloading</i>	The image is downloading in preparation for the upgrade.																	
<i>device-disconnected</i>	The image downloads are complete, but one or more devices have disconnected.																	
<i>ready</i>	The image download finished and the upgrade is pending.																	
<i>coordinating</i>	The upgrade is coordinating with other running upgrades.																	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>staging</i>	The upgrade is confirmed and images are being staged.		
	<i>final-check</i>	The upgrade is ready and final checks are in progress.		
	<i>upgrade-devices</i>	The upgrade is ready and devices are being rebooted.		
	<i>cancelled</i>	The upgrade was cancelled due to the tree not being ready.		
	<i>confirmed</i>	The upgrade was confirmed and reboots are running.		
	<i>done</i>	The upgrade completed successfully.		
	<i>failed</i>	The upgrade failed due to a local issue.		
failure-reason	Upgrade failure reason.	option	-	none
	Option	Description		
	<i>none</i>	No failure.		
	<i>internal</i>	An internal error occurred.		
	<i>timeout</i>	The upgrade timed out.		
	<i>device-type-unsupported</i>	The device type was not supported by the FortiGate.		
	<i>download-failed</i>	The image could not be downloaded.		
	<i>device-missing</i>	The device was disconnected from the FortiGate.		
	<i>version-unavailable</i>	An image matching the device and version could not be found.		
	<i>staging-failed</i>	The image could not be pushed to the device.		
	<i>reboot-failed</i>	The device could not be rebooted.		
	<i>device-not-reconnected</i>	The device did not reconnect after rebooting.		
	<i>node-not-ready</i>	A device in the Security Fabric tree was not ready.		
	<i>no-final-confirmation</i>	The coordinating FortiGate did not confirm the upgrade.		
	<i>no-confirmation-query</i>	A downstream FortiGate did not initiate final confirmation.		
	<i>config-error-log-nonempty</i>	Configuration errors encountered during the upgrade.		
<i>node-failed</i>	A device in the Security Fabric tree failed.			

config system dhcp6 server

Configure DHCPv6 servers.

```
config system dhcp6 server
  Description: Configure DHCPv6 servers.
  edit <id>
    set status [disable|enable]
    set rapid-commit [disable|enable]
    set lease-time {integer}
    set dns-service [delegated|default|...]
    set dns-search-list [delegated|specify]
    set dns-server1 {ipv6-address}
    set dns-server2 {ipv6-address}
    set dns-server3 {ipv6-address}
    set dns-server4 {ipv6-address}
    set domain {string}
    set subnet {ipv6-prefix}
    set interface {string}
    set option1 {user}
    set option2 {user}
    set option3 {user}
    set upstream-interface {string}
    set delegated-prefix-iaid {integer}
    set ip-mode [range|delegated]
    set prefix-mode [dhcp6|ra]
    config prefix-range
      Description: DHCP prefix configuration.
      edit <id>
        set start-prefix {ipv6-address}
        set end-prefix {ipv6-address}
        set prefix-length {integer}
      next
    end
    config ip-range
      Description: DHCP IP range configuration.
      edit <id>
        set start-ip {ipv6-address}
        set end-ip {ipv6-address}
      next
    end
  next
end
```

config system dhcp6 server

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Enable/disable this DHCPv6 configuration.	option	-	enable
	Option	Description		
	disable	Enable this DHCPv6 server configuration.		
	enable	Disable this DHCPv6 server configuration.		
rapid-commit	Enable/disable allow/disallow rapid commit.	option	-	disable
	Option	Description		
	disable	Do not allow rapid commit.		
	enable	Allow rapid commit.		
lease-time	Lease time in seconds, 0 means unlimited.	integer	Minimum value: 300 Maximum value: 8640000	604800
dns-service	Options for assigning DNS servers to DHCPv6 clients.	option	-	specify
	Option	Description		
	delegated	Delegated DNS settings.		
	default	Clients are assigned the FortiProxy's configured DNS servers.		
	specify	Specify up to 3 DNS servers in the DHCPv6 server configuration.		
dns-search-list	DNS search list options.	option	-	specify
	Option	Description		
	delegated	Delegated the DNS search list.		
	specify	Specify the DNS search list.		
dns-server1	DNS server 1.	ipv6-address	Not Specified	::

Parameter	Description	Type	Size	Default						
dns-server2	DNS server 2.	ipv6-address	Not Specified	::						
dns-server3	DNS server 3.	ipv6-address	Not Specified	::						
dns-server4	DNS server 4.	ipv6-address	Not Specified	::						
domain	Domain name suffix for the IP addresses that the DHCP server assigns to clients.	string	Maximum length: 35							
subnet	Subnet or subnet-id if the IP mode is delegated.	ipv6-prefix	Not Specified	::/0						
interface	DHCP server can assign IP configurations to clients connected to this interface.	string	Maximum length: 15							
option1	Option 1.	user	Not Specified							
option2	Option 2.	user	Not Specified							
option3	Option 3.	user	Not Specified							
upstream-interface	Interface name from where delegated information is provided.	string	Maximum length: 15							
delegated-prefix-iaid	IAID of obtained delegated-prefix from the upstream interface.	integer	Minimum value: 0 Maximum value: 4294967295	0						
ip-mode	Method used to assign client IP.	option	-	range						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>range</td><td>Use range defined by start IP/end IP to assign client IP.</td></tr><tr><td>delegated</td><td>Use delegated prefix method to assign client IP.</td></tr></table>				Option	Description	range	Use range defined by start IP/end IP to assign client IP.	delegated	Use delegated prefix method to assign client IP.
Option	Description									
range	Use range defined by start IP/end IP to assign client IP.									
delegated	Use delegated prefix method to assign client IP.									
prefix-mode	Assigning a prefix from a DHCPv6 client or RA.	option	-	dhcp6						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>dhcp6</td><td>Use delegated prefix from a DHCPv6 client.</td></tr><tr><td>ra</td><td>Use prefix from RA.</td></tr></table>				Option	Description	dhcp6	Use delegated prefix from a DHCPv6 client.	ra	Use prefix from RA.
Option	Description									
dhcp6	Use delegated prefix from a DHCPv6 client.									
ra	Use prefix from RA.									

config prefix-range

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-prefix	Start of prefix range.	ipv6-address	Not Specified	::
end-prefix	End of prefix range.	ipv6-address	Not Specified	::
prefix-length	Prefix length.	integer	Minimum value: 1 Maximum value: 128	0

config ip-range

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-ip	Start of IP range.	ipv6-address	Not Specified	::
end-ip	End of IP range.	ipv6-address	Not Specified	::

config system dhcp server

Configure DHCP servers.

```
config system dhcp server
  Description: Configure DHCP servers.
  edit <id>
    set status [disable|enable]
    set lease-time {integer}
    set mac-acl-default-action [assign|block]
    set forticlient-on-net-status [disable|enable]
    set dns-service [local|default|...]
    set dns-server1 {ipv4-address}
```

```
set dns-server2 {ipv4-address}
set dns-server3 {ipv4-address}
set dns-server4 {ipv4-address}
set wifi-ac-service [specify|local]
set wifi-ac1 {ipv4-address}
set wifi-ac2 {ipv4-address}
set wifi-ac3 {ipv4-address}
set ntp-service [local|default|...]
set ntp-server1 {ipv4-address}
set ntp-server2 {ipv4-address}
set ntp-server3 {ipv4-address}
set domain {string}
set wins-server1 {ipv4-address}
set wins-server2 {ipv4-address}
set default-gateway {ipv4-address}
set next-server {ipv4-address}
set netmask {ipv4-netmask}
set interface {string}
config ip-range
    Description: DHCP IP range configuration.
    edit <id>
        set start-ip {ipv4-address}
        set end-ip {ipv4-address}
        set vci-match [disable|enable]
        set vci-string <vci-string1>, <vci-string2>, ...
        set uci-match [disable|enable]
        set uci-string <uci-string1>, <uci-string2>, ...
        set lease-time {integer}
    next
end
set timezone-option [disable|default|...]
set timezone [01|02|...]
set tftp-server <tftp-server1>, <tftp-server2>, ...
set filename {string}
config options
    Description: DHCP options.
    edit <id>
        set code {integer}
        set type [hex|string|...]
        set value {string}
        set ip {user}
        set vci-match [disable|enable]
        set vci-string <vci-string1>, <vci-string2>, ...
        set uci-match [disable|enable]
        set uci-string <uci-string1>, <uci-string2>, ...
    next
end
set server-type [regular|ipsec]
set ip-mode [range|usrgrp]
set conflicted-ip-timeout {integer}
set ipsec-lease-hold {integer}
set auto-configuration [disable|enable]
set dhcp-settings-from-fortiipam [disable|enable]
set auto-managed-status [disable|enable]
set ddns-update [disable|enable]
set ddns-update-override [disable|enable]
```

```

set ddns-server-ip {ipv4-address}
set ddns-zone {string}
set ddns-auth [disable|tsig]
set ddns-keyname {string}
set ddns-key {password_aes256}
set ddns-ttl {integer}
set vci-match [disable|enable]
set vci-string <vci-string1>, <vci-string2>, ...
config exclude-range
    Description: Exclude one or more ranges of IP addresses from being assigned to
clients.
    edit <id>
        set start-ip {ipv4-address}
        set end-ip {ipv4-address}
        set vci-match [disable|enable]
        set vci-string <vci-string1>, <vci-string2>, ...
        set uci-match [disable|enable]
        set uci-string <uci-string1>, <uci-string2>, ...
        set lease-time {integer}
    next
end
config reserved-address
    Description: Options for the DHCP server to assign IP settings to specific MAC
addresses.
    edit <id>
        set type [mac|option82]
        set ip {ipv4-address}
        set mac {mac-address}
        set action [assign|block|...]
        set circuit-id-type [hex|string]
        set circuit-id {string}
        set remote-id-type [hex|string]
        set remote-id {string}
        set description {var-string}
    next
end
next
end

```

config system dhcp server

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Enable/disable this DHCP configuration.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Do not use this DHCP server configuration.		
	<i>enable</i>	Use this DHCP server configuration.		
lease-time	Lease time in seconds, 0 means unlimited.	integer	Minimum value: 300 Maximum value: 8640000	604800
mac-acl-default-action	MAC access control default action (allow or block assigning IP settings).	option	-	assign
	Option	Description		
	<i>assign</i>	Allow the DHCP server to assign IP settings to clients on the MAC access control list.		
	<i>block</i>	Block the DHCP server from assigning IP settings to clients on the MAC access control list.		
forticlient-on-net-status	Enable/disable FortiClient-On-Net service for this DHCP server.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable FortiClient On-Net Status.		
	<i>enable</i>	Enable FortiClient On-Net Status.		
dns-service	Options for assigning DNS servers to DHCP clients.	option	-	specify
	Option	Description		
	<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's DNS server IP address.		
	<i>default</i>	Clients are assigned the FortiProxy's configured DNS servers.		
	<i>specify</i>	Specify up to 3 DNS servers in the DHCP server configuration.		
dns-server1	DNS server 1.	ipv4-address	Not Specified	0.0.0.0
dns-server2	DNS server 2.	ipv4-address	Not Specified	0.0.0.0
dns-server3	DNS server 3.	ipv4-address	Not Specified	0.0.0.0
dns-server4	DNS server 4.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default								
wifi-ac-service	Options for assigning WiFi access controllers to DHCP clients.	option	-	specify								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>specify</i></td><td>Specify up to 3 WiFi Access Controllers in the DHCP server configuration.</td></tr><tr><td><i>local</i></td><td>IP address of the interface the DHCP server is added to becomes the client's WiFi Access Controller IP address.</td></tr></table>	Option	Description	<i>specify</i>	Specify up to 3 WiFi Access Controllers in the DHCP server configuration.	<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's WiFi Access Controller IP address.					
Option	Description											
<i>specify</i>	Specify up to 3 WiFi Access Controllers in the DHCP server configuration.											
<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's WiFi Access Controller IP address.											
wifi-ac1	WiFi Access Controller 1 IP address (DHCP option 138, RFC 5417).	ipv4-address	Not Specified	0.0.0.0								
wifi-ac2	WiFi Access Controller 2 IP address (DHCP option 138, RFC 5417).	ipv4-address	Not Specified	0.0.0.0								
wifi-ac3	WiFi Access Controller 3 IP address (DHCP option 138, RFC 5417).	ipv4-address	Not Specified	0.0.0.0								
ntp-service	Options for assigning Network Time Protocol (NTP) servers to DHCP clients.	option	-	specify								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>local</i></td><td>IP address of the interface the DHCP server is added to becomes the client's NTP server IP address.</td></tr><tr><td><i>default</i></td><td>Clients are assigned the FortiProxy's configured NTP servers.</td></tr><tr><td><i>specify</i></td><td>Specify up to 3 NTP servers in the DHCP server configuration.</td></tr></table>	Option	Description	<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's NTP server IP address.	<i>default</i>	Clients are assigned the FortiProxy's configured NTP servers.	<i>specify</i>	Specify up to 3 NTP servers in the DHCP server configuration.			
Option	Description											
<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's NTP server IP address.											
<i>default</i>	Clients are assigned the FortiProxy's configured NTP servers.											
<i>specify</i>	Specify up to 3 NTP servers in the DHCP server configuration.											
ntp-server1	NTP server 1.	ipv4-address	Not Specified	0.0.0.0								
ntp-server2	NTP server 2.	ipv4-address	Not Specified	0.0.0.0								
ntp-server3	NTP server 3.	ipv4-address	Not Specified	0.0.0.0								
domain	Domain name suffix for the IP addresses that the DHCP server assigns to clients.	string	Maximum length: 35									
wins-server1	WINS server 1.	ipv4-address	Not Specified	0.0.0.0								
wins-server2	WINS server 2.	ipv4-address	Not Specified	0.0.0.0								
default-gateway	Default gateway IP address assigned by the DHCP server.	ipv4-address	Not Specified	0.0.0.0								
next-server	IP address of a server (for example, a TFTP sever) that DHCP clients can download a boot file from.	ipv4-address	Not Specified	0.0.0.0								
netmask	Netmask assigned by the DHCP server.	ipv4-netmask	Not Specified	0.0.0.0								
interface	DHCP server can assign IP configurations to clients connected to this interface.	string	Maximum length: 15									

Parameter	Description	Type	Size	Default
timezone-option	Options for the DHCP server to set the client's time zone.	option	-	disable
	Option	Description		
	<i>disable</i>	Do not set the client's time zone.		
	<i>default</i>	Clients are assigned the FortiProxy's configured time zone.		
	<i>specify</i>	Specify the time zone to be assigned to DHCP clients.		
timezone	Select the time zone to be assigned to DHCP clients.	option	-	00
	Option	Description		
	01	(GMT-11:00) Midway Island, Samoa		
	02	(GMT-10:00) Hawaii		
	03	(GMT-9:00) Alaska		
	04	(GMT-8:00) Pacific Time (US & Canada)		
	05	(GMT-7:00) Arizona		
	81	(GMT-7:00) Baja California Sur, Chihuahua		
	06	(GMT-7:00) Mountain Time (US & Canada)		
	07	(GMT-6:00) Central America		
	08	(GMT-6:00) Central Time (US & Canada)		
	09	(GMT-6:00) Mexico City		
	10	(GMT-6:00) Saskatchewan		
	11	(GMT-5:00) Bogota, Lima, Quito		
	12	(GMT-5:00) Eastern Time (US & Canada)		
	13	(GMT-5:00) Indiana (East)		
	74	(GMT-4:00) Caracas		
	14	(GMT-4:00) Atlantic Time (Canada)		
	77	(GMT-4:00) Georgetown		
	15	(GMT-4:00) La Paz		
	87	(GMT-4:00) Paraguay		
	16	(GMT-3:00) Santiago		
	17	(GMT-3:30) Newfoundland		

Parameter	Description	Type	Size	Default
	Option	Description		
	18	(GMT-3:00) Brasilia		
	19	(GMT-3:00) Buenos Aires		
	20	(GMT-3:00) Nuuk (Greenland)		
	75	(GMT-3:00) Uruguay		
	21	(GMT-2:00) Mid-Atlantic		
	22	(GMT-1:00) Azores		
	23	(GMT-1:00) Cape Verde Is.		
	24	(GMT) Monrovia		
	80	(GMT) Greenwich Mean Time		
	79	(GMT) Casablanca		
	25	(GMT) Dublin, Edinburgh, Lisbon, London, Canary Is.		
	26	(GMT+1:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna		
	27	(GMT+1:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague		
	28	(GMT+1:00) Brussels, Copenhagen, Madrid, Paris		
	78	(GMT+1:00) Namibia		
	29	(GMT+1:00) Sarajevo, Skopje, Warsaw, Zagreb		
	30	(GMT+1:00) West Central Africa		
	31	(GMT+2:00) Kyiv, Athens, Sofia, Vilnius		
	32	(GMT+2:00) Bucharest		
	33	(GMT+2:00) Cairo		
	34	(GMT+2:00) Harare, Pretoria		
	35	(GMT+2:00) Helsinki, Riga, Tallinn		
	36	(GMT+2:00) Jerusalem		
	37	(GMT+3:00) Baghdad		
	38	(GMT+3:00) Kuwait, Riyadh		
	83	(GMT+3:00) Moscow		
	84	(GMT+3:00) Minsk		
	40	(GMT+3:00) Nairobi		
	85	(GMT+3:00) Istanbul		

Parameter	Description	Type	Size	Default
	Option	Description		
	39	(GMT+3:00) St. Petersburg, Volgograd		
	41	(GMT+3:30) Tehran		
	42	(GMT+4:00) Abu Dhabi, Muscat		
	43	(GMT+4:00) Baku		
	44	(GMT+4:30) Kabul		
	45	(GMT+5:00) Ekaterinburg		
	46	(GMT+5:00) Islamabad, Karachi, Tashkent		
	47	(GMT+5:30) Kolkata, Chennai, Mumbai, New Delhi		
	51	(GMT+5:30) Sri Jayawardenepara		
	48	(GMT+5:45) Kathmandu		
	49	(GMT+5:00) Almaty, Astana		
	50	(GMT+6:00) Dhaka		
	52	(GMT+6:30) Rangoon		
	53	(GMT+7:00) Bangkok, Hanoi, Jakarta, Novosibirsk		
	54	(GMT+7:00) Krasnoyarsk		
	55	(GMT+8:00) Beijing, ChongQing, HongKong, Urumqi, Irkutsk		
	56	(GMT+8:00) Ulaan Bataar		
	57	(GMT+8:00) Kuala Lumpur, Singapore		
	58	(GMT+8:00) Perth		
	59	(GMT+8:00) Taipei		
	60	(GMT+9:00) Osaka, Sapporo, Tokyo, Seoul		
	61	(GMT+9:00) Yakutsk		
	62	(GMT+9:30) Adelaide		
	63	(GMT+9:30) Darwin		
	64	(GMT+10:00) Brisbane		
	65	(GMT+10:00) Canberra, Melbourne, Sydney		
	66	(GMT+10:00) Guam, Port Moresby		
	67	(GMT+10:00) Hobart		
	68	(GMT+10:00) Vladivostok		

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>69</td><td>(GMT+10:00) Magadan</td></tr><tr><td>70</td><td>(GMT+11:00) Solomon Is., New Caledonia</td></tr><tr><td>71</td><td>(GMT+12:00) Auckland, Wellington</td></tr><tr><td>72</td><td>(GMT+12:00) Fiji, Kamchatka, Marshall Is.</td></tr><tr><td>00</td><td>(GMT+12:00) Eniwetok, Kwajalein</td></tr><tr><td>82</td><td>(GMT+12:45) Chatham Islands</td></tr><tr><td>73</td><td>(GMT+13:00) Nuku'alofa</td></tr><tr><td>86</td><td>(GMT+13:00) Samoa</td></tr><tr><td>76</td><td>(GMT+14:00) Kiritimati</td></tr></table>	Option	Description	69	(GMT+10:00) Magadan	70	(GMT+11:00) Solomon Is., New Caledonia	71	(GMT+12:00) Auckland, Wellington	72	(GMT+12:00) Fiji, Kamchatka, Marshall Is.	00	(GMT+12:00) Eniwetok, Kwajalein	82	(GMT+12:45) Chatham Islands	73	(GMT+13:00) Nuku'alofa	86	(GMT+13:00) Samoa	76	(GMT+14:00) Kiritimati			
	Option	Description																						
	69	(GMT+10:00) Magadan																						
	70	(GMT+11:00) Solomon Is., New Caledonia																						
	71	(GMT+12:00) Auckland, Wellington																						
	72	(GMT+12:00) Fiji, Kamchatka, Marshall Is.																						
	00	(GMT+12:00) Eniwetok, Kwajalein																						
	82	(GMT+12:45) Chatham Islands																						
	73	(GMT+13:00) Nuku'alofa																						
	86	(GMT+13:00) Samoa																						
76	(GMT+14:00) Kiritimati																							
tftp-server <tftp-server>	One or more hostnames or IP addresses of the TFTP servers in quotes separated by spaces. TFTP server.	string	Maximum length: 63																					
filename	Name of the boot file on the TFTP server.	string	Maximum length: 127																					
server-type	DHCP server can be a normal DHCP server or an IPsec DHCP server.	option	-	regular																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>regular</td><td>Regular DHCP service.</td></tr><tr><td>ipsec</td><td>DHCP over IPsec service.</td></tr></table>	Option	Description	regular	Regular DHCP service.	ipsec	DHCP over IPsec service.																	
	Option	Description																						
	regular	Regular DHCP service.																						
ipsec	DHCP over IPsec service.																							
ip-mode	Method used to assign client IP.	option	-	range																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>range</td><td>Use range defined by start-ip/end-ip to assign client IP.</td></tr><tr><td>usrgrp</td><td>Use user-group defined method to assign client IP.</td></tr></table>	Option	Description	range	Use range defined by start-ip/end-ip to assign client IP.	usrgrp	Use user-group defined method to assign client IP.																	
	Option	Description																						
	range	Use range defined by start-ip/end-ip to assign client IP.																						
usrgrp	Use user-group defined method to assign client IP.																							
conflicted-ip-timeout	Time in seconds to wait after a conflicted IP address is removed from the DHCP range before it can be reused.	integer	Minimum value: 60 Maximum value: 8640000	1800																				

Parameter	Description	Type	Size	Default						
ipsec-lease-hold	DHCP over IPsec leases expire this many seconds after tunnel down (0 to disable forced-expiry).	integer	Minimum value: 0 Maximum value: 8640000	60						
auto-configuration	Enable/disable auto configuration.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable auto configuration.</td></tr><tr><td>enable</td><td>Enable auto configuration.</td></tr></table>	Option	Description	disable	Disable auto configuration.	enable	Enable auto configuration.			
Option	Description									
disable	Disable auto configuration.									
enable	Enable auto configuration.									
dhcp-settings-from-fortiipam	Enable/disable populating of DHCP server settings from FortiIPAM.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable populating of DHCP server settings from FortiIPAM.</td></tr><tr><td>enable</td><td>Enable populating of DHCP server settings from FortiIPAM.</td></tr></table>	Option	Description	disable	Disable populating of DHCP server settings from FortiIPAM.	enable	Enable populating of DHCP server settings from FortiIPAM.			
Option	Description									
disable	Disable populating of DHCP server settings from FortiIPAM.									
enable	Enable populating of DHCP server settings from FortiIPAM.									
auto-managed-status	Enable/disable use of this DHCP server once this interface has been assigned an IP address from FortiIPAM.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable use of this DHCP server once this interface has been assigned an IP address from FortiIPAM.</td></tr><tr><td>enable</td><td>Enable use of this DHCP server once this interface has been assigned an IP address from FortiIPAM.</td></tr></table>	Option	Description	disable	Disable use of this DHCP server once this interface has been assigned an IP address from FortiIPAM.	enable	Enable use of this DHCP server once this interface has been assigned an IP address from FortiIPAM.			
Option	Description									
disable	Disable use of this DHCP server once this interface has been assigned an IP address from FortiIPAM.									
enable	Enable use of this DHCP server once this interface has been assigned an IP address from FortiIPAM.									
ddns-update	Enable/disable DDNS update for DHCP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable DDNS update for DHCP.</td></tr><tr><td>enable</td><td>Enable DDNS update for DHCP.</td></tr></table>	Option	Description	disable	Disable DDNS update for DHCP.	enable	Enable DDNS update for DHCP.			
Option	Description									
disable	Disable DDNS update for DHCP.									
enable	Enable DDNS update for DHCP.									
ddns-update-override	Enable/disable DDNS update override for DHCP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable DDNS update override for DHCP.</td></tr><tr><td>enable</td><td>Enable DDNS update override for DHCP.</td></tr></table>	Option	Description	disable	Disable DDNS update override for DHCP.	enable	Enable DDNS update override for DHCP.			
Option	Description									
disable	Disable DDNS update override for DHCP.									
enable	Enable DDNS update override for DHCP.									

Parameter	Description	Type	Size	Default						
ddns-server-ip	DDNS server IP.	ipv4-address	Not Specified	0.0.0.0						
ddns-zone	Zone of your domain name (ex. DDNS.com).	string	Maximum length: 64							
ddns-auth	DDNS authentication mode.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable DDNS authentication.</td></tr><tr><td><i>tsig</i></td><td>TSIG based on RFC2845.</td></tr></table>	Option	Description	<i>disable</i>	Disable DDNS authentication.	<i>tsig</i>	TSIG based on RFC2845.			
Option	Description									
<i>disable</i>	Disable DDNS authentication.									
<i>tsig</i>	TSIG based on RFC2845.									
ddns-keyname	DDNS update key name.	string	Maximum length: 64							
ddns-key	DDNS update key (base 64 encoding).	password_aes256	Not Specified							
ddns-ttl	TTL.	integer	Minimum value: 60 Maximum value: 86400	300						
vci-match	Enable/disable vendor class identifier (VCI) matching. When enabled only DHCP requests with a matching VCI are served.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable VCI matching.</td></tr><tr><td><i>enable</i></td><td>Enable VCI matching.</td></tr></table>	Option	Description	<i>disable</i>	Disable VCI matching.	<i>enable</i>	Enable VCI matching.			
Option	Description									
<i>disable</i>	Disable VCI matching.									
<i>enable</i>	Enable VCI matching.									
vci-string <vci-string>	One or more VCI strings in quotes separated by spaces. VCI strings.	string	Maximum length: 255							

config ip-range

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-ip	Start of IP range.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default						
end-ip	End of IP range.	ipv4-address	Not Specified	0.0.0.0						
vci-match	Enable/disable vendor class identifier (VCI) matching. When enabled only DHCP requests with a matching VCI are served with this range.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable VCI matching.</td></tr><tr><td>enable</td><td>Enable VCI matching.</td></tr></table>				Option	Description	disable	Disable VCI matching.	enable	Enable VCI matching.
Option	Description									
disable	Disable VCI matching.									
enable	Enable VCI matching.									
vci-string <vci-string>	One or more VCI strings in quotes separated by spaces. VCI strings.	string	Maximum length: 255							
uci-match	Enable/disable user class identifier (UCI) matching. When enabled only DHCP requests with a matching UCI are served with this range.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable UCI matching.</td></tr><tr><td>enable</td><td>Enable UCI matching.</td></tr></table>				Option	Description	disable	Disable UCI matching.	enable	Enable UCI matching.
Option	Description									
disable	Disable UCI matching.									
enable	Enable UCI matching.									
uci-string <uci-string>	One or more UCI strings in quotes separated by spaces. UCI strings.	string	Maximum length: 255							
lease-time	Lease time in seconds, 0 means default lease time.	integer	Minimum value: 300 Maximum value: 8640000	0						

config options

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default										
code	DHCP option code.	integer	Minimum value: 0 Maximum value: 255	0										
type	DHCP option type.	option	-	hex										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>hex</td><td>DHCP option in hex.</td></tr><tr><td>string</td><td>DHCP option in string.</td></tr><tr><td>ip</td><td>DHCP option in IP.</td></tr><tr><td>fqdn</td><td>DHCP option in domain search option format.</td></tr></table>				Option	Description	hex	DHCP option in hex.	string	DHCP option in string.	ip	DHCP option in IP.	fqdn	DHCP option in domain search option format.
Option	Description													
hex	DHCP option in hex.													
string	DHCP option in string.													
ip	DHCP option in IP.													
fqdn	DHCP option in domain search option format.													
value	DHCP option value.	string	Maximum length: 312											
ip	DHCP option IPs.	user	Not Specified											
vci-match	Enable/disable vendor class identifier (VCI) matching. When enabled only DHCP requests with a matching VCI are served with this option.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable VCI matching.</td></tr><tr><td>enable</td><td>Enable VCI matching.</td></tr></table>				Option	Description	disable	Disable VCI matching.	enable	Enable VCI matching.				
Option	Description													
disable	Disable VCI matching.													
enable	Enable VCI matching.													
vci-string <vci-string>	One or more VCI strings in quotes separated by spaces. VCI strings.	string	Maximum length: 255											
uci-match	Enable/disable user class identifier (UCI) matching. When enabled only DHCP requests with a matching UCI are served with this option.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable UCI matching.</td></tr><tr><td>enable</td><td>Enable UCI matching.</td></tr></table>				Option	Description	disable	Disable UCI matching.	enable	Enable UCI matching.				
Option	Description													
disable	Disable UCI matching.													
enable	Enable UCI matching.													
uci-string <uci-string>	One or more UCI strings in quotes separated by spaces. UCI strings.	string	Maximum length: 255											

config exclude-range

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
start-ip	Start of IP range.	ipv4-address	Not Specified	0.0.0.0						
end-ip	End of IP range.	ipv4-address	Not Specified	0.0.0.0						
vci-match	Enable/disable vendor class identifier (VCI) matching. When enabled only DHCP requests with a matching VCI are served with this range.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable VCI matching.</td></tr><tr><td><i>enable</i></td><td>Enable VCI matching.</td></tr></table>				Option	Description	<i>disable</i>	Disable VCI matching.	<i>enable</i>	Enable VCI matching.
	Option	Description								
	<i>disable</i>	Disable VCI matching.								
<i>enable</i>	Enable VCI matching.									
vci-string <vci-string>	One or more VCI strings in quotes separated by spaces. VCI strings.	string	Maximum length: 255							
uci-match	Enable/disable user class identifier (UCI) matching. When enabled only DHCP requests with a matching UCI are served with this range.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable UCI matching.</td></tr><tr><td><i>enable</i></td><td>Enable UCI matching.</td></tr></table>				Option	Description	<i>disable</i>	Disable UCI matching.	<i>enable</i>	Enable UCI matching.
	Option	Description								
	<i>disable</i>	Disable UCI matching.								
<i>enable</i>	Enable UCI matching.									
uci-string <uci-string>	One or more UCI strings in quotes separated by spaces. UCI strings.	string	Maximum length: 255							
lease-time	Lease time in seconds, 0 means default lease time.	integer	Minimum value: 300 Maximum value: 8640000	0						

config reserved-address

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
type	DHCP reserved-address type.	option	-	mac
	OptionDescription			
	mac	Match with MAC address.		
	option82	Match with DHCP option 82.		
ip	IP address to be reserved for the MAC address.	ipv4-address	Not Specified	0.0.0.0
mac	MAC address of the client that will get the reserved IP address.	mac-address	Not Specified	00:00:00:00:00:00
action	Options for the DHCP server to configure the client with the reserved MAC address.	option	-	reserved
	OptionDescription			
	assign	Configure the client with this MAC address like any other client.		
	block	Block the DHCP server from assigning IP settings to the client with this MAC address.		
	reserved	Assign the reserved IP address to the client with this MAC address.		
circuit-id-type	DHCP option type.	option	-	string
	OptionDescription			
	hex	DHCP option in hex.		
	string	DHCP option in string.		
circuit-id	Option 82 circuit-ID of the client that will get the reserved IP address.	string	Maximum length: 312	
remote-id-type	DHCP option type.	option	-	string
	OptionDescription			
	hex	DHCP option in hex.		
	string	DHCP option in string.		

Parameter	Description	Type	Size	Default
remote-id	Option 82 remote-ID of the client that will get the reserved IP address.	string	Maximum length: 312	
description	Description.	var-string	Maximum length: 255	

config system dns-database

Configure DNS databases.

```

config system dns-database
    Description: Configure DNS databases.
    edit <name>
        set status [enable|disable]
        set domain {string}
        set allow-transfer {user}
        set type [primary|secondary]
        set view [shadow|public|...]
        set ip-primary {ipv4-address-any}
        set primary-name {string}
        set contact {string}
        set ttl {integer}
        set authoritative [enable|disable]
        set forwarder {user}
        set source-ip {ipv4-address}
        set rr-max {integer}
        config dns-entry
            Description: DNS entry.
            edit <id>
                set status [enable|disable]
                set type [A|NS|...]
                set ttl {integer}
                set preference {integer}
                set ip {ipv4-address-any}
                set ipv6 {ipv6-address}
                set hostname {string}
                set canonical-name {string}
            next
        end
    next
end

```

config system dns-database

Parameter	Description	Type	Size	Default
name	Zone name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default								
status	Enable/disable this DNS zone.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
domain	Domain name.	string	Maximum length: 255									
allow-transfer	DNS zone transfer IP address list.	user	Not Specified									
type	Zone type (primary to manage entries directly, secondary to import entries from other zones).	option	-	primary								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>primary</i></td><td>Primary DNS zone, to manage entries directly.</td></tr><tr><td><i>secondary</i></td><td>Secondary DNS zone, to import entries from other DNS zones.</td></tr></table>				Option	Description	<i>primary</i>	Primary DNS zone, to manage entries directly.	<i>secondary</i>	Secondary DNS zone, to import entries from other DNS zones.		
	Option	Description										
	<i>primary</i>	Primary DNS zone, to manage entries directly.										
<i>secondary</i>	Secondary DNS zone, to import entries from other DNS zones.											
view	Zone view (public to serve public clients, shadow to serve internal clients).	option	-	shadow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>shadow</i></td><td>Shadow DNS zone to serve internal clients.</td></tr><tr><td><i>public</i></td><td>Public DNS zone to serve public clients.</td></tr><tr><td><i>shadow-ztna</i></td><td>implicit DNS zone for ztna dox tunnel.</td></tr></table>				Option	Description	<i>shadow</i>	Shadow DNS zone to serve internal clients.	<i>public</i>	Public DNS zone to serve public clients.	<i>shadow-ztna</i>	implicit DNS zone for ztna dox tunnel.
	Option	Description										
	<i>shadow</i>	Shadow DNS zone to serve internal clients.										
	<i>public</i>	Public DNS zone to serve public clients.										
<i>shadow-ztna</i>	implicit DNS zone for ztna dox tunnel.											
ip-primary	IP address of primary DNS server. Entries in this primary DNS server and imported into the DNS zone.	ipv4-address-any	Not Specified	0.0.0.0								
primary-name	Domain name of the default DNS server for this zone.	string	Maximum length: 255	dns								
contact	Email address of the administrator for this zone. You can specify only the username, such as admin or the full email address, such as admin@test.com When using only a username, the domain of the email will be this zone.	string	Maximum length: 255	host								
tll	Default time-to-live value for the entries of this DNS zone.	integer	Minimum value: 0 Maximum value: 2147483647	86400								
authoritative	Enable/disable authoritative zone.	option	-	enable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable authoritative zone.		
	<i>disable</i>	Disable authoritative zone.		
forwarder	DNS zone forwarder IP address list.	user	Not Specified	
source-ip	Source IP for forwarding to DNS server.	ipv4-address	Not Specified	0.0.0.0
rr-max	Maximum number of resource records.	integer	Minimum value: 10 Maximum value: 65536	16384

config dns-entry

Parameter	Description	Type	Size	Default																
id	DNS entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0																
status	Enable/disable resource record status.	option	-	enable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable resource record status.</td></tr><tr><td><i>disable</i></td><td>Disable resource record status.</td></tr></table>				Option	Description	<i>enable</i>	Enable resource record status.	<i>disable</i>	Disable resource record status.										
	Option	Description																		
	<i>enable</i>	Enable resource record status.																		
<i>disable</i>	Disable resource record status.																			
type	Resource record type.	option	-	A																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>A</i></td><td>Host type.</td></tr><tr><td><i>NS</i></td><td>Name server type.</td></tr><tr><td><i>CNAME</i></td><td>Canonical name type.</td></tr><tr><td><i>MX</i></td><td>Mail exchange type.</td></tr><tr><td><i>AAAA</i></td><td>IPv6 host type.</td></tr><tr><td><i>PTR</i></td><td>Pointer type.</td></tr><tr><td><i>PTR_V6</i></td><td>IPv6 pointer type.</td></tr></table>				Option	Description	<i>A</i>	Host type.	<i>NS</i>	Name server type.	<i>CNAME</i>	Canonical name type.	<i>MX</i>	Mail exchange type.	<i>AAAA</i>	IPv6 host type.	<i>PTR</i>	Pointer type.	<i>PTR_V6</i>	IPv6 pointer type.
	Option	Description																		
	<i>A</i>	Host type.																		
	<i>NS</i>	Name server type.																		
	<i>CNAME</i>	Canonical name type.																		
	<i>MX</i>	Mail exchange type.																		
	<i>AAAA</i>	IPv6 host type.																		
	<i>PTR</i>	Pointer type.																		
<i>PTR_V6</i>	IPv6 pointer type.																			

Parameter	Description	Type	Size	Default
ttl	Time-to-live for this entry.	integer	Minimum value: 0 Maximum value: 2147483647	0
preference	DNS entry preference.	integer	Minimum value: 0 Maximum value: 65535	10
ip	IPv4 address of the host.	ipv4-address-any	Not Specified	0.0.0.0
ipv6	IPv6 address of the host.	ipv6-address	Not Specified	::
hostname	Name of the host.	string	Maximum length: 255	
canonical-name	Canonical name of the host.	string	Maximum length: 255	

config system dns-server

Configure DNS servers.

```
config system dns-server
  Description: Configure DNS servers.
  edit <name>
    set mode [recursive|non-recursive|...]
    set dnsfilter-profile {string}
    set doh [enable|disable]
    set doh3 [enable|disable]
    set doq [enable|disable]
  next
end
```

config system dns-server

Parameter	Description	Type	Size	Default
name	DNS server name.	string	Maximum length: 15	
mode	DNS server mode.	option	-	recursive

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>recursive</i>	Shadow DNS database and forward.		
	<i>non-recursive</i>	Public DNS database only.		
	<i>forward-only</i>	Forward only.		
dnsfilter-profile	DNS filter profile.	string	Maximum length: 35	
doh	Enable/disable DNS over HTTPS/443.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable DNS over HTTPS.		
	<i>disable</i>	Disable DNS over HTTPS.		
doh3	Enable/disable DNS over QUIC/HTTP3/443.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable DNS over HTTP3/QUIC.		
	<i>disable</i>	Disable DNS over HTTP3/QUIC.		
doq	Enable/disable DNS over QUIC/853.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable DNS over QUIC.		
	<i>disable</i>	Disable DNS over QUIC.		

config system dns

Configure DNS.

```
config system dns
    Description: Configure DNS.
    set primary {ipv4-address}
    set secondary {ipv4-address}
    set protocol {option1}, {option2}, ...
    set ssl-certificate {string}
    set server-hostname <hostname1>, <hostname2>, ...
    set domain <domain1>, <domain2>, ...
    set ip6-primary {ipv6-address}
    set ip6-secondary {ipv6-address}
    set timeout {integer}
    set retry {integer}
    set dns-cache-limit {integer}
```

```

set dns-cache-ttl {integer}
set cache-notfound-responses [disable|enable]
set source-ip {ipv4-address}
set interface-select-method [auto|specify]
set interface {string}
set server-select-method [least-rtt|failover]
set alt-primary {ipv4-address}
set alt-secondary {ipv4-address}
set log [disable|error|...]
set fqdn-cache-ttl {integer}
set fqdn-min-refresh {integer}

```

```
end
```

config system dns

Parameter	Description	Type	Size	Default								
primary	Primary DNS server IP address.	ipv4-address	Not Specified	0.0.0.0								
secondary	Secondary DNS server IP address.	ipv4-address	Not Specified	0.0.0.0								
protocol	DNS transport protocols.	option	-	cleartext								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>cleartext</td><td>DNS over UDP/53, DNS over TCP/53.</td></tr><tr><td>dot</td><td>DNS over TLS/853.</td></tr><tr><td>doh</td><td>DNS over HTTPS/443.</td></tr></table>				Option	Description	cleartext	DNS over UDP/53, DNS over TCP/53.	dot	DNS over TLS/853.	doh	DNS over HTTPS/443.
	Option	Description										
	cleartext	DNS over UDP/53, DNS over TCP/53.										
	dot	DNS over TLS/853.										
doh	DNS over HTTPS/443.											
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory								
server-hostname <hostname>	DNS server host name list. DNS server host name list separated by space (maximum 4 domains).	string	Maximum length: 127									
domain <domain>	Search suffix list for hostname lookup. DNS search domain list separated by space (maximum 8 domains).	string	Maximum length: 127									
ip6-primary	Primary DNS server IPv6 address.	ipv6-address	Not Specified	::								
ip6-secondary	Secondary DNS server IPv6 address.	ipv6-address	Not Specified	::								
timeout	DNS query timeout interval in seconds.	integer	Minimum value: 1 Maximum value: 10	5								

Parameter	Description	Type	Size	Default						
retry	Number of times to retry.	integer	Minimum value: 0 Maximum value: 5	2						
dns-cache-limit	Maximum number of records in the DNS cache.	integer	Minimum value: 0 Maximum value: 4294967295	5000						
dns-cache-ttl	Duration in seconds that the DNS cache retains information.	integer	Minimum value: 60 Maximum value: 86400	1800						
cache-notfound-responses	Enable/disable response from the DNS server when a record is not in cache.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable cache NOTFOUND responses from DNS server.</td></tr><tr><td>enable</td><td>Enable cache NOTFOUND responses from DNS server.</td></tr></table>				Option	Description	disable	Disable cache NOTFOUND responses from DNS server.	enable	Enable cache NOTFOUND responses from DNS server.
Option	Description									
disable	Disable cache NOTFOUND responses from DNS server.									
enable	Enable cache NOTFOUND responses from DNS server.									
source-ip	IP address used by the DNS server as its source IP.	ipv4-address	Not Specified	0.0.0.0						
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	auto	Set outgoing interface automatically.	specify	Set outgoing interface manually.
Option	Description									
auto	Set outgoing interface automatically.									
specify	Set outgoing interface manually.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							
server-select-method	Specify how configured servers are prioritized.	option	-	least-rtt						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>least-rtt</td><td>Select servers based on least round trip time.</td></tr><tr><td>failover</td><td>Select servers based on the order they are configured.</td></tr></table>				Option	Description	least-rtt	Select servers based on least round trip time.	failover	Select servers based on the order they are configured.
Option	Description									
least-rtt	Select servers based on least round trip time.									
failover	Select servers based on the order they are configured.									
alt-primary	Alternate primary DNS server. This is not used as a failover DNS server.	ipv4-address	Not Specified	0.0.0.0						

Parameter	Description	Type	Size	Default								
alt-secondary	Alternate secondary DNS server. This is not used as a failover DNS server.	ipv4-address	Not Specified	0.0.0.0								
log	Local DNS log setting.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>error</i></td><td>Enable local DNS error log.</td></tr><tr><td><i>all</i></td><td>Enable local DNS log.</td></tr></table>				Option	Description	<i>disable</i>	Disable.	<i>error</i>	Enable local DNS error log.	<i>all</i>	Enable local DNS log.
	Option	Description										
	<i>disable</i>	Disable.										
	<i>error</i>	Enable local DNS error log.										
<i>all</i>	Enable local DNS log.											
fqdn-cache-ttl	FQDN cache time to live in seconds.	integer	Minimum value: 0 Maximum value: 86400	0								
fqdn-min-refresh	FQDN cache minimum refresh time in seconds.	integer	Minimum value: 10 Maximum value: 3600	60								

config system dscp-based-priority

Configure DSCP based priority table.

```

config system dscp-based-priority
    Description: Configure DSCP based priority table.
    edit <id>
        set ds {integer}
        set priority [low|medium|...]
    next
end

```

config system dscp-based-priority

Parameter	Description	Type	Size	Default
id	Item ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
ds	DSCP.	integer	Minimum value: 0 Maximum value: 63	0
priority	DSCP based priority level.	option	-	high
	Option	Description		
	low	Low priority.		
	medium	Medium priority.		
	high	High priority.		

config system email-server

Configure the email server used by the FortiProxy various things. For example, for sending email messages to users to support user authentication features.

```
config system email-server
    Description: Configure the email server used by the FortiProxy various things. For
example, for sending email messages to users to support user authentication features.
    set type {option}
    set reply-to {string}
    set server {string}
    set port {integer}
    set source-ip {ipv4-address}
    set source-ip6 {ipv6-address}
    set authenticate [enable|disable]
    set validate-server [enable|disable]
    set username {string}
    set password {password}
    set security [none|starttls|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set interface-select-method [auto|specify]
    set interface {string}
end
```

config system email-server

Parameter	Description	Type	Size	Default
type	Use FortiGuard Message service or custom email server.	option	-	custom

Parameter	Description	Type	Size	Default
	Option Description			
	<i>custom</i>	Use custom email server.		
reply-to	Reply-To email address.	string	Maximum length: 63	
server	SMTP server IP address or hostname.	string	Maximum length: 63	
port	SMTP server port.	integer	Minimum value: 1 Maximum value: 65535	25
source-ip	SMTP server IPv4 source IP.	ipv4-address	Not Specified	0.0.0.0
source-ip6	SMTP server IPv6 source IP.	ipv6-address	Not Specified	::
authenticate	Enable/disable authentication.	option	-	disable
	Option Description			
	<i>enable</i>	Enable authentication.		
	<i>disable</i>	Disable authentication.		
validate-server	Enable/disable validation of server certificate.	option	-	disable
	Option Description			
	<i>enable</i>	Enable validation of server certificate.		
	<i>disable</i>	Disable validation of server certificate.		
username	SMTP server user name for authentication.	string	Maximum length: 63	
password	SMTP server user password for authentication.	password	Not Specified	
security	Connection security used by the email server.	option	-	none
	Option Description			
	<i>none</i>	None.		
	<i>starttls</i>	STARTTLS.		
	<i>smtps</i>	SSL/TLS.		

Parameter	Description	Type	Size	Default												
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.			
	Option	Description														
	default	Follow system global setting.														
	SSLv3	SSLv3.														
	TLSv1	TLSv1.														
	TLSv1-1	TLSv1.1.														
TLSv1-2	TLSv1.2.															
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	specify	Set outgoing interface manually.									
	Option	Description														
	auto	Set outgoing interface automatically.														
specify	Set outgoing interface manually.															
interface	Specify outgoing interface to reach server.	string	Maximum length: 15													

config system external-resource

Configure external resource.

```

config system external-resource
    Description: Configure external resource.
    edit <name>
        set uuid {uuid}
        set status [enable|disable]
        set type [category|address|...]
        set update-method [feed|push]
        set category {integer}
        set username {string}
        set password {password}
        set comments {var-string}
        set resource {string}
        set user-agent {var-string}
        set server-identity-check [none|basic|...]
        set proxy {string}
        set proxy-port {integer}
        set proxy-username {string}
        set proxy-password {password}
        set refresh-rate {integer}
        set source-ip {ipv4-address}
        set interface-select-method [auto|specify]

```

```

        set interface {string}
    next
end

```

config system external-resource

Parameter	Description	Type	Size	Default
name	External resource name.	string	Maximum length: 35	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
status	Enable/disable user resource.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable user resource.		
	<i>disable</i>	Disable user resource.		
type	User resource type.	option	-	category
	Option	Description		
	<i>category</i>	FortiGuard category.		
	<i>address</i>	Firewall IP address.		
	<i>domain</i>	Domain Name.		
	<i>malware</i>	Malware hash.		
	<i>url</i>	URL List.		
	<i>data</i>	Data file.		
update-method	External resource update method.	option	-	feed
	Option	Description		
	<i>feed</i>	FortiGate unit will pull update from the external resource.		
	<i>push</i>	External Resource update is pushed to the FortiGate unit through the FortiGate unit's RESTAPI/CLI.		
category	User resource category.	integer	Minimum value: 192 Maximum value: 221	0

Parameter	Description	Type	Size	Default								
username	HTTP basic authentication user name.	string	Maximum length: 64									
password	HTTP basic authentication password.	password	Not Specified									
comments	Comment.	var-string	Maximum length: 255									
resource	URI of external resource.	string	Maximum length: 511									
user-agent	HTTP User-Agent header.	var-string	Maximum length: 255									
server-identity-check	Certificate verification option.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No certificate verification.</td></tr><tr><td><i>basic</i></td><td>Check server certificate only.</td></tr><tr><td><i>full</i></td><td>Check server certificate and verify the domain matches in the server certificate.</td></tr></table>				Option	Description	<i>none</i>	No certificate verification.	<i>basic</i>	Check server certificate only.	<i>full</i>	Check server certificate and verify the domain matches in the server certificate.
Option	Description											
<i>none</i>	No certificate verification.											
<i>basic</i>	Check server certificate only.											
<i>full</i>	Check server certificate and verify the domain matches in the server certificate.											
proxy	Proxy server host(ip or domain name).	string	Maximum length: 255									
proxy-port	Port number that the proxy server expects to receive HTTP sessions on.	integer	Minimum value: 1 Maximum value: 65535	8080								
proxy-username	HTTP proxy basic authentication user name.	string	Maximum length: 64									
proxy-password	HTTP proxy basic authentication password.	password	Not Specified									
refresh-rate	Time interval to refresh external resource.	integer	Minimum value: 1 Maximum value: 43200	5								
source-ip	Source IPv4 address used to communicate with server.	ipv4-address	Not Specified	0.0.0.0								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config system fabric-vpn

Setup for self orchestrated fabric auto discovery VPN.

```

config system fabric-vpn
  Description: Setup for self orchestrated fabric auto discovery VPN.
  set status [enable|disable]
  set sync-mode [enable|disable]
  set branch-name {string}
  set policy-rule [health-check|manual|...]
  set vpn-role [hub|spoke]
  config overlays
    Description: Local overlay interfaces table.
    edit <name>
      set overlay-tunnel-block {ipv4-classnet-host}
      set remote-gw {ipv4-address-any}
      set interface {string}
      set bgp-neighbor {string}
      set overlay-policy {integer}
      set bgp-network {integer}
      set route-policy {integer}
      set bgp-neighbor-group {string}
      set bgp-neighbor-range {integer}
      set ipsec-phase1 {string}
      set sdwan-member {integer}
    next
  end
  config advertised-subnets
    Description: Local advertised subnets.
    edit <id>
      set prefix {ipv4-classnet}
      set access [inbound|bidirectional]
      set bgp-network {integer}
      set firewall-address {string}
      set policies {integer}
    next
  end
  set loopback-address-block {ipv4-classnet-host}
  set loopback-interface {string}
  set loopback-advertised-subnet {integer}
  set psksecret {password-3}
  set bgp-as {integer}

```

```

set sdwan-zone {string}
set health-checks {string}
end

```

config system fabric-vpn

Parameter	Description	Type	Size	Default
status	Enable/disable Fabric VPN.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Fabric VPN.		
	<i>disable</i>	Disable Fabric VPN.		
sync-mode	Setting synchronised by fabric or manual.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable fabric led configuration synchronisation.		
	<i>disable</i>	Disable fabric led configuration synchronisation.		
branch-name	Branch name.	string	Maximum length: 35	
policy-rule	Policy creation rule.	option	-	health-check
	Option	Description		
	<i>health-check</i>	Create health check policy automatically.		
	<i>manual</i>	All policies will be created manually.		
	<i>auto</i>	Automatically create allow policies.		
vpn-role	Fabric VPN role.	option	-	hub
	Option	Description		
	<i>hub</i>	VPN hub.		
	<i>spoke</i>	VPN spoke.		
loopback-address-block	IPv4 address and subnet mask for hub's loopback address, syntax: X.X.X.X/24.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
loopback-interface	Loopback interface.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default
loopback-advertised-subnet	Loopback advertised subnet reference.	integer	Minimum value: 0 Maximum value: 4294967295	0
psksecret	Pre-shared secret for ADVPN.	password-3	Not Specified	
bgp-as	BGP Router AS number, valid from 1 to 4294967295.	integer	Minimum value: 0 Maximum value: 4294967295	0
sdwan-zone	Reference to created SD-WAN zone.	string	Maximum length: 35	
health-checks	Underlying health checks.	string	Maximum length: 35	

config overlays

Parameter	Description	Type	Size	Default
name	Overlay name.	string	Maximum length: 79	
overlay-tunnel-block	IPv4 address and subnet mask for the overlay tunnel , syntax: X.X.X.X/24.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
remote-gw	IP address of the hub gateway (Set by hub).	ipv4-address-any	Not Specified	0.0.0.0
interface	Underlying interface name.	string	Maximum length: 15	
bgp-neighbor	Underlying BGP neighbor entry.	string	Maximum length: 45	
overlay-policy	The overlay policy to allow ADVPN thru traffic.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
bgp-network	Underlying BGP network.	integer	Minimum value: 0 Maximum value: 4294967295	0
route-policy	Underlying router policy.	integer	Minimum value: 0 Maximum value: 4294967295	0
bgp-neighbor-group	Underlying BGP neighbor group entry.	string	Maximum length: 45	
bgp-neighbor-range	Underlying BGP neighbor range entry.	integer	Minimum value: 0 Maximum value: 4294967295	0
ipsec-phase1	IPsec interface.	string	Maximum length: 35	
sdwan-member	Reference to SD-WAN member entry.	integer	Minimum value: 0 Maximum value: 4294967295	0

config advertised-subnets

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 0 Maximum value: 4294967294	0						
prefix	Network prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0						
access	Access policy direction.	option	-	inbound						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>inbound</i></td><td>Allow inbound traffic to subnet.</td></tr><tr><td><i>bidirectional</i></td><td>Allow inbound and outbound traffic to subnet.</td></tr></table>	Option	Description	<i>inbound</i>	Allow inbound traffic to subnet.	<i>bidirectional</i>	Allow inbound and outbound traffic to subnet.			
Option	Description									
<i>inbound</i>	Allow inbound traffic to subnet.									
<i>bidirectional</i>	Allow inbound and outbound traffic to subnet.									

Parameter	Description	Type	Size	Default
bgp-network	Underlying BGP network.	integer	Minimum value: 0 Maximum value: 4294967295	0
firewall-address	Underlying firewall address.	string	Maximum length: 79	
policies	Underlying policies.	integer	Minimum value: 0 Maximum value: 4294967295	

config system federated-upgrade

Coordinate federated upgrades within the Security Fabric.

```

config system federated-upgrade
    Description: Coordinate federated upgrades within the Security Fabric.
    set status [disabled|initialized|...]
    set source [user|auto-firmware-upgrade]
    set failure-reason [none|internal|...]
    set failure-device {string}
    set upgrade-id {integer}
    set next-path-index {integer}
    set ha-reboot-controller {string}
    config node-list
        Description: Nodes which will be included in the upgrade.
        edit <serial>
            set timing [immediate|scheduled]
            set maximum-minutes {integer}
            set time {user}
            set setup-time {user}
            set upgrade-path {user}
            set device-type [fortiproxy|fortiswitch|...]
            set coordinating-fortiproxy {string}
        next
    end
end

```

config system federated-upgrade

Parameter	Description	Type	Size	Default
status	Current status of the upgrade.	option	-	disabled

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disabled</i></td><td>No federated upgrade has been configured.</td></tr><tr><td><i>initialized</i></td><td>The upgrade has been configured.</td></tr><tr><td><i>downloading</i></td><td>The image is downloading in preparation for the upgrade.</td></tr><tr><td><i>device-disconnected</i></td><td>The image downloads are complete, but one or more devices have disconnected.</td></tr><tr><td><i>ready</i></td><td>The image download finished and the upgrade is pending.</td></tr><tr><td><i>coordinating</i></td><td>The upgrade is coordinating with other running upgrades.</td></tr><tr><td><i>staging</i></td><td>The upgrade is confirmed and images are being staged.</td></tr><tr><td><i>final-check</i></td><td>The upgrade is ready and final checks are in progress.</td></tr><tr><td><i>upgrade-devices</i></td><td>The upgrade is ready and devices are being rebooted.</td></tr><tr><td><i>cancelled</i></td><td>The upgrade was cancelled due to the tree not being ready.</td></tr><tr><td><i>confirmed</i></td><td>The upgrade was confirmed and reboots are running.</td></tr><tr><td><i>done</i></td><td>The upgrade completed successfully.</td></tr><tr><td><i>failed</i></td><td>The upgrade failed due to a local issue.</td></tr></table>	Option	Description	<i>disabled</i>	No federated upgrade has been configured.	<i>initialized</i>	The upgrade has been configured.	<i>downloading</i>	The image is downloading in preparation for the upgrade.	<i>device-disconnected</i>	The image downloads are complete, but one or more devices have disconnected.	<i>ready</i>	The image download finished and the upgrade is pending.	<i>coordinating</i>	The upgrade is coordinating with other running upgrades.	<i>staging</i>	The upgrade is confirmed and images are being staged.	<i>final-check</i>	The upgrade is ready and final checks are in progress.	<i>upgrade-devices</i>	The upgrade is ready and devices are being rebooted.	<i>cancelled</i>	The upgrade was cancelled due to the tree not being ready.	<i>confirmed</i>	The upgrade was confirmed and reboots are running.	<i>done</i>	The upgrade completed successfully.	<i>failed</i>	The upgrade failed due to a local issue.			
	Option	Description																														
	<i>disabled</i>	No federated upgrade has been configured.																														
	<i>initialized</i>	The upgrade has been configured.																														
	<i>downloading</i>	The image is downloading in preparation for the upgrade.																														
	<i>device-disconnected</i>	The image downloads are complete, but one or more devices have disconnected.																														
	<i>ready</i>	The image download finished and the upgrade is pending.																														
	<i>coordinating</i>	The upgrade is coordinating with other running upgrades.																														
	<i>staging</i>	The upgrade is confirmed and images are being staged.																														
	<i>final-check</i>	The upgrade is ready and final checks are in progress.																														
	<i>upgrade-devices</i>	The upgrade is ready and devices are being rebooted.																														
	<i>cancelled</i>	The upgrade was cancelled due to the tree not being ready.																														
	<i>confirmed</i>	The upgrade was confirmed and reboots are running.																														
<i>done</i>	The upgrade completed successfully.																															
<i>failed</i>	The upgrade failed due to a local issue.																															
source	Source that set up the federated upgrade config.	option	-	user																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>user</i></td><td>Upgrade configured based on user input.</td></tr><tr><td><i>auto-firmware-upgrade</i></td><td>Upgrade configured by the FortiGuard auto-firmware-upgrade feature.</td></tr></table>	Option	Description	<i>user</i>	Upgrade configured based on user input.	<i>auto-firmware-upgrade</i>	Upgrade configured by the FortiGuard auto-firmware-upgrade feature.																									
	Option	Description																														
	<i>user</i>	Upgrade configured based on user input.																														
<i>auto-firmware-upgrade</i>	Upgrade configured by the FortiGuard auto-firmware-upgrade feature.																															
failure-reason	Reason for upgrade failure.	option	-	none																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No failure.</td></tr><tr><td><i>internal</i></td><td>An internal error occurred.</td></tr><tr><td><i>timeout</i></td><td>The upgrade timed out.</td></tr><tr><td><i>device-type-unsupported</i></td><td>The device type was not supported by the FortiGate.</td></tr><tr><td><i>download-failed</i></td><td>The image could not be downloaded.</td></tr><tr><td><i>device-missing</i></td><td>The device was disconnected from the FortiGate.</td></tr></table>	Option	Description	<i>none</i>	No failure.	<i>internal</i>	An internal error occurred.	<i>timeout</i>	The upgrade timed out.	<i>device-type-unsupported</i>	The device type was not supported by the FortiGate.	<i>download-failed</i>	The image could not be downloaded.	<i>device-missing</i>	The device was disconnected from the FortiGate.																	
	Option	Description																														
	<i>none</i>	No failure.																														
	<i>internal</i>	An internal error occurred.																														
	<i>timeout</i>	The upgrade timed out.																														
	<i>device-type-unsupported</i>	The device type was not supported by the FortiGate.																														
	<i>download-failed</i>	The image could not be downloaded.																														
<i>device-missing</i>	The device was disconnected from the FortiGate.																															

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>version-unavailable</i>	An image matching the device and version could not be found.		
	<i>staging-failed</i>	The image could not be pushed to the device.		
	<i>reboot-failed</i>	The device could not be rebooted.		
	<i>device-not-reconnected</i>	The device did not reconnect after rebooting.		
	<i>node-not-ready</i>	A device in the Security Fabric tree was not ready.		
	<i>no-final-confirmation</i>	The coordinating FortiGate did not confirm the upgrade.		
	<i>no-confirmation-query</i>	A downstream FortiGate did not initiate final confirmation.		
	<i>config-error-log-nonempty</i>	Configuration errors encountered during the upgrade.		
	<i>node-failed</i>	A device in the Security Fabric tree failed.		
failure-device	Serial number of the node to include.	string	Maximum length: 79	
upgrade-id	Unique identifier for this upgrade.	integer	Minimum value: 0 Maximum value: 4294967295	0
next-path-index	The index of the next image to upgrade to.	integer	Minimum value: 0 Maximum value: 10	0
ha-reboot-controller	Serial number of the FortiGate unit that will control the reboot process for the federated upgrade of the HA cluster.	string	Maximum length: 79	

config node-list

Parameter	Description	Type	Size	Default
serial	Serial number of the node to include.	string	Maximum length: 79	
timing	Run immediately or at a scheduled time.	option	-	immediate

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>immediate</i>	Begin the upgrade immediately.		
	<i>scheduled</i>	Begin the upgrade at a configured time.		
maximum-minutes	Maximum number of minutes to allow for immediate upgrade preparation.	integer	Minimum value: 5 Maximum value: 10080	15
time	Scheduled upgrade execution time in UTC (hh:mm yyyy/mm/dd UTC).	user	Not Specified	
setup-time	Upgrade preparation start time in UTC (hh:mm yyyy/mm/dd UTC).	user	Not Specified	
upgrade-path	Fortinet OS image versions to upgrade through in major-minor-patch format, such as 7-0-4.	user	Not Specified	
device-type	Fortinet device type.	option	-	fortiproxy
	Option	Description		
	<i>fortiproxy</i>	This device is a FortiProxy.		
	<i>fortiswitch</i>	This device is a FortiSwitch.		
	<i>fortiap</i>	This device is a FortiAP.		
	<i>fortiextender</i>	This device is a FortiExtender.		
coordinating-fortiproxy	Serial number of the FortiProxy unit that controls this device.	string	Maximum length: 79	

config system fips-cc

Configure FIPS-CC mode.

```
config system fips-cc
    Description: Configure FIPS-CC mode.
    set status [enable|disable]
    set self-test-period {integer}
    set key-generation-self-test [enable|disable]
end
```

config system fips-cc

Parameter	Description	Type	Size	Default						
status	Enable/disable ciphers for FIPS mode of operation.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FIPS-CC mode.</td></tr><tr><td><i>disable</i></td><td>Disable FIPS-CC mode.</td></tr></table>				Option	Description	<i>enable</i>	Enable FIPS-CC mode.	<i>disable</i>	Disable FIPS-CC mode.
	Option	Description								
	<i>enable</i>	Enable FIPS-CC mode.								
	<i>disable</i>	Disable FIPS-CC mode.								
self-test-period	Self test period.	integer	Minimum value: 1 Maximum value: 1440	1440						
key-generation-self-test	Enable/disable self tests after key generation.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable self tests after key generation.</td></tr><tr><td><i>disable</i></td><td>Disable self tests after key generation.</td></tr></table>				Option	Description	<i>enable</i>	Enable self tests after key generation.	<i>disable</i>	Disable self tests after key generation.
	Option	Description								
	<i>enable</i>	Enable self tests after key generation.								
<i>disable</i>	Disable self tests after key generation.									

config system fortianalyzer-connectivity

FortiAnalyzer Connectivity.

```
config system fortianalyzer-connectivity
    Description: FortiAnalyzer Connectivity.
end
```

config system fortiguard-log-service

Configuration of FortiCloud log service.

```
config system fortiguard-log-service
    Description: Configuration of FortiCloud log service.
end
```

config system fortiguard-service

Configuration of FortiGuard services.

```
config system fortiguard-service
    Description: Configuration of FortiGuard services.
end
```

config system fortiguard

Configure FortiGuard services.

```
config system fortiguard
    Description: Configure FortiGuard services.
    set fortiguard-anycast [enable|disable]
    set fortiguard-anycast-source [fortinet|aws|...]
    set protocol [udp|http|...]
    set port [8888|53|...]
    set load-balance-servers {integer}
    set auto-join-forticloud [enable|disable]
    set update-server-location [automatic|usa|...]
    set sandbox-region {string}
    set sandbox-inline-scan [enable|disable]
    set update-ffdb [enable|disable]
    set update-uwdb [enable|disable]
    set update-dldb [enable|disable]
    set update-extdb [enable|disable]
    set update-build-proxy [enable|disable]
    set persistent-connection [enable|disable]
    set vdom {string}
    set auto-firmware-upgrade [enable|disable]
    set auto-firmware-upgrade-day {option1}, {option2}, ...
    set auto-firmware-upgrade-delay {integer}
    set auto-firmware-upgrade-start-hour {integer}
    set auto-firmware-upgrade-end-hour {integer}
    set gui-prompt-auto-upgrade [enable|disable]
    set antispam-force-off [enable|disable]
    set antispam-cache [enable|disable]
    set antispam-cache-ttl {integer}
    set antispam-cache-mpercent {integer}
    set antispam-license {integer}
    set antispam-expiration {integer}
    set antispam-timeout {integer}
    set outbreak-prevention-force-off [enable|disable]
    set outbreak-prevention-cache [enable|disable]
    set outbreak-prevention-cache-ttl {integer}
    set outbreak-prevention-cache-mpercent {integer}
    set outbreak-prevention-license {integer}
    set outbreak-prevention-expiration {integer}
    set outbreak-prevention-timeout {integer}
    set ia-license {integer}
    set ia-expiration {integer}
    set fnbi-license {integer}
    set fnbi-expiration {integer}
    set webfilter-force-off [enable|disable]
    set webfilter-cache [enable|disable]
    set webfilter-cache-ttl {integer}
    set webfilter-license {integer}
```

```

set webfilter-expiration {integer}
set webfilter-timeout {integer}
set sdns-server-ip {user}
set sdns-server-port {integer}
set anycast-sdns-server-ip {ipv4-address}
set anycast-sdns-server-port {integer}
set sdns-options {option1}, {option2}, ...
set source-ip {ipv4-address}
set source-ip6 {ipv6-address}
set proxy-server-ip {string}
set proxy-server-port {integer}
set proxy-username {string}
set proxy-password {password}
set videofilter-license {integer}
set videofilter-expiration {integer}
set ddns-server-ip {ipv4-address}
set ddns-server-ip6 {ipv6-address}
set ddns-server-port {integer}
set interface-select-method [auto|specify]
set interface {string}

```

end

config system fortiguard

Parameter	Description	Type	Size	Default								
fortiguard-anycast	Enable/disable use of FortiGuard's Anycast network.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of FortiGuard's Anycast network.</td></tr><tr><td><i>disable</i></td><td>Disable use of FortiGuard's Anycast network.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of FortiGuard's Anycast network.	<i>disable</i>	Disable use of FortiGuard's Anycast network.					
Option	Description											
<i>enable</i>	Enable use of FortiGuard's Anycast network.											
<i>disable</i>	Disable use of FortiGuard's Anycast network.											
fortiguard-anycast-source	Configure which of Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network. Default is Fortinet.	option	-	fortinet								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortinet</i></td><td>Use Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network.</td></tr><tr><td><i>aws</i></td><td>Use Fortinet's AWS servers to provide FortiGuard services in FortiGuard's anycast network.</td></tr><tr><td><i>debug</i></td><td>Use Fortinet's internal test servers to provide FortiGuard services in FortiGuard's anycast network.</td></tr></table>	Option	Description	<i>fortinet</i>	Use Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network.	<i>aws</i>	Use Fortinet's AWS servers to provide FortiGuard services in FortiGuard's anycast network.	<i>debug</i>	Use Fortinet's internal test servers to provide FortiGuard services in FortiGuard's anycast network.			
Option	Description											
<i>fortinet</i>	Use Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network.											
<i>aws</i>	Use Fortinet's AWS servers to provide FortiGuard services in FortiGuard's anycast network.											
<i>debug</i>	Use Fortinet's internal test servers to provide FortiGuard services in FortiGuard's anycast network.											
protocol	Protocol used to communicate with the FortiGuard servers.	option	-	https								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>udp</i>	UDP for server communication (for use by FortiGuard or FortiManager).		
	<i>http</i>	HTTP for server communication (for use only by FortiManager).		
	<i>https</i>	HTTPS for server communication (for use by FortiGuard or FortiManager).		
port	Port used to communicate with the FortiGuard servers.	option	-	443
	Option	Description		
	<i>8888</i>	port 8888 for server communication.		
	<i>53</i>	port 53 for server communication.		
	<i>80</i>	port 80 for server communication.		
	<i>443</i>	port 443 for server communication.		
load-balance-servers	Number of servers to alternate between as first FortiGuard option.	integer	Minimum value: 1 Maximum value: 266	1
auto-join-forticloud	Automatically connect to and login to FortiCloud.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable automatic connection and login to FortiCloud.		
	<i>disable</i>	Disable automatic connection and login to FortiCloud.		
update-server-location	Location from which to receive FortiGuard updates.	option	-	automatic
	Option	Description		
	<i>automatic</i>	FortiGuard servers chosen based on closest proximity to FortiProxy unit.		
	<i>usa</i>	FortiGuard servers in United States.		
	<i>eu</i>	FortiGuard servers in the European Union.		
sandbox-region	FortiCloud Sandbox region.	string	Maximum length: 63	
sandbox-inline-scan	Enable/disable FortiCloud Sandbox inline-scan.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable FortiCloud Sandbox inline scan.		
	<i>disable</i>	Disable FortiCloud Sandbox inline scan.		
update-ffdb	Enable/disable Internet Service Database update.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Internet Service Database update.		
	<i>disable</i>	Disable Internet Service Database update.		
update-uwdb	Enable/disable allowlist update.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable allowlist update.		
	<i>disable</i>	Disable allowlist update.		
update-dldb	Enable/disable DLP signature update.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable DLP signature update.		
	<i>disable</i>	Disable DLP signature update.		
update-extdb	Enable/disable external resource update.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable external resource update.		
	<i>disable</i>	Disable external resource update.		
update-build-proxy	Enable/disable proxy dictionary rebuild.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable proxy dictionary rebuild.		
	<i>disable</i>	Disable proxy dictionary rebuild.		
persistent-connection	Enable/disable use of persistent connection to receive update notification from FortiGuard.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable persistent connection to receive update notification from FortiGuard.		
	<i>disable</i>	Disable persistent connection to receive update notification from FortiGuard.		
vdom	FortiGuard Service virtual domain name.	string	Maximum length: 31	
auto-firmware-upgrade	Enable/disable automatic patch-level firmware upgrade from FortiGuard. The FortiGate unit searches for new patches only in the same major and minor version.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable automatic patch-level firmware upgrade to latest version from FortiGuard.		
	<i>disable</i>	Disable automatic patch-level firmware upgrade to latest version from FortiGuard.		
auto-firmware-upgrade-day	Allowed day. Disallow any day of the week to use auto-firmware-upgrade-delay instead, which waits for designated days before installing an automatic patch-level firmware upgrade.	option	-	
	Option	Description		
	<i>sunday</i>	Sunday.		
	<i>monday</i>	Monday.		
	<i>tuesday</i>	Tuesday.		
	<i>wednesday</i>	Wednesday.		
	<i>thursday</i>	Thursday.		
	<i>friday</i>	Friday.		
	<i>saturday</i>	Saturday.		
auto-firmware-upgrade-delay	Delay of day of the week for installing an automatic patch-level firmware upgrade.	integer	Minimum value: 0 Maximum value: 14	3
auto-firmware-upgrade-start-hour	Start time in the designated time window for automatic patch-level firmware upgrade from FortiGuard in 24 hour time. The actual upgrade time is selected randomly within the time window.	integer	Minimum value: 0 Maximum value: 23	1

Parameter	Description	Type	Size	Default
auto-firmware-upgrade-end-hour	End time in the designated time window for automatic patch-level firmware upgrade from FortiGuard in 24 hour time. When the end time is smaller than the start time, the end time is interpreted as the next day. The actual upgrade time is selected randomly within the time window.	integer	Minimum value: 0 Maximum value: 23	4
gui-prompt-auto-upgrade	Enable/disable prompting of automatic patch-level firmware upgrade recommendation.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable prompting of automatic patch-level firmware upgrade recommendation.	
	<i>disable</i>		Disable prompting of automatic patch-level firmware upgrade recommendation.	
antispam-force-off	Enable/disable turning off the FortiGuard antispam service.	option	-	disable
	Option		Description	
	<i>enable</i>		Turn off the FortiGuard antispam service.	
	<i>disable</i>		Allow the FortiGuard antispam service.	
antispam-cache	Enable/disable FortiGuard antispam request caching. Uses a small amount of memory but improves performance.	option	-	enable
	Option		Description	
	<i>enable</i>		Enable FortiGuard antispam request caching.	
	<i>disable</i>		Disable FortiGuard antispam request caching.	
antispam-cache-ttl	Time-to-live for antispam cache entries in seconds. Lower times reduce the cache size. Higher times may improve performance since the cache will have more entries.	integer	Minimum value: 300 Maximum value: 86400	1800
antispam-cache-mpercent	Maximum percent of FortiProxy memory the antispam cache is allowed to use.	integer	Minimum value: 1 Maximum value: 15	2

Parameter	Description	Type	Size	Default
antispam-license	Interval of time between license checks for the FortiGuard antispam contract.	integer	Minimum value: 0 Maximum value: 4294967295	4294967295
antispam-expiration	Expiration date of the FortiGuard antispam contract.	integer	Minimum value: 0 Maximum value: 4294967295	0
antispam-timeout	Antispam query time out.	integer	Minimum value: 1 Maximum value: 30	7
outbreak-prevention-force-off	Turn off FortiGuard Virus Outbreak Prevention service.	option	-	disable
	Option Description			
	enable Turn off FortiGuard antivirus service.			
	disable Allow the FortiGuard antivirus service.			
outbreak-prevention-cache	Enable/disable FortiGuard Virus Outbreak Prevention cache.	option	-	enable
	Option Description			
	enable Enable FortiGuard antivirus caching.			
	disable Disable FortiGuard antivirus caching.			
outbreak-prevention-cache-ttl	Time-to-live for FortiGuard Virus Outbreak Prevention cache entries.	integer	Minimum value: 300 Maximum value: 86400	300
outbreak-prevention-cache-mpercent	Maximum percent of memory FortiGuard Virus Outbreak Prevention cache can use.	integer	Minimum value: 1 Maximum value: 15	2

Parameter	Description	Type	Size	Default						
outbreak-prevention-license	Interval of time between license checks for FortiGuard Virus Outbreak Prevention contract.	integer	Minimum value: 0 Maximum value: 4294967295	4294967295						
outbreak-prevention-expiration	Expiration date of FortiGuard Virus Outbreak Prevention contract.	integer	Minimum value: 0 Maximum value: 4294967295	0						
outbreak-prevention-timeout	FortiGuard Virus Outbreak Prevention time out.	integer	Minimum value: 1 Maximum value: 30	7						
ia-license	License type.	integer	Minimum value: 0 Maximum value: 4294967295	0						
ia-expiration	License expiration.	integer	Minimum value: 0 Maximum value: 4294967295	0						
fnbi-license	License type.	integer	Minimum value: 0 Maximum value: 4294967295	0						
fnbi-expiration	License expiration.	integer	Minimum value: 0 Maximum value: 4294967295	0						
webfilter-force-off	Enable/disable turning off the FortiGuard web filtering service.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Turn off the FortiGuard web filtering service.</td></tr><tr><td>disable</td><td>Allow the FortiGuard web filtering service to operate.</td></tr></table>	Option	Description	enable	Turn off the FortiGuard web filtering service.	disable	Allow the FortiGuard web filtering service to operate.			
Option	Description									
enable	Turn off the FortiGuard web filtering service.									
disable	Allow the FortiGuard web filtering service to operate.									

Parameter	Description	Type	Size	Default
webfilter-cache	Enable/disable FortiGuard web filter caching.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable FortiGuard web filter caching.		
	<i>disable</i>	Disable FortiGuard web filter caching.		
webfilter-cache-ttl	Time-to-live for web filter cache entries in seconds.	integer	Minimum value: 300 Maximum value: 86400	3600
webfilter-license	Interval of time between license checks for the FortiGuard web filter contract.	integer	Minimum value: 0 Maximum value: 4294967295	4294967295
webfilter-expiration	Expiration date of the FortiGuard web filter contract.	integer	Minimum value: 0 Maximum value: 4294967295	0
webfilter-timeout	Web filter query time out.	integer	Minimum value: 1 Maximum value: 30	15
sdns-server-ip	IP address of the FortiGuard DNS rating server.	user	Not Specified	
sdns-server-port	Port to connect to on the FortiGuard DNS rating server.	integer	Minimum value: 1 Maximum value: 65535	53
anycast-sdns-server-ip	IP address of the FortiGuard anycast DNS rating server.	ipv4-address	Not Specified	0.0.0.0
anycast-sdns-server-port	Port to connect to on the FortiGuard anycast DNS rating server.	integer	Minimum value: 1 Maximum value: 65535	853
sdns-options	Customization options for the FortiGuard DNS service.	option	-	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>include-question-section</i>	Include DNS question section in the FortiGuard DNS setup message.		
source-ip	Source IPv4 address used to communicate with FortiGuard.	ipv4-address	Not Specified	0.0.0.0
source-ip6	Source IPv6 address used to communicate with FortiGuard.	ipv6-address	Not Specified	::
proxy-server-ip	Hostname or IP address of the proxy server.	string	Maximum length: 63	
proxy-server-port	Port used to communicate with the proxy server.	integer	Minimum value: 0 Maximum value: 65535	0
proxy-username	Proxy user name.	string	Maximum length: 64	
proxy-password	Proxy user password.	password	Not Specified	
videofilter-license	Interval of time between license checks for the FortiGuard video filter contract.	integer	Minimum value: 0 Maximum value: 4294967295	4294967295
videofilter-expiration	Expiration date of the FortiGuard video filter contract.	integer	Minimum value: 0 Maximum value: 4294967295	0
ddns-server-ip	IP address of the FortiDDNS server.	ipv4-address	Not Specified	0.0.0.0
ddns-server-ip6	IPv6 address of the FortiDDNS server.	ipv6-address	Not Specified	::
ddns-server-port	Port used to communicate with FortiDDNS servers.	integer	Minimum value: 1 Maximum value: 65535	443
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config system fortindr

Configure FortiNDR.

```
config system fortindr
  Description: Configure FortiNDR.
  set status [disable|enable]
  set source-ip {string}
  set interface-select-method [auto|specify]
  set interface {string}
end
```

config system fortindr

Parameter	Description	Type	Size	Default
status	Enable/disable FortiNDR.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable FortiNDR.		
	<i>enable</i>	Enable FortiNDR.		
source-ip	Source IP address for communications to FortiNDR.	string	Maximum length: 63	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config system fortisandbox

Configure FortiSandbox.

```
config system fortisandbox
    Description: Configure FortiSandbox.
    set status [enable|disable]
    set forticloud [enable|disable]
    set inline-scan [enable|disable]
    set server {string}
    set source-ip {string}
    set interface-select-method [auto|specify]
    set interface {string}
    set enc-algorithm [default|high|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set email {string}
end
```

config system fortisandbox

Parameter	Description	Type	Size	Default
status	Enable/disable FortiSandbox.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FortiSandbox.		
	<i>disable</i>	Disable FortiSandbox.		
forticloud	Enable/disable FortiSandbox Cloud.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FortiSandbox Cloud.		
	<i>disable</i>	Disable FortiSandbox Cloud.		
inline-scan	Enable/disable FortiSandbox inline scan.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FortiSandbox inline scan.		
	<i>disable</i>	Disable FortiSandbox inline scan.		
server	Server address of the remote FortiSandbox.	string	Maximum length: 63	
source-ip	Source IP address for communications to FortiSandbox.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default												
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	auto	Set outgoing interface automatically.	specify	Set outgoing interface manually.						
Option	Description															
auto	Set outgoing interface automatically.															
specify	Set outgoing interface manually.															
interface	Specify outgoing interface to reach server.	string	Maximum length: 15													
enc-algorithm	Configure the level of SSL protection for secure communication with FortiSandbox.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>SSL communication with high and medium encryption algorithms.</td></tr><tr><td>high</td><td>SSL communication with high encryption algorithms.</td></tr><tr><td>low</td><td>SSL communication with low encryption algorithms.</td></tr></table>				Option	Description	default	SSL communication with high and medium encryption algorithms.	high	SSL communication with high encryption algorithms.	low	SSL communication with low encryption algorithms.				
Option	Description															
default	SSL communication with high and medium encryption algorithms.															
high	SSL communication with high encryption algorithms.															
low	SSL communication with low encryption algorithms.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr></table>				Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.
Option	Description															
default	Follow system global setting.															
SSLv3	SSLv3.															
TLSv1	TLSv1.															
TLSv1-1	TLSv1.1.															
TLSv1-2	TLSv1.2.															
email	Notifier email address.	string	Maximum length: 63													

config system fsso-polling

Configure Fortinet Single Sign On (FSSO) server.

```

config system fsso-polling
    Description: Configure Fortinet Single Sign On (FSSO) server.
    set status [enable|disable]
    set listening-port {integer}
    set authentication [enable|disable]
    set auth-password {password}
end

```

config system fsso-polling

Parameter	Description	Type	Size	Default
status	Enable/disable FSSO Polling Mode.	option	-	enable
	Option	Description		
	enable	Enable FSSO Polling Mode.		
	disable	Disable FSSO Polling Mode.		
listening-port	Listening port to accept clients.	integer	Minimum value: 1 Maximum value: 65535	8000
authentication	Enable/disable FSSO Agent Authentication.	option	-	disable
	Option	Description		
	enable	Enable FSSO Agent Authentication.		
	disable	Disable FSSO Agent Authentication.		
auth-password	Password to connect to FSSO Agent.	password	Not Specified	

config system ftm-push

Configure FortiToken Mobile push services.

```
config system ftm-push
  Description: Configure FortiToken Mobile push services.
  set server-port {integer}
  set server-cert {string}
  set server-ip {ipv4-address}
  set server {string}
  set status [enable|disable]
end
```

config system ftm-push

Parameter	Description	Type	Size	Default
server-port	Port to communicate with FortiToken Mobile push services server.	integer	Minimum value: 1 Maximum value: 65535	4433
server-cert	Name of the server certificate to be used for SSL.	string	Maximum length: 35	Fortinet_Factory
server-ip	IPv4 address of FortiToken Mobile push services server (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0
server	IPv4 address or domain name of FortiToken Mobile push services server.	string	Maximum length: 127	
status	Enable/disable the use of FortiToken Mobile push services.	option	-	disable

Option	Description
<i>enable</i>	Enable FortiToken Mobile push services.
<i>disable</i>	Disable FortiToken Mobile push services.

config system geoip-country

Define geoip country name-ID table.

```
config system geoip-country
    Description: Define geoip country name-ID table.
    edit <id>
        set name {string}
    next
end
```

config system geoip-country

Parameter	Description	Type	Size	Default
id	Country ID.	string	Maximum length: 2	
name	Country name.	string	Maximum length: 63	

config system geoip-override

Configure geographical location mapping for IP address(es) to override mappings from FortiGuard.

```
config system geoip-override
  Description: Configure geographical location mapping for IP address(es) to override
  mappings from FortiGuard.
  edit <name>
    set description {string}
    set country-id {string}
    config ip-range
      Description: Table of IP ranges assigned to country.
      edit <id>
        set start-ip {ipv4-address}
        set end-ip {ipv4-address}
      next
    end
  config ip6-range
    Description: Table of IPv6 ranges assigned to country.
    edit <id>
      set start-ip {ipv6-address}
      set end-ip {ipv6-address}
    next
  end
next
end
```

config system geoip-override

Parameter	Description	Type	Size	Default
name	Location name.	string	Maximum length: 63	
description	Description.	string	Maximum length: 127	
country-id	Two character Country ID code.	string	Maximum length: 2	

config ip-range

Parameter	Description	Type	Size	Default
id	ID of individual entry in the IP range table.	integer	Minimum value: 0 Maximum value: 65535	0

Parameter	Description	Type	Size	Default
start-ip	Starting IP address, inclusive, of the address range (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0
end-ip	Ending IP address, inclusive, of the address range (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0

config ip6-range

Parameter	Description	Type	Size	Default
id	ID of individual entry in the IPv6 range table.	integer	Minimum value: 0 Maximum value: 65535	0
start-ip	Starting IP address, inclusive, of the address range (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::
end-ip	Ending IP address, inclusive, of the address range (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::

config system global

Configure global attributes.

```
config system global
  Description: Configure global attributes.
  set language [english|french|...]
  set gui-ipv6 [enable|disable]
  set gui-replacement-message-groups [enable|disable]
  set gui-local-out [enable|disable]
  set gui-certificates [enable|disable]
  set gui-custom-language [enable|disable]
  set gui-app-detection-sdwan [enable|disable]
  set gui-display-hostname [enable|disable]
  set gui-fortigate-cloud-sandbox [enable|disable]
  set gui-firmware-upgrade-warning [enable|disable]
  set gui-forticare-registration-setup-warning [enable|disable]
  set gui-auto-upgrade-setup-warning [enable|disable]
  set gui-workflow-management [enable|disable]
  set gui-cdn-usage [enable|disable]
  set admin-https-ssl-versions {option1}, {option2}, ...
  set admin-https-ssl-ciphersuites {option1}, {option2}, ...
  set admin-https-ssl-banned-ciphers {option1}, {option2}, ...
  set admin-timeout {integer}
  set admin-console-timeout {integer}
  set ssd-trim-freq [never|hourly|...]
  set ssd-trim-hour {integer}
```

```
set ssd-trim-min {integer}
set ssd-trim-weekday [sunday|monday|...]
set ssd-trim-date {integer}
set admin-concurrent [enable|disable]
set admin-lockout-threshold {integer}
set admin-lockout-duration {integer}
set refresh {integer}
set interval {integer}
set failtime {integer}
set daily-restart [enable|disable]
set restart-time {user}
set wad-restart-mode [none|time|...]
set wad-restart-start-time {user}
set wad-restart-end-time {user}
set radius-port {integer}
set admin-login-max {integer}
set remoteauthtimeout {integer}
set ldapconntimeout {integer}
set batch-cmdb [enable|disable]
set multi-factor-authentication [optional|mandatory]
set ssl-min-proto-version [SSLv3|TLSv1|...]
set autorun-log-fsck [enable|disable]
set timezone [01|02|...]
set traffic-priority [tos|dscp]
set traffic-priority-level [low|medium|...]
set quic-congestion-control-algo [cubic|bbr|...]
set quic-max-datagram-size {integer}
set quic-udp-payload-size-shaping-per-cid [enable|disable]
set quic-ack-threshold {integer}
set quic-pmtud [enable|disable]
set quic-tls-handshake-timeout {integer}
set anti-replay [disable|loose|...]
set pmtu-discovery [enable|disable]
set revision-image-auto-backup [enable|disable]
set revision-backup-on-logout [enable|disable]
set hostname {string}
set alias {string}
set strong-crypto [enable|disable]
set ssl-static-key-ciphers [enable|disable]
set ssh-kex-algo {option1}, {option2}, ...
set ssh-enc-algo {option1}, {option2}, ...
set ssh-mac-algo {option1}, {option2}, ...
set snat-route-change [enable|disable]
set speedtest-server [enable|disable]
set cli-audit-log [enable|disable]
set dh-params [1024|1536|...]
set fds-statistics [enable|disable]
set fds-statistics-period {integer}
set tcp-option [enable|disable]
set lldp-transmission [enable|disable]
set lldp-reception [enable|disable]
set proxy-auth-timeout {integer}
set resigned-pkey-period {integer}
set proxy-keep-alive-mode [session|traffic|...]
set proxy-re-authentication-time {integer}
set proxy-auth-lifetime [enable|disable]
```



```
set proxy-auth-lifetime-timeout {integer}
set proxy-auth-machine-timeout {integer}
set proxy-resource-mode [enable|disable]
set proxy-cert-use-mgmt-vdom [enable|disable]
set update-tls-finger-print [enable|disable]
set sys-perf-log-interval {integer}
set check-protocol-header [loose|strict]
set vip-arp-range [unlimited|restricted]
set tcp-halfclose-timer {integer}
set tcp-halfopen-timer {integer}
set tcp-timewait-timer {integer}
set tcp-rst-timer {integer}
set udp-idle-timer {integer}
set block-session-timer {integer}
set ip-src-port-range {user}
set pre-login-banner [enable|disable]
set post-login-banner [disable|enable]
set tftp [enable|disable]
set av-failopen [pass|off|...]
set av-failopen-session [enable|disable]
set kernel-panic-timeout {integer}
set kernel-panic-debug [enable|disable]
set memory-use-threshold-extreme {integer}
set memory-use-threshold-red {integer}
set memory-use-threshold-green {integer}
set ip-fragment-mem-thresholds {integer}
set cpu-use-threshold {integer}
set log-single-cpu-high [enable|disable]
set check-reset-range [strict|disable]
set admin-port {integer}
set admin-sport {integer}
set admin-host {string}
set admin-https-redirect [enable|disable]
set admin-hsts-max-age {integer}
set admin-ssh-password [enable|disable]
set admin-restrict-local [enable|disable]
set admin-ssh-port {integer}
set admin-ssh-grace-time {integer}
set admin-ssh-vl [enable|disable]
set admin-telnet [enable|disable]
set admin-telnet-port {integer}
set admin-forticloud-sso-login [enable|disable]
set admin-forticloud-sso-default-profile {string}
set default-service-source-port {user}
set admin-server-cert {string}
set admin-https-pki-required [enable|disable]
set auth-http-port {integer}
set auth-https-port {integer}
set auth-ike-saml-port {integer}
set auth-keepalive [enable|disable]
set policy-auth-concurrent {integer}
set auth-session-limit [block-new|logout-inactive]
set auth-cert {string}
set clt-cert-req [enable|disable]
set fortiservice-port {integer}
set cfg-save [automatic|manual|...]
```

```
set cfg-revert-timeout {integer}
set reboot-upon-config-restore [enable|disable]
set admin-scp [enable|disable]
set security-rating-result-submission [enable|disable]
set security-rating-run-on-schedule [enable|disable]
set fortiextender-data-port {integer}
set fortiextender [disable|enable]
set extender-controller-reserved-network {ipv4-classnet-host}
set fortiextender-discovery-lockdown [disable|enable]
set fortiextender-provision-on-authorization [enable|disable]
set dnsproxy-worker-count {integer}
set url-filter-count {integer}
set proxy-worker-count {integer}
set scanunit-count {integer}
set fgd-alert-subscription {option1}, {option2}, ...
set ipv6-accept-dad {integer}
set ipv6-allow-multicast-probe [enable|disable]
set ipv6-allow-local-in-silent-drop [enable|disable]
set csr-ca-attribute [enable|disable]
set wimax-4g-usb [enable|disable]
set cert-chain-max {integer}
set two-factor-ftk-expiry {integer}
set two-factor-email-expiry {integer}
set two-factor-sms-expiry {integer}
set two-factor-fac-expiry {integer}
set two-factor-ftm-expiry {integer}
set max-img-cache-size {integer}
set img-cache-mode [stop|rolling]
set per-user-bal [enable|disable]
set wad-worker-count {integer}
set wad-csvc-cs-count {integer}
set wad-csvc-db-count {integer}
set http-view [enable|disable]
set wad-source-affinity [disable|enable]
set wad-memory-change-granularity {integer}
set login-timestamp [enable|disable]
set miglogd-children {integer}
set special-file-23-support [disable|enable]
set log-uuid-address [enable|disable]
set log-ssl-connection [enable|disable]
set gui-rest-api-cache [enable|disable]
set gui-fortiguard-resource-fetch [enable|disable]
set arp-max-entry {integer}
set ha-affinity {string}
set cmdbsvr-affinity {string}
set av-affinity {string}
set wad-affinity {string}
set ips-affinity {string}
set miglog-affinity {string}
set syslog-affinity {string}
set url-filter-affinity {string}
set ndp-max-entry {integer}
set br-fdb-max-entry {integer}
set max-route-cache-size {integer}
set ipsec-round-robin [enable|disable]
set ipsec-soft-dec-async [enable|disable]
```

```

set device-idle-timeout {integer}
set user-device-store-max-devices {integer}
set user-device-store-max-users {integer}
set user-device-store-max-unified-mem {integer}
set gui-device-latitude {string}
set gui-device-longitude {string}
set v-tpm [disable|enable]
set private-data-encryption [disable|enable]
set auto-auth-extension-device [enable|disable]
set gui-theme [jade|neutrino|...]
set gui-date-format [yyyy/MM/dd|dd/MM/yyyy|...]
set gui-date-time-source [system|browser]
set igmp-state-limit {integer}
set cloud-communication [enable|disable]
set ipsec-ha-seqjump-rate {integer}
set fortitoken-cloud [enable|disable]
set faz-disk-buffer-size {integer}
set irq-time-accounting [auto|force]
set management-ip {string}
set management-port {integer}
set management-port-use-admin-sport [enable|disable]
set internet-service-database [mini|standard|...]
set early-tcp-npu-session [enable|disable]
set interface-subnet-usage [disable|enable]
set sflowd-max-children-num {integer}
set license-overlimit [bypass|block]
set max-session-per-user {integer}
set conntrack {integer}
set established-timeout {integer}
set time-wait-timeout {integer}
set fin-wait-timeout {integer}
set close-wait-timeout {integer}
set syn-sent-timeout {integer}
set syn-recv-timeout {integer}
set last-ack-timeout {integer}
set udp-timeout {integer}
set udp-stream-timeout {integer}
set username-case-sensitivity [enable|disable]

```

end

config system global

Parameter	Description	Type	Size	Default
language	GUI display language.	option	-	english
	Option	Description		
	<i>english</i>	English.		
	<i>french</i>	French.		
	<i>spanish</i>	Spanish.		

Parameter	Description	Type	Size	Default
	Option Description			
	<i>portuguese</i>	Portuguese.		
	<i>japanese</i>	Japanese.		
	<i>trach</i>	Traditional Chinese.		
	<i>simch</i>	Simplified Chinese.		
	<i>korean</i>	Korean.		
gui-ipv6	Enable/disable IPv6 settings on the GUI.	option	-	enable
	Option Description			
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-replacement-message-groups	Enable/disable replacement message groups on the GUI.	option	-	disable
	Option Description			
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-local-out	Enable/disable Local-out traffic on the GUI.	option	-	disable
	Option Description			
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-certificates	Enable/disable the System > Certificate GUI page, allowing you to add and configure certificates from the GUI.	option	-	enable
	Option Description			
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-custom-language	Enable/disable custom languages in GUI.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-app-detection-sdwan	Enable/disable Allow app-detection based SD-WAN.	option	-	disable
	Option	Description		
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-display-hostname	Enable/disable displaying the FortiProxy's hostname on the GUI login page.	option	-	disable
	Option	Description		
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-fortigate-cloud-sandbox	Enable/disable displaying FortiProxy Cloud Sandbox on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-firmware-upgrade-warning	Enable/disable the firmware upgrade warning on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-forticare-registration-setup-warning	Enable/disable the FortiCare registration setup warning on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		

Parameter	Description	Type	Size	Default
gui-auto-upgrade-setup-warning	Enable/disable the automatic patch upgrade setup prompt on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-workflow-management	Enable/disable Workflow management features on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-cdn-usage	Enable/disable Load GUI static files from a CDN.	option	-	enable
	Option	Description		
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
admin-https-ssl-versions	Allowed TLS versions for web administration.	option	-	tlsv1-2 tlsv1-3
	Option	Description		
	<i>tlsv1-1</i>	TLS 1.1.		
	<i>tlsv1-2</i>	TLS 1.2.		
	<i>tlsv1-3</i>	TLS 1.3.		
admin-https-ssl-ciphersuites	Select one or more TLS 1.3 ciphersuites to enable. Does not affect ciphers in TLS 1.2 and below. At least one must be enabled. To disable all, remove TLS1.3 from admin-https-ssl-versions.	option	-	TLS-AES-128-GCM-SHA256 TLS-AES-256-GCM-SHA384 TLS-CHACHA20-POLY1305-SHA256

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>TLS-AES-128-GCM-SHA256</i>	Enable TLS-AES-128-GCM-SHA256 in TLS 1.3.		
	<i>TLS-AES-256-GCM-SHA384</i>	Enable TLS-AES-256-GCM-SHA384 in TLS 1.3.		
	<i>TLS-CHACHA20-POLY1305-SHA256</i>	Enable TLS-CHACHA20-POLY1305-SHA256 in TLS 1.3.		
	<i>TLS-AES-128-CCM-SHA256</i>	Enable TLS-AES-128-CCM-SHA256 in TLS 1.3.		
	<i>TLS-AES-128-CCM-8-SHA256</i>	Enable TLS-AES-128-CCM-8-SHA256 in TLS 1.3.		
admin-https-ssl-banned-ciphers	Select one or more cipher technologies that cannot be used in GUI HTTPS negotiations. Only applies to TLS 1.2 and below.	option	-	
	Option	Description		
	<i>RSA</i>	Ban the use of cipher suites using RSA key.		
	<i>DHE</i>	Ban the use of cipher suites using authenticated ephemeral DH key agreement.		
	<i>ECDHE</i>	Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.		
	<i>DSS</i>	Ban the use of cipher suites using DSS authentication.		
	<i>ECDSA</i>	Ban the use of cipher suites using ECDSA authentication.		
	<i>AES</i>	Ban the use of cipher suites using either 128 or 256 bit AES.		
	<i>AESGCM</i>	Ban the use of cipher suites using AES in Galois Counter Mode (GCM).		
	<i>CAMELLIA</i>	Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.		
	<i>3DES</i>	Ban the use of cipher suites using triple DES.		
	<i>SHA1</i>	Ban the use of cipher suites using HMAC-SHA1.		
	<i>SHA256</i>	Ban the use of cipher suites using HMAC-SHA256.		
	<i>SHA384</i>	Ban the use of cipher suites using HMAC-SHA384.		

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>STATIC</td><td>Ban the use of cipher suites using static keys.</td></tr><tr><td>CHACHA20</td><td>Ban the use of cipher suites using ChaCha20.</td></tr><tr><td>ARIA</td><td>Ban the use of cipher suites using ARIA.</td></tr><tr><td>AESCCM</td><td>Ban the use of cipher suites using AESCCM.</td></tr></table>	Option	Description	STATIC	Ban the use of cipher suites using static keys.	CHACHA20	Ban the use of cipher suites using ChaCha20.	ARIA	Ban the use of cipher suites using ARIA.	AESCCM	Ban the use of cipher suites using AESCCM.					
	Option	Description														
	STATIC	Ban the use of cipher suites using static keys.														
	CHACHA20	Ban the use of cipher suites using ChaCha20.														
	ARIA	Ban the use of cipher suites using ARIA.														
AESCCM	Ban the use of cipher suites using AESCCM.															
admin-timeout	Number of minutes before an idle administrator session times out. A shorter idle timeout is more secure.	integer	Minimum value: 5 1 Maximum value: 480	5												
admin-console-timeout	Console login timeout that overrides the admin timeout value.	integer	Minimum value: 15 Maximum value: 300	0												
ssd-trim-freq	How often to run SSD Trim. SSD Trim prevents SSD drive data loss by finding and isolating errors.	option	-	weekly												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>never</td><td>Never Run SSD Trim.</td></tr><tr><td>hourly</td><td>Run SSD Trim Hourly.</td></tr><tr><td>daily</td><td>Run SSD Trim Daily.</td></tr><tr><td>weekly</td><td>Run SSD Trim Weekly.</td></tr><tr><td>monthly</td><td>Run SSD Trim Monthly.</td></tr></table>	Option	Description	never	Never Run SSD Trim.	hourly	Run SSD Trim Hourly.	daily	Run SSD Trim Daily.	weekly	Run SSD Trim Weekly.	monthly	Run SSD Trim Monthly.			
	Option	Description														
	never	Never Run SSD Trim.														
	hourly	Run SSD Trim Hourly.														
	daily	Run SSD Trim Daily.														
	weekly	Run SSD Trim Weekly.														
monthly	Run SSD Trim Monthly.															
ssd-trim-hour	Hour of the day on which to run SSD Trim.	integer	Minimum value: 0 Maximum value: 23	1												
ssd-trim-min	Minute of the hour on which to run SSD Trim.	integer	Minimum value: 0 Maximum value: 60	60												
ssd-trim-weekday	Day of week to run SSD Trim.	option	-	sunday												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sunday</td><td>Sunday</td></tr><tr><td>monday</td><td>Monday</td></tr><tr><td>tuesday</td><td>Tuesday</td></tr></table>	Option	Description	sunday	Sunday	monday	Monday	tuesday	Tuesday							
	Option	Description														
	sunday	Sunday														
	monday	Monday														
tuesday	Tuesday															

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>wednesday</td><td>Wednesday</td></tr><tr><td>thursday</td><td>Thursday</td></tr><tr><td>friday</td><td>Friday</td></tr><tr><td>saturday</td><td>Saturday</td></tr></table>	Option	Description	wednesday	Wednesday	thursday	Thursday	friday	Friday	saturday	Saturday			
	Option	Description												
	wednesday	Wednesday												
	thursday	Thursday												
	friday	Friday												
saturday	Saturday													
ssd-trim-date	Date within a month to run ssd trim.	integer	Minimum value: 1 1 Maximum value: 31	1										
admin-concurrent	Enable/disable concurrent administrator logins. Use policy-auth-concurrent for firewall authenticated users.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable admin concurrent login.</td></tr><tr><td>disable</td><td>Disable admin concurrent login.</td></tr></table>	Option	Description	enable	Enable admin concurrent login.	disable	Disable admin concurrent login.							
	Option	Description												
	enable	Enable admin concurrent login.												
disable	Disable admin concurrent login.													
admin-lockout-threshold	Number of failed login attempts before an administrator account is locked out for the admin-lockout-duration.	integer	Minimum value: 1 1 Maximum value: 10	3										
admin-lockout-duration	Amount of time in seconds that an administrator account is locked out after reaching the admin-lockout-threshold for repeated failed login attempts.	integer	Minimum value: 60 1 Maximum value: 2147483647	60										
refresh	Statistics refresh interval second(s) in GUI.	integer	Minimum value: 0 0 Maximum value: 4294967295	0										
interval	Dead gateway detection interval.	integer	Minimum value: 5 0 Maximum value: 4294967295	5										

Parameter	Description	Type	Size	Default								
failtime	Fail-time for server lost.	integer	Minimum value: 0 Maximum value: 4294967295	5								
daily-restart	Enable/disable daily restart of FortiProxy unit. Use the restart-time option to set the time of day for the restart.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable daily reboot of the FortiProxy.</td></tr><tr><td>disable</td><td>Disable daily reboot of the FortiProxy.</td></tr></table>				Option	Description	enable	Enable daily reboot of the FortiProxy.	disable	Disable daily reboot of the FortiProxy.		
Option	Description											
enable	Enable daily reboot of the FortiProxy.											
disable	Disable daily reboot of the FortiProxy.											
restart-time	Daily restart time (hh:mm).	user	Not Specified									
wad-restart-mode	WAD worker restart mode.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>Disable restart of WAD workers.</td></tr><tr><td>time</td><td>Enable daily restart of WAD workers.</td></tr><tr><td>memory</td><td>Enable restart of WAD workers based on memory usage.</td></tr></table>				Option	Description	none	Disable restart of WAD workers.	time	Enable daily restart of WAD workers.	memory	Enable restart of WAD workers based on memory usage.
Option	Description											
none	Disable restart of WAD workers.											
time	Enable daily restart of WAD workers.											
memory	Enable restart of WAD workers based on memory usage.											
wad-restart-start-time	WAD workers daily restart time (hh:mm).	user	Not Specified									
wad-restart-end-time	WAD workers daily restart end time (hh:mm).	user	Not Specified									
radius-port	RADIUS service port number.	integer	Minimum value: 1 Maximum value: 65535	1812								
admin-login-max	Maximum number of administrators who can be logged in at the same time.	integer	Minimum value: 1 Maximum value: 100	100								
remoteauthtimeout	Number of seconds that the FortiProxy waits for responses from remote RADIUS, LDAP, or TACACS+ authentication servers.	integer	Minimum value: 1 Maximum value: 300	5								
ldapconntimeout	Global timeout for connections with remote LDAP servers in milliseconds.	integer	Minimum value: 1 Maximum value: 300000	500								

Parameter	Description	Type	Size	Default												
batch-cmdb	Enable/disable batch mode, allowing you to enter a series of CLI commands that will execute as a group once they are loaded.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable batch mode to execute in CMDB server.</td></tr><tr><td><i>disable</i></td><td>Disable batch mode to execute in CMDB server.</td></tr></table>	Option	Description	<i>enable</i>	Enable batch mode to execute in CMDB server.	<i>disable</i>	Disable batch mode to execute in CMDB server.									
Option	Description															
<i>enable</i>	Enable batch mode to execute in CMDB server.															
<i>disable</i>	Disable batch mode to execute in CMDB server.															
multi-factor-authentication	Enforce all login methods to require an additional authentication factor.	option	-	optional												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>optional</i></td><td>Do not enforce all login methods to require an additional authentication factor (controlled by user settings).</td></tr><tr><td><i>mandatory</i></td><td>Enforce all login methods to require an additional authentication factor.</td></tr></table>	Option	Description	<i>optional</i>	Do not enforce all login methods to require an additional authentication factor (controlled by user settings).	<i>mandatory</i>	Enforce all login methods to require an additional authentication factor.									
Option	Description															
<i>optional</i>	Do not enforce all login methods to require an additional authentication factor (controlled by user settings).															
<i>mandatory</i>	Enforce all login methods to require an additional authentication factor.															
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections.	option	-	TLSv1-2												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr><tr><td><i>TLSv1-3</i></td><td>TLSv1.3.</td></tr></table>	Option	Description	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.	<i>TLSv1-3</i>	TLSv1.3.			
Option	Description															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
<i>TLSv1-3</i>	TLSv1.3.															
autorun-log-fsck	Enable/disable automatic log partition check after ungraceful shutdown.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic log partition check after ungraceful shutdown.</td></tr><tr><td><i>disable</i></td><td>Disable automatic log partition check after ungraceful shutdown.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic log partition check after ungraceful shutdown.	<i>disable</i>	Disable automatic log partition check after ungraceful shutdown.									
Option	Description															
<i>enable</i>	Enable automatic log partition check after ungraceful shutdown.															
<i>disable</i>	Disable automatic log partition check after ungraceful shutdown.															

Parameter	Description	Type	Size	Default
timezone	Number corresponding to your time zone from 00 to 86. Enter set timezone ? to view the list of time zones and the numbers that represent them.	option	-	00

Option	Description
01	(GMT-11:00) Midway Island, Samoa
02	(GMT-10:00) Hawaii
03	(GMT-9:00) Alaska
04	(GMT-8:00) Pacific Time (US & Canada)
05	(GMT-7:00) Arizona
81	(GMT-7:00) Baja California Sur, Chihuahua
06	(GMT-7:00) Mountain Time (US & Canada)
07	(GMT-6:00) Central America
08	(GMT-6:00) Central Time (US & Canada)
09	(GMT-6:00) Mexico City
10	(GMT-6:00) Saskatchewan
11	(GMT-5:00) Bogota, Lima, Quito
12	(GMT-5:00) Eastern Time (US & Canada)
13	(GMT-5:00) Indiana (East)
74	(GMT-4:00) Caracas
14	(GMT-4:00) Atlantic Time (Canada)
77	(GMT-4:00) Georgetown
15	(GMT-4:00) La Paz
87	(GMT-4:00) Paraguay
16	(GMT-3:00) Santiago
17	(GMT-3:30) Newfoundland
18	(GMT-3:00) Brasilia
19	(GMT-3:00) Buenos Aires
20	(GMT-3:00) Nuuk (Greenland)
75	(GMT-3:00) Uruguay

Parameter	Description	Type	Size	Default
	Option	Description		
	21	(GMT-2:00) Mid-Atlantic		
	22	(GMT-1:00) Azores		
	23	(GMT-1:00) Cape Verde Is.		
	24	(GMT) Monrovia		
	80	(GMT) Greenwich Mean Time		
	79	(GMT) Casablanca		
	25	(GMT) Dublin, Edinburgh, Lisbon, London, Canary Is.		
	26	(GMT+1:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna		
	27	(GMT+1:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague		
	28	(GMT+1:00) Brussels, Copenhagen, Madrid, Paris		
	78	(GMT+1:00) Namibia		
	29	(GMT+1:00) Sarajevo, Skopje, Warsaw, Zagreb		
	30	(GMT+1:00) West Central Africa		
	31	(GMT+2:00) Kyiv, Athens, Sofia, Vilnius		
	32	(GMT+2:00) Bucharest		
	33	(GMT+2:00) Cairo		
	34	(GMT+2:00) Harare, Pretoria		
	35	(GMT+2:00) Helsinki, Riga, Tallinn		
	36	(GMT+2:00) Jerusalem		
	37	(GMT+3:00) Baghdad		
	38	(GMT+3:00) Kuwait, Riyadh		
	83	(GMT+3:00) Moscow		
	84	(GMT+3:00) Minsk		
	40	(GMT+3:00) Nairobi		
	85	(GMT+3:00) Istanbul		
	39	(GMT+3:00) St. Petersburg, Volgograd		
	41	(GMT+3:30) Tehran		
	42	(GMT+4:00) Abu Dhabi, Muscat		
	43	(GMT+4:00) Baku		

Parameter	Description	Type	Size	Default
	Option	Description		
	44	(GMT+4:30) Kabul		
	45	(GMT+5:00) Ekaterinburg		
	46	(GMT+5:00) Islamabad, Karachi, Tashkent		
	47	(GMT+5:30) Kolkata, Chennai, Mumbai, New Delhi		
	51	(GMT+5:30) Sri Jayawardenepara		
	48	(GMT+5:45) Kathmandu		
	49	(GMT+5:00) Almaty, Astana		
	50	(GMT+6:00) Dhaka		
	52	(GMT+6:30) Rangoon		
	53	(GMT+7:00) Bangkok, Hanoi, Jakarta, Novosibirsk		
	54	(GMT+7:00) Krasnoyarsk		
	55	(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi, Irkutsk		
	56	(GMT+8:00) Ulaan Bataar		
	57	(GMT+8:00) Kuala Lumpur, Singapore		
	58	(GMT+8:00) Perth		
	59	(GMT+8:00) Taipei		
	60	(GMT+9:00) Osaka, Sapporo, Tokyo, Seoul		
	61	(GMT+9:00) Yakutsk		
	62	(GMT+9:30) Adelaide		
	63	(GMT+9:30) Darwin		
	64	(GMT+10:00) Brisbane		
	65	(GMT+10:00) Canberra, Melbourne, Sydney		
	66	(GMT+10:00) Guam, Port Moresby		
	67	(GMT+10:00) Hobart		
	68	(GMT+10:00) Vladivostok		
	69	(GMT+10:00) Magadan		
	70	(GMT+11:00) Solomon Is., New Caledonia		
	71	(GMT+12:00) Auckland, Wellington		
	72	(GMT+12:00) Fiji, Kamchatka, Marshall Is.		

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>00</td><td>(GMT+12:00) Eniwetok, Kwajalein</td></tr><tr><td>82</td><td>(GMT+12:45) Chatham Islands</td></tr><tr><td>73</td><td>(GMT+13:00) Nuku'alofa</td></tr><tr><td>86</td><td>(GMT+13:00) Samoa</td></tr><tr><td>76</td><td>(GMT+14:00) Kiritimati</td></tr></table>	Option	Description	00	(GMT+12:00) Eniwetok, Kwajalein	82	(GMT+12:45) Chatham Islands	73	(GMT+13:00) Nuku'alofa	86	(GMT+13:00) Samoa	76	(GMT+14:00) Kiritimati			
	Option	Description														
	00	(GMT+12:00) Eniwetok, Kwajalein														
	82	(GMT+12:45) Chatham Islands														
	73	(GMT+13:00) Nuku'alofa														
	86	(GMT+13:00) Samoa														
76	(GMT+14:00) Kiritimati															
traffic-priority	Choose Type of Service (ToS) or Differentiated Services Code Point (DSCP) for traffic prioritization in traffic shaping.	option	-	tos												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tos</td><td>IP TOS.</td></tr><tr><td>dscp</td><td>DSCP (DiffServ) DS.</td></tr></table>	Option	Description	tos	IP TOS.	dscp	DSCP (DiffServ) DS.									
	Option	Description														
	tos	IP TOS.														
dscp	DSCP (DiffServ) DS.															
traffic-priority-level	Default system-wide level of priority for traffic prioritization.	option	-	medium												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>low</td><td>Low priority.</td></tr><tr><td>medium</td><td>Medium priority.</td></tr><tr><td>high</td><td>High priority.</td></tr></table>	Option	Description	low	Low priority.	medium	Medium priority.	high	High priority.							
	Option	Description														
	low	Low priority.														
	medium	Medium priority.														
high	High priority.															
quic-congestion-control-algo	QUIC congestion control algorithm.	option	-	cubic												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>cubic</td><td>Cubic.</td></tr><tr><td>bbr</td><td>BBR.</td></tr><tr><td>bbr2</td><td>BBR2.</td></tr><tr><td>reno</td><td>Reno.</td></tr></table>	Option	Description	cubic	Cubic.	bbr	BBR.	bbr2	BBR2.	reno	Reno.					
	Option	Description														
	cubic	Cubic.														
	bbr	BBR.														
	bbr2	BBR2.														
reno	Reno.															
quic-max-datagram-size	Maximum transmit datagram size.	integer	Minimum value: 1200 Maximum value: 1500	1500												

Parameter	Description	Type	Size	Default
quic-udp-payload-size-shaping-per-cid	Enable/disable UDP payload size shaping per connection ID.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable UDP payload size shaping per connection ID.		
	<i>disable</i>	Disable UDP payload size shaping per connection ID.		
quic-ack-thresold	Maximum number of unacknowledged packets before sending ACK.	integer	Minimum value: 2 Maximum value: 5	3
quic-pmtud	Enable/disable path MTU discovery.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable path MTU discovery.		
	<i>disable</i>	Disable path MTU discovery.		
quic-tls-handshake-timeout	Time-to-live.	integer	Minimum value: 1 Maximum value: 60	5
anti-replay	Level of checking for packet replay and TCP sequence checking.	option	-	strict
	Option	Description		
	<i>disable</i>	Disable anti-replay check.		
	<i>loose</i>	Loose anti-replay check.		
	<i>strict</i>	Strict anti-replay check.		
pmtu-discovery	Enable/disable path MTU discovery.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable path MTU discovery.		
	<i>disable</i>	Disable path MTU discovery.		
revision-image-auto-backup	Enable/disable back-up of the latest image revision after the firmware is upgraded.	option	-	disable

Parameter	Description	Type	Size	Default
	Option		Description	
	<i>enable</i>		Enable revision image backup automatically when upgrading image.	
	<i>disable</i>		Disable revision image backup automatically when upgrading image.	
revision-backup-on-logout	Enable/disable back-up of the latest configuration revision when an administrator logs out of the CLI or GUI.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable revision config backup automatically when logout.	
	<i>disable</i>		Disable revision config backup automatically when logout.	
hostname	FortiProxy unit's hostname. Most models will truncate names longer than 24 characters. Some models support hostnames up to 35 characters.	string	Maximum length: 35	
alias	Alias for your FortiProxy unit.	string	Maximum length: 35	
strong-crypto	Enable to use strong encryption and only allow strong ciphers and digest for HTTPS/SSH/TLS/SSL functions.	option	-	enable
	Option		Description	
	<i>enable</i>		Enable strong crypto for HTTPS/SSH/TLS/SSL.	
	<i>disable</i>		Disable strong crypto for HTTPS/SSH/TLS/SSL.	
ssl-static-key-ciphers	Enable/disable static key ciphers in SSL/TLS connections (e.g. AES128-SHA, AES256-SHA, AES128-SHA256, AES256-SHA256).	option	-	enable
	Option		Description	
	<i>enable</i>		Enable static key ciphers in SSL/TLS connections.	
	<i>disable</i>		Disable static key ciphers in SSL/TLS connections.	

Parameter	Description	Type	Size	Default																								
ssh-kex-algo	Select one or more SSH kex algorithms.	option	-	diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>diffie-hellman-group1-sha1</td><td>diffie-hellman-group1-sha1</td></tr><tr><td>diffie-hellman-group14-sha1</td><td>diffie-hellman-group14-sha1</td></tr><tr><td>diffie-hellman-group14-sha256</td><td>diffie-hellman-group14-sha256</td></tr><tr><td>diffie-hellman-group16-sha512</td><td>diffie-hellman-group16-sha512</td></tr><tr><td>diffie-hellman-group18-sha512</td><td>diffie-hellman-group18-sha512</td></tr><tr><td>diffie-hellman-group-exchange-sha1</td><td>diffie-hellman-group-exchange-sha1</td></tr><tr><td>diffie-hellman-group-exchange-sha256</td><td>diffie-hellman-group-exchange-sha256</td></tr><tr><td>curve25519-sha256@libssh.org</td><td>curve25519-sha256@libssh.org</td></tr><tr><td>ecdh-sha2-nistp256</td><td>ecdh-sha2-nistp256</td></tr><tr><td>ecdh-sha2-nistp384</td><td>ecdh-sha2-nistp384</td></tr><tr><td>ecdh-sha2-nistp521</td><td>ecdh-sha2-nistp521</td></tr></table>				Option	Description	diffie-hellman-group1-sha1	diffie-hellman-group1-sha1	diffie-hellman-group14-sha1	diffie-hellman-group14-sha1	diffie-hellman-group14-sha256	diffie-hellman-group14-sha256	diffie-hellman-group16-sha512	diffie-hellman-group16-sha512	diffie-hellman-group18-sha512	diffie-hellman-group18-sha512	diffie-hellman-group-exchange-sha1	diffie-hellman-group-exchange-sha1	diffie-hellman-group-exchange-sha256	diffie-hellman-group-exchange-sha256	curve25519-sha256@libssh.org	curve25519-sha256@libssh.org	ecdh-sha2-nistp256	ecdh-sha2-nistp256	ecdh-sha2-nistp384	ecdh-sha2-nistp384	ecdh-sha2-nistp521	ecdh-sha2-nistp521
Option	Description																											
diffie-hellman-group1-sha1	diffie-hellman-group1-sha1																											
diffie-hellman-group14-sha1	diffie-hellman-group14-sha1																											
diffie-hellman-group14-sha256	diffie-hellman-group14-sha256																											
diffie-hellman-group16-sha512	diffie-hellman-group16-sha512																											
diffie-hellman-group18-sha512	diffie-hellman-group18-sha512																											
diffie-hellman-group-exchange-sha1	diffie-hellman-group-exchange-sha1																											
diffie-hellman-group-exchange-sha256	diffie-hellman-group-exchange-sha256																											
curve25519-sha256@libssh.org	curve25519-sha256@libssh.org																											
ecdh-sha2-nistp256	ecdh-sha2-nistp256																											
ecdh-sha2-nistp384	ecdh-sha2-nistp384																											
ecdh-sha2-nistp521	ecdh-sha2-nistp521																											
ssh-enc-algo	Select one or more SSH ciphers.	option	-	aes256-ctr aes256-gcm@openssh.com																								

Parameter	Description	Type	Size	Default																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>chacha20-poly1305@openssh.com</i></td><td>chacha20-poly1305@openssh.com</td></tr><tr><td><i>aes128-ctr</i></td><td>aes128-ctr</td></tr><tr><td><i>aes192-ctr</i></td><td>aes192-ctr</td></tr><tr><td><i>aes256-ctr</i></td><td>aes256-ctr</td></tr><tr><td><i>arcfour256</i></td><td>arcfour256</td></tr><tr><td><i>arcfour128</i></td><td>arcfour128</td></tr><tr><td><i>aes128-cbc</i></td><td>aes128-cbc</td></tr><tr><td><i>3des-cbc</i></td><td>3des-cbc</td></tr><tr><td><i>blowfish-cbc</i></td><td>blowfish-cbc</td></tr><tr><td><i>cast128-cbc</i></td><td>cast128-cbc</td></tr><tr><td><i>aes192-cbc</i></td><td>aes192-cbc</td></tr><tr><td><i>aes256-cbc</i></td><td>aes256-cbc</td></tr><tr><td><i>arcfour</i></td><td>arcfour</td></tr><tr><td><i>rijndael-cbc@lysator.liu.se</i></td><td>rijndael-cbc@lysator.liu.se</td></tr><tr><td><i>aes128-gcm@openssh.com</i></td><td>aes128-gcm@openssh.com</td></tr><tr><td><i>aes256-gcm@openssh.com</i></td><td>aes256-gcm@openssh.com</td></tr></table>	Option	Description	<i>chacha20-poly1305@openssh.com</i>	chacha20-poly1305@openssh.com	<i>aes128-ctr</i>	aes128-ctr	<i>aes192-ctr</i>	aes192-ctr	<i>aes256-ctr</i>	aes256-ctr	<i>arcfour256</i>	arcfour256	<i>arcfour128</i>	arcfour128	<i>aes128-cbc</i>	aes128-cbc	<i>3des-cbc</i>	3des-cbc	<i>blowfish-cbc</i>	blowfish-cbc	<i>cast128-cbc</i>	cast128-cbc	<i>aes192-cbc</i>	aes192-cbc	<i>aes256-cbc</i>	aes256-cbc	<i>arcfour</i>	arcfour	<i>rijndael-cbc@lysator.liu.se</i>	rijndael-cbc@lysator.liu.se	<i>aes128-gcm@openssh.com</i>	aes128-gcm@openssh.com	<i>aes256-gcm@openssh.com</i>	aes256-gcm@openssh.com				
	Option	Description																																					
	<i>chacha20-poly1305@openssh.com</i>	chacha20-poly1305@openssh.com																																					
	<i>aes128-ctr</i>	aes128-ctr																																					
	<i>aes192-ctr</i>	aes192-ctr																																					
	<i>aes256-ctr</i>	aes256-ctr																																					
	<i>arcfour256</i>	arcfour256																																					
	<i>arcfour128</i>	arcfour128																																					
	<i>aes128-cbc</i>	aes128-cbc																																					
	<i>3des-cbc</i>	3des-cbc																																					
	<i>blowfish-cbc</i>	blowfish-cbc																																					
	<i>cast128-cbc</i>	cast128-cbc																																					
	<i>aes192-cbc</i>	aes192-cbc																																					
	<i>aes256-cbc</i>	aes256-cbc																																					
	<i>arcfour</i>	arcfour																																					
	<i>rijndael-cbc@lysator.liu.se</i>	rijndael-cbc@lysator.liu.se																																					
	<i>aes128-gcm@openssh.com</i>	aes128-gcm@openssh.com																																					
<i>aes256-gcm@openssh.com</i>	aes256-gcm@openssh.com																																						
ssh-mac-algo	Select one or more SSH MAC algorithms.	option	-	hmac-sha2-256 hmac-sha2-256-etm@openssh.com hmac-sha2-512 hmac-sha2-512-etm@openssh.com																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hmac-md5</i></td><td>hmac-md5</td></tr><tr><td><i>hmac-md5-etm@openssh.com</i></td><td>hmac-md5-etm@openssh.com</td></tr><tr><td><i>hmac-md5-96</i></td><td>hmac-md5-96</td></tr><tr><td><i>hmac-md5-96-etm@openssh.com</i></td><td>hmac-md5-96-etm@openssh.com</td></tr></table>	Option	Description	<i>hmac-md5</i>	hmac-md5	<i>hmac-md5-etm@openssh.com</i>	hmac-md5-etm@openssh.com	<i>hmac-md5-96</i>	hmac-md5-96	<i>hmac-md5-96-etm@openssh.com</i>	hmac-md5-96-etm@openssh.com																												
	Option	Description																																					
	<i>hmac-md5</i>	hmac-md5																																					
	<i>hmac-md5-etm@openssh.com</i>	hmac-md5-etm@openssh.com																																					
	<i>hmac-md5-96</i>	hmac-md5-96																																					
<i>hmac-md5-96-etm@openssh.com</i>	hmac-md5-96-etm@openssh.com																																						

Parameter	Description	Type	Size	Default																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hmac-sha1</i></td><td>hmac-sha1</td></tr><tr><td><i>hmac-sha1-etm@openssh.com</i></td><td>hmac-sha1-etm@openssh.com</td></tr><tr><td><i>hmac-sha2-256</i></td><td>hmac-sha2-256</td></tr><tr><td><i>hmac-sha2-256-etm@openssh.com</i></td><td>hmac-sha2-256-etm@openssh.com</td></tr><tr><td><i>hmac-sha2-512</i></td><td>hmac-sha2-512</td></tr><tr><td><i>hmac-sha2-512-etm@openssh.com</i></td><td>hmac-sha2-512-etm@openssh.com</td></tr><tr><td><i>hmac-ripemd160</i></td><td>hmac-ripemd160</td></tr><tr><td><i>hmac-ripemd160@openssh.com</i></td><td>hmac-ripemd160@openssh.com</td></tr><tr><td><i>hmac-ripemd160-etm@openssh.com</i></td><td>hmac-ripemd160-etm@openssh.com</td></tr><tr><td><i>umac-64@openssh.com</i></td><td>umac-64@openssh.com</td></tr><tr><td><i>umac-128@openssh.com</i></td><td>umac-128@openssh.com</td></tr><tr><td><i>umac-64-etm@openssh.com</i></td><td>umac-64-etm@openssh.com</td></tr><tr><td><i>umac-128-etm@openssh.com</i></td><td>umac-128-etm@openssh.com</td></tr></table>	Option	Description	<i>hmac-sha1</i>	hmac-sha1	<i>hmac-sha1-etm@openssh.com</i>	hmac-sha1-etm@openssh.com	<i>hmac-sha2-256</i>	hmac-sha2-256	<i>hmac-sha2-256-etm@openssh.com</i>	hmac-sha2-256-etm@openssh.com	<i>hmac-sha2-512</i>	hmac-sha2-512	<i>hmac-sha2-512-etm@openssh.com</i>	hmac-sha2-512-etm@openssh.com	<i>hmac-ripemd160</i>	hmac-ripemd160	<i>hmac-ripemd160@openssh.com</i>	hmac-ripemd160@openssh.com	<i>hmac-ripemd160-etm@openssh.com</i>	hmac-ripemd160-etm@openssh.com	<i>umac-64@openssh.com</i>	umac-64@openssh.com	<i>umac-128@openssh.com</i>	umac-128@openssh.com	<i>umac-64-etm@openssh.com</i>	umac-64-etm@openssh.com	<i>umac-128-etm@openssh.com</i>	umac-128-etm@openssh.com				
	Option	Description																															
	<i>hmac-sha1</i>	hmac-sha1																															
	<i>hmac-sha1-etm@openssh.com</i>	hmac-sha1-etm@openssh.com																															
	<i>hmac-sha2-256</i>	hmac-sha2-256																															
	<i>hmac-sha2-256-etm@openssh.com</i>	hmac-sha2-256-etm@openssh.com																															
	<i>hmac-sha2-512</i>	hmac-sha2-512																															
	<i>hmac-sha2-512-etm@openssh.com</i>	hmac-sha2-512-etm@openssh.com																															
	<i>hmac-ripemd160</i>	hmac-ripemd160																															
	<i>hmac-ripemd160@openssh.com</i>	hmac-ripemd160@openssh.com																															
	<i>hmac-ripemd160-etm@openssh.com</i>	hmac-ripemd160-etm@openssh.com																															
	<i>umac-64@openssh.com</i>	umac-64@openssh.com																															
	<i>umac-128@openssh.com</i>	umac-128@openssh.com																															
	<i>umac-64-etm@openssh.com</i>	umac-64-etm@openssh.com																															
<i>umac-128-etm@openssh.com</i>	umac-128-etm@openssh.com																																
snat-route-change	Enable/disable the ability to change the source NAT route.	option	-	disable																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SNAT route change.</td></tr><tr><td><i>disable</i></td><td>Disable SNAT route change.</td></tr></table>	Option	Description	<i>enable</i>	Enable SNAT route change.	<i>disable</i>	Disable SNAT route change.																										
	Option	Description																															
	<i>enable</i>	Enable SNAT route change.																															
<i>disable</i>	Disable SNAT route change.																																
speedtest-server	Enable/disable speed test server.	option	-	disable																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable speed test server service.</td></tr><tr><td><i>disable</i></td><td>Disable speed test server service.</td></tr></table>	Option	Description	<i>enable</i>	Enable speed test server service.	<i>disable</i>	Disable speed test server service.																										
	Option	Description																															
	<i>enable</i>	Enable speed test server service.																															
<i>disable</i>	Disable speed test server service.																																

Parameter	Description	Type	Size	Default																
cli-audit-log	Enable/disable CLI audit log.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable CLI audit log.</td></tr><tr><td><i>disable</i></td><td>Disable CLI audit log.</td></tr></table>	Option	Description	<i>enable</i>	Enable CLI audit log.	<i>disable</i>	Disable CLI audit log.													
Option	Description																			
<i>enable</i>	Enable CLI audit log.																			
<i>disable</i>	Disable CLI audit log.																			
dh-params	Number of bits to use in the Diffie-Hellman exchange for HTTPS/SSH protocols.	option	-	2048																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>1024</i></td><td>1024 bits.</td></tr><tr><td><i>1536</i></td><td>1536 bits.</td></tr><tr><td><i>2048</i></td><td>2048 bits.</td></tr><tr><td><i>3072</i></td><td>3072 bits.</td></tr><tr><td><i>4096</i></td><td>4096 bits.</td></tr><tr><td><i>6144</i></td><td>6144 bits.</td></tr><tr><td><i>8192</i></td><td>8192 bits.</td></tr></table>	Option	Description	<i>1024</i>	1024 bits.	<i>1536</i>	1536 bits.	<i>2048</i>	2048 bits.	<i>3072</i>	3072 bits.	<i>4096</i>	4096 bits.	<i>6144</i>	6144 bits.	<i>8192</i>	8192 bits.			
Option	Description																			
<i>1024</i>	1024 bits.																			
<i>1536</i>	1536 bits.																			
<i>2048</i>	2048 bits.																			
<i>3072</i>	3072 bits.																			
<i>4096</i>	4096 bits.																			
<i>6144</i>	6144 bits.																			
<i>8192</i>	8192 bits.																			
fds-statistics	Enable/disable sending IPS, Application Control, and AntiVirus data to FortiGuard. This data is used to improve FortiGuard services and is not shared with external parties and is protected by Fortinet's privacy policy.	option	-	enable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiGuard statistics.</td></tr><tr><td><i>disable</i></td><td>Disable FortiGuard statistics.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiGuard statistics.	<i>disable</i>	Disable FortiGuard statistics.													
Option	Description																			
<i>enable</i>	Enable FortiGuard statistics.																			
<i>disable</i>	Disable FortiGuard statistics.																			
fds-statistics-period	FortiGuard statistics collection period in minutes.	integer	Minimum value: 1 Maximum value: 1440	60																
tcp-option	Enable SACK, timestamp and MSS TCP options.	option	-	enable																

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable TCP option.		
	<i>disable</i>	Disable TCP option.		
lldp-transmission	Enable/disable Link Layer Discovery Protocol (LLDP) transmission.	option	-	disable
	Option Description			
	<i>enable</i>	Enable transmission of Link Layer Discovery Protocol (LLDP).		
	<i>disable</i>	Disable transmission of Link Layer Discovery Protocol (LLDP).		
lldp-reception	Enable/disable Link Layer Discovery Protocol (LLDP) reception.	option	-	disable
	Option Description			
	<i>enable</i>	Enable reception of Link Layer Discovery Protocol (LLDP).		
	<i>disable</i>	Disable reception of Link Layer Discovery Protocol (LLDP).		
proxy-auth-timeout	Authentication timeout in minutes for authenticated users.	integer	Minimum value: 1 Maximum value: 600	10
resigned-pkey-period	Resigned cert private key regeneration period in hours.	integer	Minimum value: 0 Maximum value: 600	0
proxy-keep-alive-mode	Control if users must re-authenticate after a session is closed, traffic has been idle, or from the point at which the user was authenticated.	option	-	session
	Option Description			
	<i>session</i>	Proxy keep-alive timeout begins at the closure of the session.		
	<i>traffic</i>	Proxy keep-alive timeout begins after traffic has not been received.		
	<i>re-authentication</i>	Proxy keep-alive timeout begins when the user was authenticated.		

Parameter	Description	Type	Size	Default						
proxy-re-authentication-time	The time limit that users must re-authenticate if proxy-keep-alive-mode is set to re-authenticate (1 - 86400 sec, default=30s.	integer	Minimum value: 1 Maximum value: 86400	30						
proxy-auth-lifetime	Enable/disable authenticated users lifetime control. This is a cap on the total time a proxy user can be authenticated for after which re-authentication will take place.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable authenticated users lifetime control.</td></tr><tr><td><i>disable</i></td><td>Disable authenticated users lifetime control.</td></tr></table>				Option	Description	<i>enable</i>	Enable authenticated users lifetime control.	<i>disable</i>	Disable authenticated users lifetime control.
Option	Description									
<i>enable</i>	Enable authenticated users lifetime control.									
<i>disable</i>	Disable authenticated users lifetime control.									
proxy-auth-lifetime-timeout	Lifetime timeout in minutes for authenticated users.	integer	Minimum value: 5 Maximum value: 65535	480						
proxy-auth-machine-timeout	Machine account timeout in seconds for authenticated machines.	integer	Minimum value: 5 Maximum value: 30	15						
proxy-resource-mode	Enable/disable use of the maximum memory usage on the FortiProxy unit's proxy processing of resources, such as block lists, allow lists, and external resources.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of the maximum memory usage.</td></tr><tr><td><i>disable</i></td><td>Disable use of the maximum memory usage.</td></tr></table>				Option	Description	<i>enable</i>	Enable use of the maximum memory usage.	<i>disable</i>	Disable use of the maximum memory usage.
Option	Description									
<i>enable</i>	Enable use of the maximum memory usage.									
<i>disable</i>	Disable use of the maximum memory usage.									
proxy-cert-use-mgmt-vdom	Enable/disable using management VDOM to send requests.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
update-tls-finger-print	Enable/disable update TLS fingerprint when deep-inspection is enabled.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
sys-perf-log-interval	Time in minutes between updates of performance statistics logging.	integer	Minimum value: 0 Maximum value: 15	5						
check-protocol-header	Level of checking performed on protocol headers. Strict checking is more thorough but may affect performance. Loose checking is OK in most cases.	option	-	loose						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>loose</i></td><td>Check protocol header loosely.</td></tr><tr><td><i>strict</i></td><td>Check protocol header strictly.</td></tr></table>	Option	Description	<i>loose</i>	Check protocol header loosely.	<i>strict</i>	Check protocol header strictly.			
Option	Description									
<i>loose</i>	Check protocol header loosely.									
<i>strict</i>	Check protocol header strictly.									
vip-arp-range	Controls the number of ARPs that the FortiProxy sends for a Virtual IP (VIP) address range.	option	-	restricted						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>unlimited</i></td><td>Send ARPs for all addresses in VIP range.</td></tr><tr><td><i>restricted</i></td><td>Send ARPs for the first 8192 addresses in VIP range.</td></tr></table>	Option	Description	<i>unlimited</i>	Send ARPs for all addresses in VIP range.	<i>restricted</i>	Send ARPs for the first 8192 addresses in VIP range.			
Option	Description									
<i>unlimited</i>	Send ARPs for all addresses in VIP range.									
<i>restricted</i>	Send ARPs for the first 8192 addresses in VIP range.									
tcp-halfclose-timer	Number of seconds the FortiProxy unit should wait to close a session after one peer has sent a FIN packet but the other has not responded.	integer	Minimum value: 1 Maximum value: 86400	120						
tcp-halfopen-timer	Number of seconds the FortiProxy unit should wait to close a session after one peer has sent an open session packet but the other has not responded.	integer	Minimum value: 1 Maximum value: 86400	10						

Parameter	Description	Type	Size	Default						
tcp-timewait-timer	Length of the TCP TIME-WAIT state in seconds.	integer	Minimum value: 0 Maximum value: 300	1						
tcp-rst-timer	Length of the TCP CLOSE state in seconds.	integer	Minimum value: 5 Maximum value: 300	5						
udp-idle-timer	UDP connection session timeout. This command can be useful in managing CPU and memory resources.	integer	Minimum value: 1 Maximum value: 86400	180						
block-session-timer	Duration in seconds for blocked sessions.	integer	Minimum value: 1 Maximum value: 300	30						
ip-src-port-range	IP source port range used for traffic originating from the FortiProxy unit.	user	Not Specified	1024-65001						
pre-login-banner	Enable/disable displaying the administrator access disclaimer message on the login page before an administrator logs in.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable pre-login banner.</td></tr><tr><td>disable</td><td>Disable pre-login banner.</td></tr></table>				Option	Description	enable	Enable pre-login banner.	disable	Disable pre-login banner.
Option	Description									
enable	Enable pre-login banner.									
disable	Disable pre-login banner.									
post-login-banner	Enable/disable displaying the administrator access disclaimer message after an administrator successfully logs in.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable post-login banner.</td></tr><tr><td>enable</td><td>Enable post-login banner.</td></tr></table>				Option	Description	disable	Disable post-login banner.	enable	Enable post-login banner.
Option	Description									
disable	Disable post-login banner.									
enable	Enable post-login banner.									
tftp	Enable/disable TFTP.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable TFTP.</td></tr><tr><td>disable</td><td>Disable TFTP.</td></tr></table>				Option	Description	enable	Enable TFTP.	disable	Disable TFTP.
Option	Description									
enable	Enable TFTP.									
disable	Disable TFTP.									

Parameter	Description	Type	Size	Default								
av-failopen	Set the action to take if the FortiProxy is running low on memory or the proxy connection limit has been reached.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Bypass the antivirus system when memory is low. Antivirus scanning resumes when the low memory condition is resolved.</td></tr><tr><td><i>off</i></td><td>Stop accepting new AV sessions when entering conserve mode, but continue to process current active sessions.</td></tr><tr><td><i>one-shot</i></td><td>Bypass the antivirus system when memory is low.</td></tr></table>	Option	Description	<i>pass</i>	Bypass the antivirus system when memory is low. Antivirus scanning resumes when the low memory condition is resolved.	<i>off</i>	Stop accepting new AV sessions when entering conserve mode, but continue to process current active sessions.	<i>one-shot</i>	Bypass the antivirus system when memory is low.			
Option	Description											
<i>pass</i>	Bypass the antivirus system when memory is low. Antivirus scanning resumes when the low memory condition is resolved.											
<i>off</i>	Stop accepting new AV sessions when entering conserve mode, but continue to process current active sessions.											
<i>one-shot</i>	Bypass the antivirus system when memory is low.											
av-failopen-session	When enabled and a proxy for a protocol runs out of room in its session table, that protocol goes into failopen mode and enacts the action specified by av-failopen.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AV fail open session option.</td></tr><tr><td><i>disable</i></td><td>Disable AV fail open session option.</td></tr></table>	Option	Description	<i>enable</i>	Enable AV fail open session option.	<i>disable</i>	Disable AV fail open session option.					
Option	Description											
<i>enable</i>	Enable AV fail open session option.											
<i>disable</i>	Disable AV fail open session option.											
kernel-panic-timeout	Reboot timeout after kernel panic in seconds. Value of 0 means do not reboot.	integer	Minimum value: 0 Maximum value: 3600	5								
kernel-panic-debug	Enable/disable kernel panic debug messages.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable kernel panic debug messages.</td></tr><tr><td><i>disable</i></td><td>Disable kernel panic debug messages.</td></tr></table>	Option	Description	<i>enable</i>	Enable kernel panic debug messages.	<i>disable</i>	Disable kernel panic debug messages.					
Option	Description											
<i>enable</i>	Enable kernel panic debug messages.											
<i>disable</i>	Disable kernel panic debug messages.											
memory-use-threshold-extreme	Threshold at which memory usage is considered extreme.	integer	Minimum value: 70 Maximum value: 97	95								
memory-use-threshold-red	Threshold at which memory usage forces the FortiProxy to enter conserve mode.	integer	Minimum value: 70 Maximum value: 97	88								

Parameter	Description	Type	Size	Default						
memory-use-threshold-green	Threshold at which memory usage forces the FortiProxy to exit conserve mode.	integer	Minimum value: 70 Maximum value: 97	82						
ip-fragment-mem-thresholds	Maximum memory (MB) used to reassemble IPv4/IPv6 fragments.	integer	Minimum value: 32 Maximum value: 2047	32						
cpu-use-threshold	Threshold at which CPU usage is reported.	integer	Minimum value: 50 Maximum value: 99	90						
log-single-cpu-high	Enable/disable logging the event of a single CPU core reaching CPU usage threshold.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging the event of a single CPU core reaching CPU usage threshold.</td></tr><tr><td><i>disable</i></td><td>Disable logging the event of a single CPU core reaching CPU usage threshold.</td></tr></table>				Option	Description	<i>enable</i>	Enable logging the event of a single CPU core reaching CPU usage threshold.	<i>disable</i>	Disable logging the event of a single CPU core reaching CPU usage threshold.
Option	Description									
<i>enable</i>	Enable logging the event of a single CPU core reaching CPU usage threshold.									
<i>disable</i>	Disable logging the event of a single CPU core reaching CPU usage threshold.									
check-reset-range	Configure ICMP error message verification. You can either apply strict RST range checking or disable it.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>strict</i></td><td>Check RST range strictly.</td></tr><tr><td><i>disable</i></td><td>Disable RST range check.</td></tr></table>				Option	Description	<i>strict</i>	Check RST range strictly.	<i>disable</i>	Disable RST range check.
Option	Description									
<i>strict</i>	Check RST range strictly.									
<i>disable</i>	Disable RST range check.									
admin-port	Administrative access port for HTTP.	integer	Minimum value: 1 Maximum value: 65535	80						
admin-sport	Administrative access port for HTTPS.	integer	Minimum value: 1 Maximum value: 65535	443						
admin-host	Administrative host for HTTP and HTTPS. When set, will be used in lieu of the client's Host header for any redirection.	string	Maximum length: 255							

Parameter	Description	Type	Size	Default
admin-https-redirect	Enable/disable redirection of HTTP administration access to HTTPS.	option	-	enable
	Option Description			
	<i>enable</i>	Enable redirecting HTTP administration access to HTTPS.		
	<i>disable</i>	Disable redirecting HTTP administration access to HTTPS.		
admin-hsts-max-age	HTTPS Strict-Transport-Security header max-age in seconds. A value of 0 will reset any HSTS records in the browser. When admin-https-redirect is disabled the header max-age will be 0.	integer	Minimum value: 0 Maximum value: 2147483647	15552000
admin-ssh-password	Enable/disable password authentication for SSH admin access.	option	-	enable
	Option Description			
	<i>enable</i>	Enable password authentication for SSH admin access.		
	<i>disable</i>	Disable password authentication for SSH admin access.		
admin-restrict-local	Enable/disable local admin authentication restriction when remote authenticator is up and running.	option	-	disable
	Option Description			
	<i>enable</i>	Enable local admin authentication restriction.		
	<i>disable</i>	Disable local admin authentication restriction.		
admin-ssh-port	Administrative access port for SSH.	integer	Minimum value: 22 Maximum value: 65535	22
admin-ssh-grace-time	Maximum time in seconds permitted between making an SSH connection to the FortiProxy unit and authenticating.	integer	Minimum value: 10 Maximum value: 3600	120
admin-ssh-v1	Enable/disable SSH v1 compatibility.	option	-	disable

Parameter	Description	Type	Size	Default
	Option		Description	
	<i>enable</i>	Enable SSH v1 compatibility.		
	<i>disable</i>	Disable SSH v1 compatibility.		
admin-telnet	Enable/disable TELNET service.	option	-	enable
	Option		Description	
	<i>enable</i>	Enable TELNET service.		
	<i>disable</i>	Disable TELNET service.		
admin-telnet-port	Administrative access port for TELNET.	integer	Minimum value: 1 Maximum value: 65535	23
admin-forticloud-ssologin	Enable/disable FortiCloud admin login via SSO.	option	-	disable
	Option		Description	
	<i>enable</i>	Enable FortiCloud admin login via SSO.		
	<i>disable</i>	Disable FortiCloud admin login via SSO.		
admin-forticloud-ssodefault-profile	Override access profile.	string	Maximum length: 35	
default-service-source-port	Default service source port range.	user	Not Specified	
admin-server-cert	Server certificate that the FortiProxy uses for HTTPS administrative connections.	string	Maximum length: 35	Fortinet_GUI_Server
admin-https-pki-required	Enable/disable admin login method. Enable to force administrators to provide a valid certificate to log in if PKI is enabled. Disable to allow administrators to log in with a certificate or password.	option	-	disable
	Option		Description	
	<i>enable</i>	Admin users must provide a valid certificate when PKI is enabled for HTTPS admin access.		
	<i>disable</i>	Admin users can login by providing a valid certificate or password.		

Parameter	Description	Type	Size	Default
auth-http-port	User authentication HTTP port.	integer	Minimum value: 1 Maximum value: 65535	1000
auth-https-port	User authentication HTTPS port.	integer	Minimum value: 1 Maximum value: 65535	1003
auth-ike-saml-port	User IKE SAML authentication port.	integer	Minimum value: 0 Maximum value: 65535	1001
auth-keepalive	Enable to prevent user authentication sessions from timing out when idle.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable use of keep alive to extend authentication.	
	<i>disable</i>		Disable use of keep alive to extend authentication.	
policy-auth-concurrent	Number of concurrent firewall use logins from the same user.	integer	Minimum value: 0 Maximum value: 100	0
auth-session-limit	Action to take when the number of allowed user authenticated sessions is reached.	option	-	block-new
	Option		Description	
	<i>block-new</i>		Block new user authentication attempts.	
	<i>logout-inactive</i>		Logout the most inactive user authenticated sessions.	
auth-cert	Server certificate that the FortiProxy uses for HTTPS firewall authentication connections.	string	Maximum length: 35	Fortinet_Factory
clt-cert-req	Enable/disable requiring administrators to have a client certificate to log into the GUI using HTTPS.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable require client certificate for GUI login.	
	<i>disable</i>		Disable require client certificate for GUI login.	

Parameter	Description	Type	Size	Default								
fortiservice-port	FortiService port. Used by FortiClient endpoint compliance. Older versions of FortiClient used a different port.	integer	Minimum value: 1 Maximum value: 65535	8013								
cfg-save	Configuration file save mode for CLI changes.	option	-	automatic								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>automatic</i></td><td>Automatically save config.</td></tr><tr><td><i>manual</i></td><td>Manually save config.</td></tr><tr><td><i>revert</i></td><td>Manually save config and revert the config when timeout.</td></tr></table>	Option	Description	<i>automatic</i>	Automatically save config.	<i>manual</i>	Manually save config.	<i>revert</i>	Manually save config and revert the config when timeout.			
Option	Description											
<i>automatic</i>	Automatically save config.											
<i>manual</i>	Manually save config.											
<i>revert</i>	Manually save config and revert the config when timeout.											
cfg-revert-timeout	Time-out for reverting to the last saved configuration.	integer	Minimum value: 10 Maximum value: 4294967295	600								
reboot-upon-config-restore	Enable/disable reboot of system upon restoring configuration.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable reboot of system upon restoring configuration.</td></tr><tr><td><i>disable</i></td><td>Disable reboot of system upon restoring configuration.</td></tr></table>	Option	Description	<i>enable</i>	Enable reboot of system upon restoring configuration.	<i>disable</i>	Disable reboot of system upon restoring configuration.					
Option	Description											
<i>enable</i>	Enable reboot of system upon restoring configuration.											
<i>disable</i>	Disable reboot of system upon restoring configuration.											
admin-scp	Enable/disable using SCP to download the system configuration. You can use SCP as an alternative method for backing up the configuration.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable allow system configuration download by SCP.</td></tr><tr><td><i>disable</i></td><td>Disable allow system configuration download by SCP.</td></tr></table>	Option	Description	<i>enable</i>	Enable allow system configuration download by SCP.	<i>disable</i>	Disable allow system configuration download by SCP.					
Option	Description											
<i>enable</i>	Enable allow system configuration download by SCP.											
<i>disable</i>	Disable allow system configuration download by SCP.											
security-rating-result-submission	Enable/disable the submission of Security Rating results to FortiGuard.	option	-	enable								

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable submission of Security Rating results to FortiGuard.		
	<i>disable</i>	Disable submission of Security Rating results to FortiGuard.		
security-rating-run-on-schedule	Enable/disable scheduled runs of Security Rating.	option	-	enable
	Option Description			
	<i>enable</i>	Enable scheduled runs of Security Rating.		
	<i>disable</i>	Disable scheduled runs of Security Rating.		
fortiextender-data-port	FortiExtender data port.	integer	Minimum value: 1024 Maximum value: 49150	25246
fortiextender	Enable/disable FortiExtender.	option	-	disable
	Option Description			
	<i>disable</i>	Disable FortiExtender controller.		
	<i>enable</i>	Enable FortiExtender controller.		
extender-controller-reserved-network	Configure reserved network subnet for managed LAN extension FortiExtender units. This is available when the FortiExtender daemon is running.	ipv4-classnet-host	Not Specified	10.252.0.1 255.255.0.0
fortiextender-discovery-lockdown	Enable/disable FortiExtender CAPWAP lockdown.	option	-	disable
	Option Description			
	<i>disable</i>	Unlock down new FortiExtender device discovery.		
	<i>enable</i>	Lock down new FortiExtender device discovery.		
fortiextender-provision-on-authorization	Enable/disable automatic provisioning of latest FortiExtender firmware on authorization.	option	-	disable
	Option Description			
	<i>enable</i>	Enable FortiExtender firmware provision on authorization.		
	<i>disable</i>	Disable FortiExtender firmware provision on authorization.		

Parameter	Description	Type	Size	Default														
dnsproxy-worker-count	DNS proxy worker count. For a FortiGate with multiple logical CPUs, you can set the DNS process number from 1 to the number of logical CPUs.	integer	Minimum value: 1 Maximum value: 255	1														
url-filter-count	URL filter daemon count.	integer	Minimum value: 1 Maximum value: 10	1														
proxy-worker-count	Proxy worker count.	integer	Minimum value: 1 Maximum value: 255	0														
scanunit-count	Number of scanunits. The range and the default depend on the number of CPUs. Only available on FortiProxy units with multiple CPUs.	integer	Minimum value: 2 Maximum value: 255	0														
fgd-alert-subscription	Type of alert to retrieve from FortiGuard.	option	-															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>advisory</i></td><td>Retrieve FortiGuard advisories, report and news alerts.</td></tr><tr><td><i>latest-threat</i></td><td>Retrieve latest FortiGuard threats alerts.</td></tr><tr><td><i>latest-virus</i></td><td>Retrieve latest FortiGuard virus alerts.</td></tr><tr><td><i>latest-attack</i></td><td>Retrieve latest FortiGuard attack alerts.</td></tr><tr><td><i>new-antivirus-db</i></td><td>Retrieve FortiGuard AV database release alerts.</td></tr><tr><td><i>new-attack-db</i></td><td>Retrieve FortiGuard IPS database release alerts.</td></tr></table>				Option	Description	<i>advisory</i>	Retrieve FortiGuard advisories, report and news alerts.	<i>latest-threat</i>	Retrieve latest FortiGuard threats alerts.	<i>latest-virus</i>	Retrieve latest FortiGuard virus alerts.	<i>latest-attack</i>	Retrieve latest FortiGuard attack alerts.	<i>new-antivirus-db</i>	Retrieve FortiGuard AV database release alerts.	<i>new-attack-db</i>	Retrieve FortiGuard IPS database release alerts.
Option	Description																	
<i>advisory</i>	Retrieve FortiGuard advisories, report and news alerts.																	
<i>latest-threat</i>	Retrieve latest FortiGuard threats alerts.																	
<i>latest-virus</i>	Retrieve latest FortiGuard virus alerts.																	
<i>latest-attack</i>	Retrieve latest FortiGuard attack alerts.																	
<i>new-antivirus-db</i>	Retrieve FortiGuard AV database release alerts.																	
<i>new-attack-db</i>	Retrieve FortiGuard IPS database release alerts.																	
ipv6-accept-dad	Enable/disable acceptance of IPv6 Duplicate Address Detection (DAD).	integer	Minimum value: 0 Maximum value: 2	1														
ipv6-allow-multicast-probe	Enable/disable IPv6 address probe through Multicast.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable probing of IPv6 address space through Multicast.</td></tr><tr><td><i>disable</i></td><td>Disable probing of IPv6 address space through Multicast.</td></tr></table>				Option	Description	<i>enable</i>	Enable probing of IPv6 address space through Multicast.	<i>disable</i>	Disable probing of IPv6 address space through Multicast.								
Option	Description																	
<i>enable</i>	Enable probing of IPv6 address space through Multicast.																	
<i>disable</i>	Disable probing of IPv6 address space through Multicast.																	

Parameter	Description	Type	Size	Default
ipv6-allow-local-in-silent-drop	Enable/disable silent drop of IPv6 local-in traffic.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable silent drop of IPv6 local-in traffic.		
	<i>disable</i>	Disable silent drop of IPv6 local-in traffic.		
csr-ca-attribute	Enable/disable the CA attribute in certificates. Some CA servers reject CSRs that have the CA attribute.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable CA attribute in CSR.		
	<i>disable</i>	Disable CA attribute in CSR.		
wimax-4g-usb	Enable/disable comparability with WiMAX 4G USB devices.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable WiMax 4G.		
	<i>disable</i>	Disable WiMax 4G.		
cert-chain-max	Maximum number of certificates that can be traversed in a certificate chain.	integer	Minimum value: 1 Maximum value: 2147483647	8
two-factor-ftk-expiry	FortiToken authentication session timeout.	integer	Minimum value: 60 Maximum value: 600	60
two-factor-email-expiry	Email-based two-factor authentication session timeout.	integer	Minimum value: 30 Maximum value: 300	60
two-factor-sms-expiry	SMS-based two-factor authentication session timeout.	integer	Minimum value: 30 Maximum value: 300	60
two-factor-fac-expiry	FortiAuthenticator token authentication session timeout.	integer	Minimum value: 10 Maximum value: 3600	60

Parameter	Description	Type	Size	Default						
two-factor-ftm-expiry	FortiToken Mobile session timeout.	integer	Minimum value: 1 Maximum value: 168	72						
max-img-cache-size	Maximum space (MB) can be used by image-analyzer to store blocked images into ram disk.	integer	Minimum value: 30 Maximum value: 300	60						
img-cache-mode	Select image cache mode for image-analyzer	option	-	rolling						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>stop</td><td>Stop caching blocked images into ram disk when limit reaches.</td></tr><tr><td>rolling</td><td>Evict old cached images when limit reaches.</td></tr></table>	Option	Description	stop	Stop caching blocked images into ram disk when limit reaches.	rolling	Evict old cached images when limit reaches.			
Option	Description									
stop	Stop caching blocked images into ram disk when limit reaches.									
rolling	Evict old cached images when limit reaches.									
per-user-bal	Enable/disable per-user block/allow list filter.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable per-user block/allow list filter.</td></tr><tr><td>disable</td><td>Disable per-user block/allow list filter.</td></tr></table>	Option	Description	enable	Enable per-user block/allow list filter.	disable	Disable per-user block/allow list filter.			
Option	Description									
enable	Enable per-user block/allow list filter.									
disable	Disable per-user block/allow list filter.									
wad-worker-count	Number of explicit proxy WAN optimization daemon (WAD) processes. By default WAN optimization, explicit proxy, and web caching is handled by all of the CPU cores in a FortiProxy unit.	integer	Minimum value: 0 Maximum value: 255	0						
wad-csvc-cs-count	Number of concurrent WAD-cache-service object-cache processes.	integer	Minimum value: 1 Maximum value: 1	1						
wad-csvc-db-count	Number of concurrent WAD-cache-service byte-cache processes.	integer	Minimum value: 0 Maximum value: 255	0						
http-view	Enable/disable logging and viewing of HTTP/S cache traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable logging and viewing of HTTP/S cache traffic.</td></tr><tr><td>disable</td><td>Disable logging and viewing of HTTP/S cache traffic.</td></tr></table>	Option	Description	enable	Enable logging and viewing of HTTP/S cache traffic.	disable	Disable logging and viewing of HTTP/S cache traffic.			
Option	Description									
enable	Enable logging and viewing of HTTP/S cache traffic.									
disable	Disable logging and viewing of HTTP/S cache traffic.									

Parameter	Description	Type	Size	Default						
wad-source-affinity	Enable/disable dispatching traffic to WAD workers based on source affinity.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable dispatching traffic to WAD workers based on source affinity.</td></tr><tr><td><i>enable</i></td><td>Enable dispatching traffic to WAD workers based on source affinity.</td></tr></table>	Option	Description	<i>disable</i>	Disable dispatching traffic to WAD workers based on source affinity.	<i>enable</i>	Enable dispatching traffic to WAD workers based on source affinity.			
Option	Description									
<i>disable</i>	Disable dispatching traffic to WAD workers based on source affinity.									
<i>enable</i>	Enable dispatching traffic to WAD workers based on source affinity.									
wad-memory-change-granularity	Minimum percentage change in system memory usage detected by the wad daemon prior to adjusting TCP window size for any active connection.	integer	Minimum value: 5 Maximum value: 25	10						
login-timestamp	Enable/disable login time recording.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable login time recording.</td></tr><tr><td><i>disable</i></td><td>Disable login time recording.</td></tr></table>	Option	Description	<i>enable</i>	Enable login time recording.	<i>disable</i>	Disable login time recording.			
Option	Description									
<i>enable</i>	Enable login time recording.									
<i>disable</i>	Disable login time recording.									
miglogd-children	Number of logging (miglogd) processes to be allowed to run. Higher number can reduce performance; lower number can slow log processing time. No logs will be dropped or lost if the number is changed.	integer	Minimum value: 0 Maximum value: 15	0						
special-file-23-support	Enable/disable detection of those special format files when using Data Leak Prevention.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable detection of those special format files when using Data Leak Prevention.</td></tr><tr><td><i>enable</i></td><td>Enable detection of those special format files when using Data Leak Prevention.</td></tr></table>	Option	Description	<i>disable</i>	Disable detection of those special format files when using Data Leak Prevention.	<i>enable</i>	Enable detection of those special format files when using Data Leak Prevention.			
Option	Description									
<i>disable</i>	Disable detection of those special format files when using Data Leak Prevention.									
<i>enable</i>	Enable detection of those special format files when using Data Leak Prevention.									
log-uuid-address	Enable/disable insertion of address UUIDs to traffic logs.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable insertion of address UUID to traffic logs.		
	<i>disable</i>	Disable insertion of address UUID to traffic logs.		
log-ssl-connection	Enable/disable logging of SSL connection events.	option	-	disable
	Option Description			
	<i>enable</i>	Enable logging of SSL connection events.		
	<i>disable</i>	Disable logging of SSL connection events.		
gui-rest-api-cache	Enable/disable REST API result caching on FortiProxy.	option	-	enable
	Option Description			
	<i>enable</i>	Enable REST API result caching on FortiProxy.		
	<i>disable</i>	Disable REST API result caching on FortiProxy.		
gui-fortiguard-resource-fetch	Enable/disable retrieving static GUI resources from FortiGuard. Disabling it will improve GUI load time for air-gapped environments.	option	-	enable
	Option Description			
	<i>enable</i>	Enable retrieving static GUI resources from FortiGuard.		
	<i>disable</i>	Disable retrieving static GUI resources from FortiGuard.		
arp-max-entry	Maximum number of dynamically learned MAC addresses that can be added to the ARP table.	integer	Minimum value: 131072 Maximum value: 2147483647	131072
ha-affinity	Affinity setting for HA daemons (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxx).	string	Maximum length: 79	1
cmdbsvr-affinity	Affinity setting for cmdbsvr (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxx).	string	Maximum length: 79	1

Parameter	Description	Type	Size	Default
av-affinity	Affinity setting for AV scanning (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxx).	string	Maximum length: 79	0
wad-affinity	Affinity setting for wad (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxx).	string	Maximum length: 79	0
ips-affinity	Affinity setting for IPS (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxx; allowed CPUs must be less than total number of IPS engine daemons).	string	Maximum length: 79	0
miglog-affinity	Affinity setting for logging (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxx).	string	Maximum length: 79	0
syslog-affinity	Affinity setting for syslog (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxx).	string	Maximum length: 79	0
url-filter-affinity	URL filter CPU affinity.	string	Maximum length: 79	0
ndp-max-entry	Maximum number of NDP table entries (set to 65,536 or higher; if set to 0, kernel holds 65,536 entries).	integer	Minimum value: 65536 Maximum value: 2147483647	0
br-fdb-max-entry	Maximum number of bridge forwarding database (FDB) entries.	integer	Minimum value: 8192 Maximum value: 2147483647	8192
max-route-cache-size	Maximum number of IP route cache entries.	integer	Minimum value: 0 Maximum value: 2147483647	0
ipsec-round-robin	Enable/disable round-robin redistribution to multiple CPUs for IPsec VPN traffic.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable round-robin redistribution for IPsec VPN.		
	<i>disable</i>	Disable round-robin redistribution for IPsec VPN.		
ipsec-soft-dec-async	Enable/disable software decryption asynchronization (using multiple CPUs to do decryption) for IPsec VPN traffic.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable software decryption asynchronization for IPsec VPN.		
	<i>disable</i>	Disable software decryption asynchronization for IPsec VPN.		
device-idle-timeout	Time in seconds that a device must be idle to automatically log the device user out.	integer	Minimum value: 30 Maximum value: 31536000	300
user-device-store-max-devices	Maximum number of devices allowed in user device store.	integer	Minimum value: 20654 Maximum value: 59012	41308
user-device-store-max-users	Maximum number of users allowed in user device store.	integer	Minimum value: 20654 Maximum value: 59012	41308
user-device-store-max-unified-mem	Maximum unified memory allowed in user device store.	integer	Minimum value: 41308815 Maximum value: 413088153	206544076
gui-device-latitude	Add the latitude of the location of this FortiProxy to position it on the Threat Map.	string	Maximum length: 19	
gui-device-longitude	Add the longitude of the location of this FortiProxy to position it on the Threat Map.	string	Maximum length: 19	
v-tpm	Enable/disable vTPM on VM.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable vTPM.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable vTPM		
private-data-encryption	Enable/disable private data encryption using an AES 128-bit key or passphrase.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable private data encryption using an AES 128-bit key.		
	<i>enable</i>	Enable private data encryption using an AES 128-bit key.		
auto-auth-extension-device	Enable/disable automatic authorization of dedicated Fortinet extension devices.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable automatic authorization of dedicated Fortinet extension device globally.		
	<i>disable</i>	Disable automatic authorization of dedicated Fortinet extension device globally.		
gui-theme	Color scheme for the administration GUI.	option	-	jade
	Option	Description		
	<i>jade</i>	Jade theme.		
	<i>neutrino</i>	Neutrino theme.		
	<i>mariner</i>	Mariner theme.		
	<i>graphite</i>	Graphite theme.		
	<i>melongene</i>	Melongene theme.		
	<i>retro</i>	FortiProxy v3 Retro theme.		
	<i>dark-matter</i>	Dark Matter theme.		
	<i>onyx</i>	Onyx theme.		
<i>eclipse</i>	Eclipse theme.			
gui-date-format	Default date format used throughout GUI.	option	-	yyyy/MM/dd

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>yyyy/MM/dd</i></td><td>Year/Month/Day.</td></tr><tr><td><i>dd/MM/yyyy</i></td><td>Day/Month/Year.</td></tr><tr><td><i>MM/dd/yyyy</i></td><td>Month/Day/Year.</td></tr><tr><td><i>yyyy-MM-dd</i></td><td>Year-Month-Day.</td></tr><tr><td><i>dd-MM-yyyy</i></td><td>Day-Month-Year.</td></tr><tr><td><i>MM-dd-yyyy</i></td><td>Month-Day-Year.</td></tr></table>	Option	Description	<i>yyyy/MM/dd</i>	Year/Month/Day.	<i>dd/MM/yyyy</i>	Day/Month/Year.	<i>MM/dd/yyyy</i>	Month/Day/Year.	<i>yyyy-MM-dd</i>	Year-Month-Day.	<i>dd-MM-yyyy</i>	Day-Month-Year.	<i>MM-dd-yyyy</i>	Month-Day-Year.			
	Option	Description																
	<i>yyyy/MM/dd</i>	Year/Month/Day.																
	<i>dd/MM/yyyy</i>	Day/Month/Year.																
	<i>MM/dd/yyyy</i>	Month/Day/Year.																
	<i>yyyy-MM-dd</i>	Year-Month-Day.																
	<i>dd-MM-yyyy</i>	Day-Month-Year.																
<i>MM-dd-yyyy</i>	Month-Day-Year.																	
gui-date-time-source	Source from which the FortiProxy GUI uses to display date and time entries.	option	-	system														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>system</i></td><td>Use this FortiProxy unit's configured timezone.</td></tr><tr><td><i>browser</i></td><td>Use the web browser's timezone.</td></tr></table>	Option	Description	<i>system</i>	Use this FortiProxy unit's configured timezone.	<i>browser</i>	Use the web browser's timezone.											
	Option	Description																
	<i>system</i>	Use this FortiProxy unit's configured timezone.																
<i>browser</i>	Use the web browser's timezone.																	
igmp-state-limit	Maximum number of IGMP memberships.	integer	Minimum value: 96 Maximum value: 128000	3200														
cloud-communication	Enable/disable all cloud communication.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow cloud communication.</td></tr><tr><td><i>disable</i></td><td>Disable all cloud-related settings.</td></tr></table>	Option	Description	<i>enable</i>	Allow cloud communication.	<i>disable</i>	Disable all cloud-related settings.											
	Option	Description																
	<i>enable</i>	Allow cloud communication.																
<i>disable</i>	Disable all cloud-related settings.																	
ipsec-ha-seqjump-rate	ESP jump ahead rate (1G - 10G pps equivalent).	integer	Minimum value: 1 Maximum value: 10	10														
fortitoken-cloud	Enable/disable FortiToken Cloud service.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiToken Cloud service.</td></tr><tr><td><i>disable</i></td><td>Disable FortiToken Cloud service.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiToken Cloud service.	<i>disable</i>	Disable FortiToken Cloud service.											
	Option	Description																
	<i>enable</i>	Enable FortiToken Cloud service.																
<i>disable</i>	Disable FortiToken Cloud service.																	

Parameter	Description	Type	Size	Default
faz-disk-buffer-size	Maximum disk buffer size to temporarily store logs destined for FortiAnalyzer. To be used in the event that FortiAnalyzer is unavailable.	integer	Not Specified	0
irq-time-accounting	Configure CPU IRQ time accounting mode.	option	-	auto
	Option	Description		
	auto	Automatically switch CPU accounting mode.		
	force	Force the use of CPU IRQ time accounting mode.		
management-ip	Management IP address of this FortiProxy. Used to log into this FortiProxy from another FortiProxy in the Security Fabric.	string	Maximum length: 255	
management-port	Overriding port for management connection (Overrides admin port).	integer	Minimum value: 443 1 Maximum value: 65535	
management-port-use-admin-sport	Enable/disable use of the admin-sport setting for the management port. If disabled, FortiGate will allow user to specify management-port.	option	-	enable
	Option	Description		
	enable	Enable use of the admin-sport setting for the management port.		
	disable	Disable use of the admin-sport setting for the management port.		
internet-service-database	Configure which Internet Service database size to download from FortiGuard and use.	option	-	full
	Option	Description		
	mini	Small sized Internet Service database with very limited IP addresses.		
	standard	Medium sized Internet Service database with most IP addresses.		
	full	Full sized Internet Service database with all IP addresses.		
	on-demand	Internet Service database with customer selected IP addresses.		

Parameter	Description	Type	Size	Default						
early-tcp-npu-session	Enable/disable early TCP NPU session.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable early TCP NPU session in order to guarantee packet order of 3-way handshake.</td></tr><tr><td><i>disable</i></td><td>Disable early TCP NPU session in order to guarantee packet order of 3-way handshake.</td></tr></table>	Option	Description	<i>enable</i>	Enable early TCP NPU session in order to guarantee packet order of 3-way handshake.	<i>disable</i>	Disable early TCP NPU session in order to guarantee packet order of 3-way handshake.			
Option	Description									
<i>enable</i>	Enable early TCP NPU session in order to guarantee packet order of 3-way handshake.									
<i>disable</i>	Disable early TCP NPU session in order to guarantee packet order of 3-way handshake.									
interface-subnet-usage	Enable/disable allowing use of interface-subnet setting in firewall addresses.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disallow use of the interface-subnet setting in firewall addresses. Use in conjunction with the FortiGate REST API and when a large number of firewall addresses exist in the configuration.</td></tr><tr><td><i>enable</i></td><td>Allow use of the interface-subnet setting in firewall addresses.</td></tr></table>	Option	Description	<i>disable</i>	Disallow use of the interface-subnet setting in firewall addresses. Use in conjunction with the FortiGate REST API and when a large number of firewall addresses exist in the configuration.	<i>enable</i>	Allow use of the interface-subnet setting in firewall addresses.			
Option	Description									
<i>disable</i>	Disallow use of the interface-subnet setting in firewall addresses. Use in conjunction with the FortiGate REST API and when a large number of firewall addresses exist in the configuration.									
<i>enable</i>	Allow use of the interface-subnet setting in firewall addresses.									
sflowd-max-children-num	Maximum number of sflowd child processes allowed to run.	integer	Minimum value: 0 Maximum value: 6	6						
license-overlimit	System behaviour when max licensed proxy user is reached.	option	-	bypass						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass further traffic when licensed user is reached.</td></tr><tr><td><i>block</i></td><td>Block further traffic when licensed user is reached.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass further traffic when licensed user is reached.	<i>block</i>	Block further traffic when licensed user is reached.			
Option	Description									
<i>bypass</i>	Bypass further traffic when licensed user is reached.									
<i>block</i>	Block further traffic when licensed user is reached.									
max-session-per-user	Max UTM sessions per user.	integer	Minimum value: 0 Maximum value: 4294967295	0						
conntrack	Max numbers of conntrack.	integer	Minimum value: 60000 Maximum value: 10000000	700000						
established-timeout	Default established session timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	1800						

Parameter	Description	Type	Size	Default
time-wait-timeout	Default time-wait timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	60
fin-wait-timeout	Default fin-wait timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	60
close-wait-timeout	Default close-wait timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	30
syn-sent-timeout	Default syn-sent timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	60
syn-recv-timeout	Default syn-recv timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	30
last-ack-timeout	Default last-ack timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	15
udp-timeout	Default last-ack timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	30
udp-stream-timeout	Default last-ack timeout (seconds).	integer	Minimum value: 10 Maximum value: 432000	180
username-case-sensitivity	Case sensitivity when performing username matching	option	-	enable
		Option	Description	
		<i>enable</i>	Check case when performing username matching	
		<i>disable</i>	Ignore case when performing username matching	

config system gre-tunnel

Configure GRE tunnel.

```
config system gre-tunnel
  Description: Configure GRE tunnel.
  edit <name>
    set interface {string}
    set remote-gw {ipv4-address}
```

```

    set local-gw {ipv4-address-any}
    set sequence-number-transmission [disable|enable]
    set sequence-number-reception [disable|enable]
    set checksum-transmission [disable|enable]
    set checksum-reception [disable|enable]
    set key-outbound {integer}
    set key-inbound {integer}
    set keepalive-interval {integer}
    set keepalive-failtimes {integer}
next
end

```

config system gre-tunnel

Parameter	Description	Type	Size	Default						
name	Tunnel name.	string	Maximum length: 15							
interface	Interface name.	string	Maximum length: 15							
remote-gw	IP address of the remote gateway.	ipv4-address	Not Specified	0.0.0.0						
local-gw	IP address of the local gateway.	ipv4-address-any	Not Specified	0.0.0.0						
sequence-number-transmission	Enable/disable including of sequence numbers in transmitted GRE packets.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Include sequence numbers in transmitted GRE packets.</td></tr><tr><td><i>enable</i></td><td>Do not include sequence numbers in transmitted GRE packets.</td></tr></table>				Option	Description	<i>disable</i>	Include sequence numbers in transmitted GRE packets.	<i>enable</i>	Do not include sequence numbers in transmitted GRE packets.
Option	Description									
<i>disable</i>	Include sequence numbers in transmitted GRE packets.									
<i>enable</i>	Do not include sequence numbers in transmitted GRE packets.									
sequence-number-reception	Enable/disable validating sequence numbers in received GRE packets.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not validate sequence number in received GRE packets.</td></tr><tr><td><i>enable</i></td><td>Validate sequence numbers in received GRE packets.</td></tr></table>				Option	Description	<i>disable</i>	Do not validate sequence number in received GRE packets.	<i>enable</i>	Validate sequence numbers in received GRE packets.
Option	Description									
<i>disable</i>	Do not validate sequence number in received GRE packets.									
<i>enable</i>	Validate sequence numbers in received GRE packets.									
checksum-transmission	Enable/disable including checksums in transmitted GRE packets.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	disable	Do not include checksums in transmitted GRE packets.		
	enable	Include checksums in transmitted GRE packets.		
checksum-reception	Enable/disable validating checksums in received GRE packets.	option	-	disable
	Option	Description		
	disable	Do not validate checksums in received GRE packets.		
	enable	Validate checksums in received GRE packets.		
key-outbound	Include this key in transmitted GRE packets.	integer	Minimum value: 0 Maximum value: 4294967295	0
key-inbound	Require received GRE packets contain this key.	integer	Minimum value: 0 Maximum value: 4294967295	0
keepalive-interval	Keepalive message interval.	integer	Minimum value: 0 Maximum value: 32767	0
keepalive-failtimes	Number of consecutive unreturned keepalive messages before a GRE connection is considered down.	integer	Minimum value: 1 Maximum value: 255	10

config system ha-lic

ha-lic

```

config system ha-lic
  Description: ha-lic
  edit <serial-num>
    set last-sync-time {password}
    set last-sync-seat {password}
    set last-sync-seat-fnbi {password}
    set last-sync-seat-fcas {password}
  next
end

```

config system ha-lic

Parameter	Description	Type	Size	Default
serial-num	The Serial Number that joined an HA cluster.	string	Maximum length: 16	
last-sync-time	Last time_t when SN updated the user seats.	password	Not Specified	
last-sync-seat	Last seats when SN updated the user seats.	password	Not Specified	
last-sync-seat-fnbi	Last seats when SN updated the isolator seats.	password	Not Specified	
last-sync-seat-fcas	Last seats when SN updated the image AI seats.	password	Not Specified	

config system ha-monitor

Configure HA monitor.

```
config system ha-monitor
    Description: Configure HA monitor.
    set monitor-vlan [enable|disable]
    set vlan-hb-interval {integer}
    set vlan-hb-lost-threshold {integer}
end
```

config system ha-monitor

Parameter	Description	Type	Size	Default						
monitor-vlan	Enable/disable monitor VLAN interfaces.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable monitor VLAN interfaces.</td></tr><tr><td><i>disable</i></td><td>Disable monitor VLAN interfaces.</td></tr></table>				Option	Description	<i>enable</i>	Enable monitor VLAN interfaces.	<i>disable</i>	Disable monitor VLAN interfaces.
	Option	Description								
	<i>enable</i>	Enable monitor VLAN interfaces.								
<i>disable</i>	Disable monitor VLAN interfaces.									
vlan-hb-interval	Configure heartbeat interval (seconds).	integer	Minimum value: 1 Maximum value: 30	5						
vlan-hb-lost-threshold	VLAN lost heartbeat threshold.	integer	Minimum value: 1 Maximum value: 60	3						

config system ha-nonsync-csum

System checksum for FortiManager use only.

```
config system ha-nonsync-csum
    Description: System checksum for FortiManager use only.
end
```

config system ha

Configure HA.

```
config system ha
    Description: Configure HA.
    set group-id {integer}
    set group-name {string}
    set mode [standalone|config-sync-only|...]
    set sync-packet-balance [enable|disable]
    set password {password}
    set key {password}
    set hbdev {user}
    set unicast-hb [enable|disable]
    set unicast-hb-peerip {ipv4-address}
    set unicast-hb-netmask {ipv4-netmask}
    set route-ttl {integer}
    set route-wait {integer}
    set route-hold {integer}
    set multicast-ttl {integer}
    set encryption [enable|disable]
    set authentication [enable|disable]
    set hb-interval {integer}
    set hb-interval-in-milliseconds [100ms|10ms]
    set hb-lost-threshold {integer}
    set hello-holddown {integer}
    set gratuitous-arps [enable|disable]
    set arps {integer}
    set arps-interval {integer}
    set link-failed-signal [enable|disable]
    set uninterruptible-upgrade [enable|disable]
    set sequential-upgrade [enable|disable]
    set uninterruptible-primary-wait {integer}
    set primary-hold-before-reboot {integer}
    set ha-mgmt-status [enable|disable]
    config ha-mgmt-interfaces
        Description: Reserve interfaces to manage individual cluster units.
        edit <id>
            set interface {string}
            set dst {ipv4-classnet}
            set gateway {ipv4-address}
            set gateway6 {ipv6-address}
        next
    end
```



```
set ha-uptime-diff-margin {integer}
set unicast-status [enable|disable]
set unicast-gateway {ipv4-address}
config unicast-peers
    Description: Number of unicast peers.
    edit <id>
        set peer-ip {ipv4-address}
    next
end
set weight {user}
set cpu-threshold {user}
set memory-threshold {user}
set http-proxy-threshold {user}
set ftp-proxy-threshold {user}
set imap-proxy-threshold {user}
set nntp-proxy-threshold {user}
set pop3-proxy-threshold {user}
set smtp-proxy-threshold {user}
set override [enable|disable]
set priority {integer}
set override-wait-time {integer}
set monitor {user}
set pingserver-monitor-interface {user}
set pingserver-failover-threshold {integer}
set pingserver-secondary-force-reset [enable|disable]
set pingserver-flip-timeout {integer}
set vcluster-status [enable|disable]
config vcluster
    Description: Virtual cluster table.
    edit <vcluster-id>
        set override [enable|disable]
        set priority {integer}
        set override-wait-time {integer}
        set monitor {user}
        set pingserver-monitor-interface {user}
        set pingserver-failover-threshold {integer}
        set pingserver-secondary-force-reset [enable|disable]
        set vdom <name1>, <name2>, ...
    next
end
set ha-direct [enable|disable]
set ssd-failover [enable|disable]
set memory-compatible-mode [enable|disable]
set memory-based-failover [enable|disable]
set memory-failover-threshold {integer}
set memory-failover-monitor-period {integer}
set memory-failover-sample-rate {integer}
set memory-failover-flip-timeout {integer}
set failover-hold-time {integer}
end
```

config system ha

Parameter	Description	Type	Size	Default
group-id	HA group ID . Must be the same for all members.	integer	Minimum value: 0 Maximum value: 1023	0
group-name	Cluster group name. Must be the same for all members.	string	Maximum length: 32	
mode	HA mode. Must be the same for all members. FGSP requires standalone.	option	-	standalone
	Option Description			
	standalone Disable HA feature.			
	config-sync-only Enable Config sync only			
	active-passive Enable Active-passive mode.			
sync-packet-balance	Enable/disable HA packet distribution to multiple CPUs.	option	-	disable
	Option Description			
	enable Enable HA packet distribution to multiple CPUs.			
	disable Disable HA packet distribution to multiple CPUs.			
password	Cluster password. Must be the same for all members.	password	Not Specified	
key	Key.	password	Not Specified	
hbdev	Heartbeat interfaces. Must be the same for all members.	user	Not Specified	
unicast-hb	Enable/disable unicast heartbeat.	option	-	disable
	Option Description			
	enable Enable setting.			
	disable Disable setting.			
unicast-hb-peerip	Unicast heartbeat peer IP.	ipv4-address	Not Specified	0.0.0.0
unicast-hb-netmask	Unicast heartbeat netmask.	ipv4-netmask	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default						
route-ttl	TTL for primary unit routes. Increase to maintain active routes during failover.	integer	Minimum value: 5 Maximum value: 3600	10						
route-wait	Time to wait before sending new routes to the cluster.	integer	Minimum value: 0 Maximum value: 3600	0						
route-hold	Time to wait between routing table updates to the cluster.	integer	Minimum value: 0 Maximum value: 3600	10						
multicast-ttl	HA multicast TTL on primary.	integer	Minimum value: 5 Maximum value: 3600	600						
encryption	Enable/disable heartbeat message encryption.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable heartbeat message encryption.</td></tr><tr><td><i>disable</i></td><td>Disable heartbeat message encryption.</td></tr></table>	Option	Description	<i>enable</i>	Enable heartbeat message encryption.	<i>disable</i>	Disable heartbeat message encryption.			
	Option	Description								
	<i>enable</i>	Enable heartbeat message encryption.								
<i>disable</i>	Disable heartbeat message encryption.									
authentication	Enable/disable heartbeat message authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable heartbeat message authentication.</td></tr><tr><td><i>disable</i></td><td>Disable heartbeat message authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable heartbeat message authentication.	<i>disable</i>	Disable heartbeat message authentication.			
	Option	Description								
	<i>enable</i>	Enable heartbeat message authentication.								
<i>disable</i>	Disable heartbeat message authentication.									
hb-interval	Time between sending heartbeat packets. Increase to reduce false positives.	integer	Minimum value: 1 Maximum value: 20	2						
hb-interval-in-milliseconds	Number of milliseconds for each heartbeat interval: 100ms or 10ms.	option	-	100ms						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>100ms</i></td><td>Each heartbeat interval is 100ms.</td></tr><tr><td><i>10ms</i></td><td>Each heartbeat interval is 10ms.</td></tr></table>	Option	Description	<i>100ms</i>	Each heartbeat interval is 100ms.	<i>10ms</i>	Each heartbeat interval is 10ms.			
	Option	Description								
	<i>100ms</i>	Each heartbeat interval is 100ms.								
<i>10ms</i>	Each heartbeat interval is 10ms.									

Parameter	Description	Type	Size	Default
hb-lost-threshold	Number of lost heartbeats to signal a failure. Increase to reduce false positives.	integer	Minimum value: 1 Maximum value: 60	20
hello-holddown	Time to wait before changing from hello to work state.	integer	Minimum value: 5 Maximum value: 300	20
gratuitous-arps	Enable/disable gratuitous ARPs. Disable if link-failed-signal enabled.	option	-	enable
	Option		Description	
	<i>enable</i>		Enable gratuitous ARPs.	
	<i>disable</i>		Disable gratuitous ARPs.	
arps	Number of gratuitous ARPs. Lower to reduce traffic. Higher to reduce failover time.	integer	Minimum value: 1 Maximum value: 60	5
arps-interval	Time between gratuitous ARPs . Lower to reduce failover time. Higher to reduce traffic.	integer	Minimum value: 1 Maximum value: 20	8
link-failed-signal	Enable to shut down all interfaces for 1 sec after a failover. Use if gratuitous ARPs do not update network.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable setting.	
	<i>disable</i>		Disable setting.	
uninterruptible-upgrade	Enable to upgrade a cluster without blocking network traffic.	option	-	enable
	Option		Description	
	<i>enable</i>		Enable setting.	
	<i>disable</i>		Disable setting.	
sequential-upgrade	Enable to upgrade secondaries one by one.	option	-	enable

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
uninterruptible-primary-wait	Number of minutes the primary HA unit waits before the secondary HA unit is considered upgraded and the system is started before starting its own upgrade.	integer	Minimum value: 15 Maximum value: 300	30						
primary-hold-before-reboot	Number of seconds the primary HA unit waits after the secondary HA unit upgraded and joined back HA then starts its own upgrade.	integer	Minimum value: 0 Maximum value: 600	0						
ha-mgmt-status	Enable to reserve interfaces to manage individual cluster units.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
ha-uptime-diff-margin	Normally you would only reduce this value for failover testing.	integer	Minimum value: 1 Maximum value: 65535	300						
unicast-status	Enable/disable unicast connection.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
unicast-gateway	Default route gateway for unicast interface.	ipv4-address	Not Specified	0.0.0.0						
weight	Weight-round-robin weight for each cluster unit. Syntax <priority> <weight>.	user	Not Specified	0 40						
cpu-threshold	Dynamic weighted load balancing CPU usage weight and high and low thresholds.	user	Not Specified							
memory-threshold	Dynamic weighted load balancing memory usage weight and high and low thresholds.	user	Not Specified							
http-proxy-threshold	Dynamic weighted load balancing weight and high and low number of HTTP proxy sessions.	user	Not Specified							

Parameter	Description	Type	Size	Default
ftp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of FTP proxy sessions.	user	Not Specified	
imap-proxy-threshold	Dynamic weighted load balancing weight and high and low number of IMAP proxy sessions.	user	Not Specified	
nntp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of NNTP proxy sessions.	user	Not Specified	
pop3-proxy-threshold	Dynamic weighted load balancing weight and high and low number of POP3 proxy sessions.	user	Not Specified	
smtp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of SMTP proxy sessions.	user	Not Specified	
override	Enable and increase the priority of the unit that should always be primary (master).	option	-	disable
	Option		Description	
	<i>enable</i>		Enable setting.	
	<i>disable</i>		Disable setting.	
priority	Increase the priority to select the primary unit.	integer	Minimum value: 0 Maximum value: 255	128
override-wait-time	Delay negotiating if override is enabled. Reduces how often the cluster negotiates.	integer	Minimum value: 0 Maximum value: 3600	0
monitor	Interfaces to check for port monitoring (or link failure).	user	Not Specified	
pingserver-monitor-interface	Interfaces to check for remote IP monitoring.	user	Not Specified	
pingserver-failover-threshold	Remote IP monitoring failover threshold.	integer	Minimum value: 0 Maximum value: 50	0
pingserver-secondary-force-reset	Enable to force the cluster to negotiate after a remote IP monitoring failover.	option	-	enable
	Option		Description	
	<i>enable</i>		Enable force reset of secondary member after PING server failure.	

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable force reset of secondary member after PING server failure.</td></tr></table>	Option	Description	<i>disable</i>	Disable force reset of secondary member after PING server failure.					
Option	Description									
<i>disable</i>	Disable force reset of secondary member after PING server failure.									
pingserver-flip-timeout	Time to wait in minutes before renegotiating after a remote IP monitoring failover.	integer	Minimum value: 6 Maximum value: 2147483647	60						
vcluster-status	Enable/disable virtual cluster for virtual clustering.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ha-direct	Enable/disable using ha-mgmt interface for syslog, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox.</td></tr><tr><td><i>disable</i></td><td>Disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox.</td></tr></table>	Option	Description	<i>enable</i>	Enable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox.	<i>disable</i>	Disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox.			
Option	Description									
<i>enable</i>	Enable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox.									
<i>disable</i>	Disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox.									
ssd-failover	Enable/disable automatic HA failover on SSD disk failure.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
memory-compatible-mode	Enable/disable memory compatible mode.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
memory-based-failover	Enable/disable memory based failover.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
memory-failover-threshold	Memory usage threshold to trigger memory based failover (0 means using conserve mode threshold in system.global).	integer	Minimum value: 0 Maximum value: 95	0
memory-failover-monitor-period	Duration of high memory usage before memory based failover is triggered in seconds.	integer	Minimum value: 1 Maximum value: 300	60
memory-failover-sample-rate	Rate at which memory usage is sampled in order to measure memory usage in seconds.	integer	Minimum value: 1 Maximum value: 60	1
memory-failover-flip-timeout	Time to wait between subsequent memory based failovers in minutes.	integer	Minimum value: 6 Maximum value: 2147483647	6
failover-hold-time	Time to wait before failover , to avoid flip.	integer	Minimum value: 0 Maximum value: 300	0

config ha-mgmt-interfaces

Parameter	Description	Type	Size	Default
id	Table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
interface	Interface to reserve for HA management.	string	Maximum length: 15	
dst	Default route destination for reserved HA management interface.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
gateway	Default route gateway for reserved HA management interface.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
gateway6	Default IPv6 gateway for reserved HA management interface.	ipv6-address	Not Specified	::

config unicast-peers

Parameter	Description	Type	Size	Default
id	Table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
peer-ip	Unicast peer IP.	ipv4-address	Not Specified	0.0.0.0

config vcluster

Parameter	Description	Type	Size	Default
vcluster-id	ID.	integer	Minimum value: 1 Maximum value: 30	1
override	Enable and increase the priority of the unit that should always be primary (master).	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
priority	Increase the priority to select the primary unit.	integer	Minimum value: 0 Maximum value: 255	128
override-wait-time	Delay negotiating if override is enabled. Reduces how often the cluster negotiates.	integer	Minimum value: 0 Maximum value: 3600	0
monitor	Interfaces to check for port monitoring (or link failure).	user	Not Specified	

Parameter	Description	Type	Size	Default
pingserver-monitor-interface	Interfaces to check for remote IP monitoring.	user	Not Specified	
pingserver-failover-threshold	Remote IP monitoring failover threshold.	integer	Minimum value: 0 Maximum value: 50	0
pingserver-secondary-force-reset	Enable to force the cluster to negotiate after a remote IP monitoring failover.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable force reset of secondary member after PING server failure.		
	<i>disable</i>	Disable force reset of secondary member after PING server failure.		
vdom <name>	Virtual domain(s) in the virtual cluster. Virtual domain name.	string	Maximum length: 79	

config system info admin ssh

Show SSH status.

```
config system info admin ssh
    Description: Show SSH status.
end
```

config system info admin status

Show logged in administrators.

```
config system info admin status
    Description: Show logged in administrators.
end
```

config system interface

Configure interfaces.

```
config system interface
    Description: Configure interfaces.
```

```
edit <name>
  set vdom {string}
  set cli-conn-status {integer}
  set mode [static|dhcp|...]
  config client-options
    Description: DHCP client options.
    edit <id>
      set code {integer}
      set type [hex|string|...]
      set value {string}
      set ip {user}
    next
  end
  set distance {integer}
  set priority {integer}
  set dhcp-relay-interface-select-method [auto|specify]
  set dhcp-relay-interface {string}
  set dhcp-relay-service [disable|enable]
  set dhcp-relay-ip {user}
  set dhcp-relay-link-selection {ipv4-address}
  set dhcp-relay-request-all-server [disable|enable]
  set dhcp-relay-type [regular|ipsec]
  set dhcp-relay-agent-option [enable|disable]
  set dhcp-classless-route-addition [enable|disable]
  set management-ip {ipv4-classnet-host}
  set ip {ipv4-classnet-host}
  set allowaccess {option1}, {option2}, ...
  set gwdetect [enable|disable]
  set ping-serv-status {integer}
  set detectserver {user}
  set detectprotocol {option1}, {option2}, ...
  set ha-priority {integer}
  set fail-detect [enable|disable]
  set fail-detect-option {option1}, {option2}, ...
  set fail-alert-method [link-failed-signal|link-down]
  set fail-action-on-extender [soft-restart|hard-restart|...]
  set fail-alert-interfaces <name1>, <name2>, ...
  set dhcp-client-identifier {string}
  set dhcp-renew-time {integer}
  set ipunnumbered {ipv4-address}
  set username {string}
  set pppoe-unnumbered-negotiate [enable|disable]
  set password {password}
  set idle-timeout {integer}
  set detected-peer-mtu {integer}
  set disc-retry-timeout {integer}
  set padt-retry-timeout {integer}
  set service-name {string}
  set ac-name {string}
  set lcp-echo-interval {integer}
  set lcp-max-echo-fails {integer}
  set defaultgw [enable|disable]
  set dns-server-override [enable|disable]
  set dns-server-protocol {option1}, {option2}, ...
  set auth-type [auto|pap|...]
  set pptp-client [enable|disable]
```

```
set ptp-user {string}
set ptp-password {password}
set ptp-server-ip {ipv4-address}
set ptp-auth-type [auto|pap|...]
set ptp-timeout {integer}
set arpforward [enable|disable]
set broadcast-forward [enable|disable]
set bfd [global|enable|...]
set bfd-desired-min-tx {integer}
set bfd-detect-mult {integer}
set bfd-required-min-rx {integer}
set l2forward [enable|disable]
set icmp-send-redirect [enable|disable]
set icmp-accept-redirect [enable|disable]
set stpforward [enable|disable]
set stpforward-mode [rpl-all-ext-id|rpl-bridge-ext-id|...]
set macaddr {mac-address}
set substitute-dst-mac {mac-address}
set large-receive-offload [enable|disable]
set generic-receive-offload [enable|disable]
set speed [auto|10full|...]
set status [up|down]
set netbios-forward [disable|enable]
set wins-ip {ipv4-address}
set type [physical|vlan|...]
set dedicated-to [none|management]
set trust-ip-1 {ipv4-classnet-any}
set trust-ip-2 {ipv4-classnet-any}
set trust-ip-3 {ipv4-classnet-any}
set trust-ip6-1 {ipv6-prefix}
set trust-ip6-2 {ipv6-prefix}
set trust-ip6-3 {ipv6-prefix}
set ring-rx {integer}
set ring-tx {integer}
set wccp [enable|disable]
set drop-overlapped-fragment [enable|disable]
set drop-fragment [enable|disable]
set src-check [enable|disable]
set explicit-web-proxy [enable|disable]
set explicit-ftp-proxy [enable|disable]
set proxy-captive-portal [enable|disable]
set tcp-mss {integer}
set inbandwidth {integer}
set outbandwidth {integer}
set egress-shaping-profile {string}
set ingress-shaping-profile {string}
set disconnect-threshold {integer}
set spillover-threshold {integer}
set ingress-spillover-threshold {integer}
set weight {integer}
set interface {string}
set external [enable|disable]
set mtu-override [enable|disable]
set mtu {integer}
set vlan-protocol [8021q|8021ad]
set vlanid {integer}
```

```

set forward-domain {integer}
set remote-ip {ipv4-classnet-host}
set member <interface-name1>, <interface-name2>, ...
set lacp-mode {option}
set lacp-ha-secondary [enable|disable]
set system-id-type [auto|user]
set system-id {mac-address}
set lacp-speed [slow|fast]
set min-links {integer}
set min-links-down [operational|administrative]
set algorithm [L2|L3|...]
set link-up-delay {integer}
set aggregate-type [physical|vxlan]
set priority-override [enable|disable]
set aggregate {string}
set redundant-interface {string}
set devindex {integer}
set switch {string}
set description {var-string}
set alias {string}
set security-mode [none|captive-portal|...]
set security-mac-auth-bypass [mac-auth-only|enable|...]
set security-external-web {var-string}
set security-external-logout {string}
set replacemsg-override-group {string}
set security-redirect-url {var-string}
set auth-cert {string}
set auth-portal-addr {string}
set security-exempt-list {string}
set security-groups <name1>, <name2>, ...
set ike-saml-server {string}
set role [lan|wan|...]
set snmp-index {integer}
set secondary-IP [enable|disable]
config secondaryip
    Description: Second IP address of interface.
    edit <id>
        set ip {ipv4-classnet-host}
        set allowaccess {option1}, {option2}, ...
        set gwdetect [enable|disable]
        set ping-serv-status {integer}
        set detectserver {user}
        set detectprotocol {option1}, {option2}, ...
        set ha-priority {integer}
    next
end
set color {integer}
config tagging
    Description: Config object tagging.
    edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
    next
end
set eap-supPLICant [enable|disable]
set eap-method [tls|peap]

```

```

set eap-identity {string}
set eap-password {password}
set eap-ca-cert {string}
set eap-user-cert {string}
config ipv6
    Description: IPv6 of interface.
    set ip6-mode [static|dhcp|...]
    set nd-mode [basic|SEND-compatible]
    set nd-cert {string}
    set nd-security-level {integer}
    set nd-timestamp-delta {integer}
    set nd-timestamp-fuzz {integer}
    set nd-cga-modifier {user}
    set ip6-dns-server-override [enable|disable]
    set ip6-address {ipv6-prefix}
    config ip6-extra-addr
        Description: Extra IPv6 address prefixes of interface.
        edit <prefix>
            next
        end
    set ip6-allowaccess {option1}, {option2}, ...
    set ip6-send-adv [enable|disable]
    set icmp6-send-redirect [enable|disable]
    set ip6-manage-flag [enable|disable]
    set ip6-other-flag [enable|disable]
    set ip6-max-interval {integer}
    set ip6-min-interval {integer}
    set ip6-link-mtu {integer}
    set ra-send-mtu [enable|disable]
    set ip6-reachable-time {integer}
    set ip6-retrans-time {integer}
    set ip6-default-life {integer}
    set ip6-hop-limit {integer}
    set autoconf [enable|disable]
    set unique-autoconf-addr [enable|disable]
    set interface-identifier {ipv6-address}
    set ip6-prefix-mode [dhcp6|ra]
    set ip6-delegated-prefix-iaid {integer}
    set ip6-upstream-interface {string}
    set ip6-subnet {ipv6-prefix}
    config ip6-prefix-list
        Description: Advertised prefix list.
        edit <prefix>
            set autonomous-flag [enable|disable]
            set onlink-flag [enable|disable]
            set valid-life-time {integer}
            set preferred-life-time {integer}
            set rdns {user}
            set dnssl <domain1>, <domain2>, ...
        next
    end
    config ip6-delegated-prefix-list
        Description: Advertised IPv6 delegated prefix list.
        edit <prefix-id>
            set upstream-interface {string}
            set delegated-prefix-iaid {integer}

```

```

        set autonomous-flag [enable|disable]
        set onlink-flag [enable|disable]
        set subnet {ipv6-network}
        set rdns-service [delegated|default|...]
        set rdns {user}
    next
end
set dhcp6-relay-service [disable|enable]
set dhcp6-relay-type {option}
set dhcp6-relay-source-interface [disable|enable]
set dhcp6-relay-ip {user}
set dhcp6-client-options {option1}, {option2}, ...
set dhcp6-prefix-delegation [enable|disable]
set dhcp6-information-request [enable|disable]
config dhcp6-iapd-list
    Description: DHCPv6 IA-PD list.
    edit <iaid>
        set prefix-hint {ipv6-network}
        set prefix-hint-plt {integer}
        set prefix-hint-vlt {integer}
    next
end
set cli-conn6-status {integer}
end
next
end

```

config system interface

Parameter	Description	Type	Size	Default								
name	Name.	string	Maximum length: 15									
vdom	Interface is in this virtual domain (VDM).	string	Maximum length: 31									
cli-conn-status	CLI connection status.	integer	Minimum value: 0 Maximum value: 4294967295	0								
mode	Addressing mode (static, DHCP, PPPoE).	option	-	static								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>static</td><td>Static setting.</td></tr><tr><td>dhcp</td><td>External DHCP client mode.</td></tr><tr><td>pppoe</td><td>External PPPoE mode.</td></tr></table>				Option	Description	static	Static setting.	dhcp	External DHCP client mode.	pppoe	External PPPoE mode.
	Option	Description										
	static	Static setting.										
	dhcp	External DHCP client mode.										
pppoe	External PPPoE mode.											

Parameter	Description	Type	Size	Default
distance	Distance for routes learned through PPPoE or DHCP, lower distance indicates preferred route.	integer	Minimum value: 1 Maximum value: 255	5
priority	Priority of learned routes.	integer	Minimum value: 1 Maximum value: 65535	0
dhcp-relay-interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option		Description	
	<i>auto</i>		Set outgoing interface automatically.	
	<i>specify</i>		Set outgoing interface manually.	
dhcp-relay-interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
dhcp-relay-service	Enable/disable allowing this interface to act as a DHCP relay.	option	-	disable
	Option		Description	
	<i>disable</i>		None.	
	<i>enable</i>		DHCP relay agent.	
dhcp-relay-ip	DHCP relay IP address.	user	Not Specified	
dhcp-relay-link-selection	DHCP relay link selection.	ipv4-address	Not Specified	0.0.0.0
dhcp-relay-request-all-server	Enable/disable sending of DHCP requests to all servers.	option	-	disable
	Option		Description	
	<i>disable</i>		Send DHCP requests only to a matching server.	
	<i>enable</i>		Send DHCP requests to all servers.	
dhcp-relay-type	DHCP relay type (regular or IPsec).	option	-	regular
	Option		Description	
	<i>regular</i>		Regular DHCP relay.	

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ipsec</i></td><td>DHCP relay for IPsec.</td></tr></table>	Option	Description	<i>ipsec</i>	DHCP relay for IPsec.																			
	Option	Description																						
	<i>ipsec</i>	DHCP relay for IPsec.																						
dhcp-relay-agent-option	Enable/disable DHCP relay agent option.	option	-	enable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DHCP relay agent option.</td></tr><tr><td><i>disable</i></td><td>Disable DHCP relay agent option.</td></tr></table>	Option	Description	<i>enable</i>	Enable DHCP relay agent option.	<i>disable</i>	Disable DHCP relay agent option.																	
	Option	Description																						
	<i>enable</i>	Enable DHCP relay agent option.																						
<i>disable</i>	Disable DHCP relay agent option.																							
dhcp-classless-route-addition	Enable/disable addition of classless static routes retrieved from DHCP server.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable addition of classless static routes retrieved from DHCP server.</td></tr><tr><td><i>disable</i></td><td>Disable addition of classless static routes retrieved from DHCP server.</td></tr></table>	Option	Description	<i>enable</i>	Enable addition of classless static routes retrieved from DHCP server.	<i>disable</i>	Disable addition of classless static routes retrieved from DHCP server.																	
	Option	Description																						
	<i>enable</i>	Enable addition of classless static routes retrieved from DHCP server.																						
<i>disable</i>	Disable addition of classless static routes retrieved from DHCP server.																							
management-ip	High Availability in-band management IP address of this interface.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0																				
ip	Interface IPv4 address and subnet mask, syntax: X.X.X.X/24.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0																				
allowaccess	Permitted types of management access to this interface.	option	-																					
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING access.</td></tr><tr><td><i>https</i></td><td>HTTPS access.</td></tr><tr><td><i>ssh</i></td><td>SSH access.</td></tr><tr><td><i>snmp</i></td><td>SNMP access.</td></tr><tr><td><i>http</i></td><td>HTTP access.</td></tr><tr><td><i>telnet</i></td><td>TELNET access.</td></tr><tr><td><i>fgfm</i></td><td>FortiManager access.</td></tr><tr><td><i>radius-acct</i></td><td>RADIUS accounting access.</td></tr><tr><td><i>probe-response</i></td><td>Probe access.</td></tr></table>	Option	Description	<i>ping</i>	PING access.	<i>https</i>	HTTPS access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.	<i>http</i>	HTTP access.	<i>telnet</i>	TELNET access.	<i>fgfm</i>	FortiManager access.	<i>radius-acct</i>	RADIUS accounting access.	<i>probe-response</i>	Probe access.			
	Option	Description																						
	<i>ping</i>	PING access.																						
	<i>https</i>	HTTPS access.																						
	<i>ssh</i>	SSH access.																						
	<i>snmp</i>	SNMP access.																						
	<i>http</i>	HTTP access.																						
	<i>telnet</i>	TELNET access.																						
	<i>fgfm</i>	FortiManager access.																						
<i>radius-acct</i>	RADIUS accounting access.																							
<i>probe-response</i>	Probe access.																							

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fabric</i></td><td>Security Fabric access.</td></tr><tr><td><i>ftm</i></td><td>FTM access.</td></tr><tr><td><i>speed-test</i></td><td>Speed test access.</td></tr></table>	Option	Description	<i>fabric</i>	Security Fabric access.	<i>ftm</i>	FTM access.	<i>speed-test</i>	Speed test access.			
	Option	Description										
	<i>fabric</i>	Security Fabric access.										
	<i>ftm</i>	FTM access.										
<i>speed-test</i>	Speed test access.											
gwdetect	Enable/disable detect gateway alive for first.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable detect gateway alive for first.</td></tr><tr><td><i>disable</i></td><td>Disable detect gateway alive for first.</td></tr></table>	Option	Description	<i>enable</i>	Enable detect gateway alive for first.	<i>disable</i>	Disable detect gateway alive for first.					
	Option	Description										
	<i>enable</i>	Enable detect gateway alive for first.										
<i>disable</i>	Disable detect gateway alive for first.											
ping-serv-status	PING server status.	integer	Minimum value: 0 Maximum value: 255	0								
detectserver	Gateway's ping server for this IP.	user	Not Specified									
detectprotocol	Protocols used to detect the server.	option	-	ping								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING.</td></tr><tr><td><i>tcp-echo</i></td><td>TCP echo.</td></tr><tr><td><i>udp-echo</i></td><td>UDP echo.</td></tr></table>	Option	Description	<i>ping</i>	PING.	<i>tcp-echo</i>	TCP echo.	<i>udp-echo</i>	UDP echo.			
	Option	Description										
	<i>ping</i>	PING.										
	<i>tcp-echo</i>	TCP echo.										
<i>udp-echo</i>	UDP echo.											
ha-priority	HA election priority for the PING server.	integer	Minimum value: 1 Maximum value: 50	1								
fail-detect	Enable/disable fail detection features for this interface.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable interface failed option status.</td></tr><tr><td><i>disable</i></td><td>Disable interface failed option status.</td></tr></table>	Option	Description	<i>enable</i>	Enable interface failed option status.	<i>disable</i>	Disable interface failed option status.					
	Option	Description										
	<i>enable</i>	Enable interface failed option status.										
<i>disable</i>	Disable interface failed option status.											
fail-detect-option	Options for detecting that this interface has failed.	option	-	link-down								

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>detectserver</i></td><td>Use a ping server to determine if the interface has failed.</td></tr><tr><td><i>link-down</i></td><td>Use port detection to determine if the interface has failed.</td></tr></table>	Option	Description	<i>detectserver</i>	Use a ping server to determine if the interface has failed.	<i>link-down</i>	Use port detection to determine if the interface has failed.					
	Option	Description										
	<i>detectserver</i>	Use a ping server to determine if the interface has failed.										
<i>link-down</i>	Use port detection to determine if the interface has failed.											
fail-alert-method	Select link-failed-signal or link-down method to alert about a failed link.	option	-	link-down								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>link-failed-signal</i></td><td>Link-failed-signal.</td></tr><tr><td><i>link-down</i></td><td>Link-down.</td></tr></table>	Option	Description	<i>link-failed-signal</i>	Link-failed-signal.	<i>link-down</i>	Link-down.					
	Option	Description										
	<i>link-failed-signal</i>	Link-failed-signal.										
<i>link-down</i>	Link-down.											
fail-action-on-extender	Action on FortiExtender when interface fail.	option	-	soft-restart								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>soft-restart</i></td><td>Soft-restart-on-extender.</td></tr><tr><td><i>hard-restart</i></td><td>Hard-restart-on-extender.</td></tr><tr><td><i>reboot</i></td><td>Reboot-on-extender.</td></tr></table>	Option	Description	<i>soft-restart</i>	Soft-restart-on-extender.	<i>hard-restart</i>	Hard-restart-on-extender.	<i>reboot</i>	Reboot-on-extender.			
	Option	Description										
	<i>soft-restart</i>	Soft-restart-on-extender.										
	<i>hard-restart</i>	Hard-restart-on-extender.										
<i>reboot</i>	Reboot-on-extender.											
fail-alert-interfaces <name>	Names of the FortiProxy interfaces to which the link failure alert is sent. Names of the non-virtual interface.	string	Maximum length: 15									
dhcp-client-identifier	DHCP client identifier.	string	Maximum length: 48									
dhcp-renew-time	DHCP renew time in seconds , 0 means use the renew time provided by the server.	integer	Minimum value: 300 Maximum value: 604800	0								
ipunnumbered	Unnumbered IP used for PPPoE interfaces for which no unique local address is provided.	ipv4-address	Not Specified	0.0.0.0								
username	Username of the PPPoE account, provided by your ISP.	string	Maximum length: 64									
pppoe-unnumbered-negotiate	Enable/disable PPPoE unnumbered negotiation.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IP address negotiating for unnumbered.</td></tr></table>	Option	Description	<i>enable</i>	Enable IP address negotiating for unnumbered.							
	Option	Description										
<i>enable</i>	Enable IP address negotiating for unnumbered.											

Parameter	Description	Type	Size	Default				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable IP address negotiating for unnumbered.</td></tr></table>	Option	Description	<i>disable</i>	Disable IP address negotiating for unnumbered.			
Option	Description							
<i>disable</i>	Disable IP address negotiating for unnumbered.							
password	PPPoE account's password.	password	Not Specified					
idle-timeout	PPPoE auto disconnect after idle timeout seconds, 0 means no timeout.	integer	Minimum value: 0 Maximum value: 32767	0				
detected-peer-mtu	MTU of detected peer.	integer	Minimum value: 0 Maximum value: 4294967295	0				
disc-retry-timeout	Time in seconds to wait before retrying to start a PPPoE discovery, 0 means no timeout.	integer	Minimum value: 0 Maximum value: 4294967295	1				
padt-retry-timeout	PPPoE Active Discovery Terminate (PADT) used to terminate sessions after an idle time.	integer	Minimum value: 0 Maximum value: 4294967295	1				
service-name	PPPoE service name.	string	Maximum length: 63					
ac-name	PPPoE server name.	string	Maximum length: 63					
lcp-echo-interval	Time in seconds between PPPoE Link Control Protocol (LCP) echo requests.	integer	Minimum value: 0 Maximum value: 32767	5				
lcp-max-echo-fails	Maximum missed LCP echo messages before disconnect.	integer	Minimum value: 0 Maximum value: 32767	3				
defaultgw	Enable to get the gateway IP from the DHCP or PPPoE server.	option	-	enable				

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable default gateway.		
	<i>disable</i>	Disable default gateway.		
dns-server-override	Enable/disable use DNS acquired by DHCP or PPPoE.	option	-	enable
	Option Description			
	<i>enable</i>	Use DNS acquired by DHCP or PPPoE.		
	<i>disable</i>	No not use DNS acquired by DHCP or PPPoE.		
dns-server-protocol	DNS transport protocols.	option	-	cleartext
	Option Description			
	<i>cleartext</i>	DNS over UDP/53, DNS over TCP/53.		
	<i>dot</i>	DNS over TLS/853.		
	<i>doh</i>	DNS over HTTPS/443.		
auth-type	PPP authentication type to use.	option	-	auto
	Option Description			
	<i>auto</i>	Automatically choose authentication.		
	<i>pap</i>	PAP authentication.		
	<i>chap</i>	CHAP authentication.		
	<i>mschapv1</i>	MS-CHAPv1 authentication.		
	<i>mschapv2</i>	MS-CHAPv2 authentication.		
pptp-client	Enable/disable PPTP client.	option	-	disable
	Option Description			
	<i>enable</i>	Enable PPTP client.		
	<i>disable</i>	Disable PPTP client.		
pptp-user	PPTP user name.	string	Maximum length: 64	
pptp-password	PPTP password.	password	Not Specified	

Parameter	Description	Type	Size	Default												
pptp-server-ip	PPTP server IP address.	ipv4-address	Not Specified	0.0.0.0												
pptp-auth-type	PPTP authentication type.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Automatically choose authentication.</td></tr><tr><td>pap</td><td>PAP authentication.</td></tr><tr><td>chap</td><td>CHAP authentication.</td></tr><tr><td>mschapv1</td><td>MS-CHAPv1 authentication.</td></tr><tr><td>mschapv2</td><td>MS-CHAPv2 authentication.</td></tr></table>	Option	Description	auto	Automatically choose authentication.	pap	PAP authentication.	chap	CHAP authentication.	mschapv1	MS-CHAPv1 authentication.	mschapv2	MS-CHAPv2 authentication.			
Option	Description															
auto	Automatically choose authentication.															
pap	PAP authentication.															
chap	CHAP authentication.															
mschapv1	MS-CHAPv1 authentication.															
mschapv2	MS-CHAPv2 authentication.															
pptp-timeout	Idle timer in minutes (0 for disabled).	integer	Minimum value: 0 Maximum value: 65535	0												
arpforward	Enable/disable ARP forwarding.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable ARP forwarding.</td></tr><tr><td>disable</td><td>Disable ARP forwarding.</td></tr></table>	Option	Description	enable	Enable ARP forwarding.	disable	Disable ARP forwarding.									
Option	Description															
enable	Enable ARP forwarding.															
disable	Disable ARP forwarding.															
broadcast-forward	Enable/disable broadcast forwarding.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable broadcast forwarding.</td></tr><tr><td>disable</td><td>Disable broadcast forwarding.</td></tr></table>	Option	Description	enable	Enable broadcast forwarding.	disable	Disable broadcast forwarding.									
Option	Description															
enable	Enable broadcast forwarding.															
disable	Disable broadcast forwarding.															
bfd	Bidirectional Forwarding Detection (BFD) settings.	option	-	global												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>global</td><td>BFD behavior of this interface will be based on global configuration.</td></tr><tr><td>enable</td><td>Enable BFD on this interface and ignore global configuration.</td></tr><tr><td>disable</td><td>Disable BFD on this interface and ignore global configuration.</td></tr></table>	Option	Description	global	BFD behavior of this interface will be based on global configuration.	enable	Enable BFD on this interface and ignore global configuration.	disable	Disable BFD on this interface and ignore global configuration.							
Option	Description															
global	BFD behavior of this interface will be based on global configuration.															
enable	Enable BFD on this interface and ignore global configuration.															
disable	Disable BFD on this interface and ignore global configuration.															
bfd-desired-min-tx	BFD desired minimal transmit interval.	integer	Minimum value: 1 Maximum value: 100000	250												

Parameter	Description	Type	Size	Default								
bfd-detect-mult	BFD detection multiplier.	integer	Minimum value: 1 Maximum value: 50	3								
bfd-required-min-rx	BFD required minimal receive interval.	integer	Minimum value: 1 Maximum value: 100000	250								
l2forward	Enable/disable l2 forwarding.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable L2 forwarding.</td></tr><tr><td>disable</td><td>Disable L2 forwarding.</td></tr></table>	Option	Description	enable	Enable L2 forwarding.	disable	Disable L2 forwarding.					
Option	Description											
enable	Enable L2 forwarding.											
disable	Disable L2 forwarding.											
icmp-send-redirect	Enable/disable sending of ICMP redirects.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sending of ICMP redirects.</td></tr><tr><td>disable</td><td>Disable sending of ICMP redirects.</td></tr></table>	Option	Description	enable	Enable sending of ICMP redirects.	disable	Disable sending of ICMP redirects.					
Option	Description											
enable	Enable sending of ICMP redirects.											
disable	Disable sending of ICMP redirects.											
icmp-accept-redirect	Enable/disable ICMP accept redirect.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable ICMP accept redirect.</td></tr><tr><td>disable</td><td>Disable ICMP accept redirect.</td></tr></table>	Option	Description	enable	Enable ICMP accept redirect.	disable	Disable ICMP accept redirect.					
Option	Description											
enable	Enable ICMP accept redirect.											
disable	Disable ICMP accept redirect.											
stpforward	Enable/disable STP forwarding.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable STP forwarding.</td></tr><tr><td>disable</td><td>Disable STP forwarding.</td></tr></table>	Option	Description	enable	Enable STP forwarding.	disable	Disable STP forwarding.					
Option	Description											
enable	Enable STP forwarding.											
disable	Disable STP forwarding.											
stpforward-mode	Configure STP forwarding mode.	option	-	rpl-all-ext-id								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>rpl-all-ext-id</td><td>Replace all extension IDs (root, bridge).</td></tr><tr><td>rpl-bridge-ext-id</td><td>Replace the bridge extension ID only.</td></tr><tr><td>rpl-nothing</td><td>Replace nothing.</td></tr></table>	Option	Description	rpl-all-ext-id	Replace all extension IDs (root, bridge).	rpl-bridge-ext-id	Replace the bridge extension ID only.	rpl-nothing	Replace nothing.			
Option	Description											
rpl-all-ext-id	Replace all extension IDs (root, bridge).											
rpl-bridge-ext-id	Replace the bridge extension ID only.											
rpl-nothing	Replace nothing.											

Parameter	Description	Type	Size	Default																
macaddr	Change the interface's MAC address.	mac-address	Not Specified	00:00:00:00:00:00																
substitute-dst-mac	Destination MAC address that all packets are sent to from this interface.	mac-address	Not Specified	00:00:00:00:00:00																
large-receive-offload	Enable/disable large-receive-offload.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable large-receive-offload.</td></tr><tr><td><i>disable</i></td><td>Disable large-receive-offload.</td></tr></table>	Option	Description	<i>enable</i>	Enable large-receive-offload.	<i>disable</i>	Disable large-receive-offload.													
Option	Description																			
<i>enable</i>	Enable large-receive-offload.																			
<i>disable</i>	Disable large-receive-offload.																			
generic-receive-offload	Enable/disable generic-receive-offload.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable generic-receive-offload.</td></tr><tr><td><i>disable</i></td><td>Disable generic-receive-offload.</td></tr></table>	Option	Description	<i>enable</i>	Enable generic-receive-offload.	<i>disable</i>	Disable generic-receive-offload.													
Option	Description																			
<i>enable</i>	Enable generic-receive-offload.																			
<i>disable</i>	Disable generic-receive-offload.																			
speed	Interface speed. The default setting and the options available depend on the interface hardware.	option	-	auto																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Automatically adjust speed.</td></tr><tr><td><i>10full</i></td><td>10M full-duplex.</td></tr><tr><td><i>10half</i></td><td>10M half-duplex.</td></tr><tr><td><i>100full</i></td><td>100M full-duplex.</td></tr><tr><td><i>100half</i></td><td>100M half-duplex.</td></tr><tr><td><i>1000full</i></td><td>1000M full-duplex.</td></tr><tr><td><i>1000auto</i></td><td>1000M auto adjust.</td></tr></table>	Option	Description	<i>auto</i>	Automatically adjust speed.	<i>10full</i>	10M full-duplex.	<i>10half</i>	10M half-duplex.	<i>100full</i>	100M full-duplex.	<i>100half</i>	100M half-duplex.	<i>1000full</i>	1000M full-duplex.	<i>1000auto</i>	1000M auto adjust.			
Option	Description																			
<i>auto</i>	Automatically adjust speed.																			
<i>10full</i>	10M full-duplex.																			
<i>10half</i>	10M half-duplex.																			
<i>100full</i>	100M full-duplex.																			
<i>100half</i>	100M half-duplex.																			
<i>1000full</i>	1000M full-duplex.																			
<i>1000auto</i>	1000M auto adjust.																			
status	Bring the interface up or shut the interface down.	option	-	up																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>up</i></td><td>Bring the interface up.</td></tr><tr><td><i>down</i></td><td>Shut the interface down.</td></tr></table>	Option	Description	<i>up</i>	Bring the interface up.	<i>down</i>	Shut the interface down.													
Option	Description																			
<i>up</i>	Bring the interface up.																			
<i>down</i>	Shut the interface down.																			
netbios-forward	Enable/disable NETBIOS forwarding.	option	-	disable																

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable NETBIOS forwarding.</td></tr><tr><td><i>enable</i></td><td>Enable NETBIOS forwarding.</td></tr></table>	Option	Description	<i>disable</i>	Disable NETBIOS forwarding.	<i>enable</i>	Enable NETBIOS forwarding.															
	Option	Description																				
	<i>disable</i>	Disable NETBIOS forwarding.																				
<i>enable</i>	Enable NETBIOS forwarding.																					
wins-ip	WINS server IP.	ipv4-address	Not Specified	0.0.0.0																		
type	Interface type.	option	-	vlan																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>physical</i></td><td>Physical interface.</td></tr><tr><td><i>vlan</i></td><td>VLAN interface.</td></tr><tr><td><i>aggregate</i></td><td>Aggregate interface.</td></tr><tr><td><i>redundant</i></td><td>Redundant interface.</td></tr><tr><td><i>tunnel</i></td><td>Tunnel interface.</td></tr><tr><td><i>loopback</i></td><td>Loopback interface.</td></tr><tr><td><i>vdom-link</i></td><td>VDOM link interface.</td></tr><tr><td><i>vxlan</i></td><td>VXLAN interface.</td></tr></table>	Option	Description	<i>physical</i>	Physical interface.	<i>vlan</i>	VLAN interface.	<i>aggregate</i>	Aggregate interface.	<i>redundant</i>	Redundant interface.	<i>tunnel</i>	Tunnel interface.	<i>loopback</i>	Loopback interface.	<i>vdom-link</i>	VDOM link interface.	<i>vxlan</i>	VXLAN interface.			
	Option	Description																				
	<i>physical</i>	Physical interface.																				
	<i>vlan</i>	VLAN interface.																				
	<i>aggregate</i>	Aggregate interface.																				
	<i>redundant</i>	Redundant interface.																				
	<i>tunnel</i>	Tunnel interface.																				
	<i>loopback</i>	Loopback interface.																				
<i>vdom-link</i>	VDOM link interface.																					
<i>vxlan</i>	VXLAN interface.																					
dedicated-to	Configure interface for single purpose.	option	-	none																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Interface not dedicated for any purpose.</td></tr><tr><td><i>management</i></td><td>Dedicate this interface for management purposes only.</td></tr></table>	Option	Description	<i>none</i>	Interface not dedicated for any purpose.	<i>management</i>	Dedicate this interface for management purposes only.															
	Option	Description																				
	<i>none</i>	Interface not dedicated for any purpose.																				
<i>management</i>	Dedicate this interface for management purposes only.																					
trust-ip-1	Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0																		
trust-ip-2	Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0																		
trust-ip-3	Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0																		
trust-ip6-1	Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).	ipv6-prefix	Not Specified	::/0																		
trust-ip6-2	Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).	ipv6-prefix	Not Specified	::/0																		

Parameter	Description	Type	Size	Default						
trust-ip6-3	Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).	ipv6-prefix	Not Specified	::/0						
ring-rx	RX ring size.	integer	Minimum value: 0 Maximum value: 4294967295	0						
ring-tx	TX ring size.	integer	Minimum value: 0 Maximum value: 4294967295	0						
wccp	Enable/disable WCCP on this interface. Used for encapsulated WCCP communication between WCCP clients and servers.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WCCP protocol on this interface.</td></tr><tr><td><i>disable</i></td><td>Disable WCCP protocol on this interface.</td></tr></table>				Option	Description	<i>enable</i>	Enable WCCP protocol on this interface.	<i>disable</i>	Disable WCCP protocol on this interface.
Option	Description									
<i>enable</i>	Enable WCCP protocol on this interface.									
<i>disable</i>	Disable WCCP protocol on this interface.									
drop-overlapped-fragment	Enable/disable drop overlapped fragment packets.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable drop of overlapped fragment packets.</td></tr><tr><td><i>disable</i></td><td>Disable drop of overlapped fragment packets.</td></tr></table>				Option	Description	<i>enable</i>	Enable drop of overlapped fragment packets.	<i>disable</i>	Disable drop of overlapped fragment packets.
Option	Description									
<i>enable</i>	Enable drop of overlapped fragment packets.									
<i>disable</i>	Disable drop of overlapped fragment packets.									
drop-fragment	Enable/disable drop fragment packets.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable/disable drop fragment packets.</td></tr><tr><td><i>disable</i></td><td>Do not drop fragment packets.</td></tr></table>				Option	Description	<i>enable</i>	Enable/disable drop fragment packets.	<i>disable</i>	Do not drop fragment packets.
Option	Description									
<i>enable</i>	Enable/disable drop fragment packets.									
<i>disable</i>	Do not drop fragment packets.									
src-check	Enable/disable source IP check.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable source IP check.</td></tr><tr><td><i>disable</i></td><td>Disable source IP check.</td></tr></table>				Option	Description	<i>enable</i>	Enable source IP check.	<i>disable</i>	Disable source IP check.
Option	Description									
<i>enable</i>	Enable source IP check.									
<i>disable</i>	Disable source IP check.									

Parameter	Description	Type	Size	Default						
explicit-web-proxy	Enable/disable the explicit web proxy on this interface.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable explicit Web proxy on this interface.</td></tr><tr><td><i>disable</i></td><td>Disable explicit Web proxy on this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable explicit Web proxy on this interface.	<i>disable</i>	Disable explicit Web proxy on this interface.			
	Option	Description								
	<i>enable</i>	Enable explicit Web proxy on this interface.								
<i>disable</i>	Disable explicit Web proxy on this interface.									
explicit-ftp-proxy	Enable/disable the explicit FTP proxy on this interface.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable explicit FTP proxy on this interface.</td></tr><tr><td><i>disable</i></td><td>Disable explicit FTP proxy on this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable explicit FTP proxy on this interface.	<i>disable</i>	Disable explicit FTP proxy on this interface.			
	Option	Description								
	<i>enable</i>	Enable explicit FTP proxy on this interface.								
<i>disable</i>	Disable explicit FTP proxy on this interface.									
proxy-captive-portal	Enable/disable proxy captive portal on this interface.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable proxy captive portal on this interface.</td></tr><tr><td><i>disable</i></td><td>Disable proxy captive portal on this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable proxy captive portal on this interface.	<i>disable</i>	Disable proxy captive portal on this interface.			
	Option	Description								
	<i>enable</i>	Enable proxy captive portal on this interface.								
<i>disable</i>	Disable proxy captive portal on this interface.									
tcp-mss	TCP maximum segment size. 0 means do not change segment size.	integer	Minimum value: 48 Maximum value: 65535	0						
inbandwidth	Bandwidth limit for incoming traffic , 0 means unlimited.	integer	Minimum value: 0 Maximum value: 80000000	0						
outbandwidth	Bandwidth limit for outgoing traffic.	integer	Minimum value: 0 Maximum value: 80000000	0						
egress-shaping-profile	Outgoing traffic shaping profile.	string	Maximum length: 35							
ingress-shaping-profile	Incoming traffic shaping profile.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default						
disconnect-threshold	Time in milliseconds to wait before sending a notification that this interface is down or disconnected.	integer	Minimum value: 0 Maximum value: 10000	0						
spillover-threshold	Egress Spillover threshold , 0 means unlimited.	integer	Minimum value: 0 Maximum value: 16776000	0						
ingress-spillover-threshold	Ingress Spillover threshold , 0 means unlimited.	integer	Minimum value: 0 Maximum value: 16776000	0						
weight	Default weight for static routes (if route has no weight configured).	integer	Minimum value: 0 Maximum value: 255	0						
interface	Interface name.	string	Maximum length: 15							
external	Enable/disable identifying the interface as an external interface (which usually means it's connected to the Internet).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable identifying the interface as an external interface.</td></tr><tr><td><i>disable</i></td><td>Disable identifying the interface as an external interface.</td></tr></table>				Option	Description	<i>enable</i>	Enable identifying the interface as an external interface.	<i>disable</i>	Disable identifying the interface as an external interface.
Option	Description									
<i>enable</i>	Enable identifying the interface as an external interface.									
<i>disable</i>	Disable identifying the interface as an external interface.									
mtu-override	Enable to set a custom MTU for this interface.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override default MTU.</td></tr><tr><td><i>disable</i></td><td>Use default MTU.</td></tr></table>				Option	Description	<i>enable</i>	Override default MTU.	<i>disable</i>	Use default MTU.
Option	Description									
<i>enable</i>	Override default MTU.									
<i>disable</i>	Use default MTU.									
mtu	MTU value for this interface.	integer	Minimum value: 0 Maximum value: 4294967295	1500						
vlan-protocol	Ethernet protocol of VLAN.	option	-	8021q						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>8021q</td><td>IEEE 802.1Q.</td></tr><tr><td>8021ad</td><td>IEEE 802.1AD.</td></tr></table>	Option	Description	8021q	IEEE 802.1Q.	8021ad	IEEE 802.1AD.			
	Option	Description								
	8021q	IEEE 802.1Q.								
8021ad	IEEE 802.1AD.									
vlanid	VLAN ID.	integer	Minimum value: 1 Maximum value: 4094	0						
forward-domain	Transparent mode forward domain.	integer	Minimum value: 1 Maximum value: 4094	1						
remote-ip	Remote IP address of tunnel.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0						
member <interface-name>	Physical interfaces that belong to the aggregate or redundant interface. Physical interface name.	string	Maximum length: 79							
lacp-mode	LACP mode.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>static</td><td>Use static aggregation, do not send and ignore any LACP messages.</td></tr></table>	Option	Description	static	Use static aggregation, do not send and ignore any LACP messages.					
	Option	Description								
static	Use static aggregation, do not send and ignore any LACP messages.									
lacp-ha-secondary	LACP HA secondary member.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Allow HA secondary member to send/receive LACP messages.</td></tr><tr><td>disable</td><td>Block HA secondary member from sending/receiving LACP messages.</td></tr></table>	Option	Description	enable	Allow HA secondary member to send/receive LACP messages.	disable	Block HA secondary member from sending/receiving LACP messages.			
	Option	Description								
	enable	Allow HA secondary member to send/receive LACP messages.								
disable	Block HA secondary member from sending/receiving LACP messages.									
system-id-type	Method in which system ID is generated.	option	-	auto						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Use the MAC address of the first member.</td></tr><tr><td>user</td><td>User-defined system ID.</td></tr></table>	Option	Description	auto	Use the MAC address of the first member.	user	User-defined system ID.			
	Option	Description								
	auto	Use the MAC address of the first member.								
user	User-defined system ID.									
system-id	Define a system ID for the aggregate interface.	mac-address	Not Specified	00:00:00:00:00:00						
lacp-speed	How often the interface sends LACP messages.	option	-	slow						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>slow</i>	Send LACP message every 30 seconds.		
	<i>fast</i>	Send LACP message every second.		
min-links	Minimum number of aggregated ports that must be up.	integer	Minimum value: 1 Maximum value: 32	1
min-links-down	Action to take when less than the configured minimum number of links are active.	option	-	operational
	Option	Description		
	<i>operational</i>	Set the aggregate operationally down.		
	<i>administrative</i>	Set the aggregate administratively down.		
algorithm	Frame distribution algorithm.	option	-	L4
	Option	Description		
	<i>L2</i>	Use layer 2 address for distribution.		
	<i>L3</i>	Use layer 3 address for distribution.		
	<i>L4</i>	Use layer 4 information for distribution.		
	<i>Source-MAC</i>	Use source MAC address for distribution.		
link-up-delay	Number of milliseconds to wait before considering a link is up.	integer	Minimum value: 50 Maximum value: 3600000	50
aggregate-type	Type of aggregation.	option	-	physical
	Option	Description		
	<i>physical</i>	Physical interface aggregation.		
	<i>vxlan</i>	VXLAN interface aggregation.		
priority-override	Enable/disable fail back to higher priority port once recovered.	option	-	enable

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable fail back to higher priority port once recovered.</td></tr><tr><td><i>disable</i></td><td>Disable fail back to higher priority port once recovered.</td></tr></table>	Option	Description	<i>enable</i>	Enable fail back to higher priority port once recovered.	<i>disable</i>	Disable fail back to higher priority port once recovered.					
	Option	Description										
	<i>enable</i>	Enable fail back to higher priority port once recovered.										
<i>disable</i>	Disable fail back to higher priority port once recovered.											
aggregate	Aggregate interface.	string	Maximum length: 15									
redundant-interface	Redundant interface.	string	Maximum length: 15									
devindex	Device Index.	integer	Minimum value: 0 Maximum value: 4294967295	0								
switch	Contained in switch.	string	Maximum length: 15									
description	Description.	var-string	Maximum length: 255									
alias	Alias will be displayed with the interface name to make it easier to distinguish.	string	Maximum length: 25									
security-mode	Turn on captive portal authentication for this interface.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No security option.</td></tr><tr><td><i>captive-portal</i></td><td>Captive portal authentication.</td></tr><tr><td><i>802.1X</i></td><td>802.1X port-based authentication.</td></tr></table>	Option	Description	<i>none</i>	No security option.	<i>captive-portal</i>	Captive portal authentication.	<i>802.1X</i>	802.1X port-based authentication.			
	Option	Description										
	<i>none</i>	No security option.										
	<i>captive-portal</i>	Captive portal authentication.										
<i>802.1X</i>	802.1X port-based authentication.											
security-mac-auth-bypass	Enable/disable MAC authentication bypass.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mac-auth-only</i></td><td>Enable MAC authentication bypass without EAP.</td></tr><tr><td><i>enable</i></td><td>Enable MAC authentication bypass.</td></tr><tr><td><i>disable</i></td><td>Disable MAC authentication bypass.</td></tr></table>	Option	Description	<i>mac-auth-only</i>	Enable MAC authentication bypass without EAP.	<i>enable</i>	Enable MAC authentication bypass.	<i>disable</i>	Disable MAC authentication bypass.			
	Option	Description										
	<i>mac-auth-only</i>	Enable MAC authentication bypass without EAP.										
	<i>enable</i>	Enable MAC authentication bypass.										
<i>disable</i>	Disable MAC authentication bypass.											
security-external-web	URL of external authentication web server.	var-string	Maximum length: 1023									

Parameter	Description	Type	Size	Default										
security-external-logout	URL of external authentication logout server.	string	Maximum length: 127											
replacemsg-override-group	Replacement message override group.	string	Maximum length: 35											
security-redirect-url	URL redirection after disclaimer/authentication.	var-string	Maximum length: 1023											
auth-cert	HTTPS server certificate.	string	Maximum length: 35											
auth-portal-addr	Address of captive portal.	string	Maximum length: 63											
security-exempt-list	Name of security-exempt-list.	string	Maximum length: 35											
security-groups <name>	User groups that can authenticate with the captive portal. Names of user groups that can authenticate with the captive portal.	string	Maximum length: 79											
ike-saml-server	Configure IKE authentication SAML server.	string	Maximum length: 35											
role	Interface role.	option	-	undefined										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>lan</i></td><td>Connected to local network of endpoints.</td></tr><tr><td><i>wan</i></td><td>Connected to Internet.</td></tr><tr><td><i>dmz</i></td><td>Connected to server zone.</td></tr><tr><td><i>undefined</i></td><td>Interface has no specific role.</td></tr></table>				Option	Description	<i>lan</i>	Connected to local network of endpoints.	<i>wan</i>	Connected to Internet.	<i>dmz</i>	Connected to server zone.	<i>undefined</i>	Interface has no specific role.
Option	Description													
<i>lan</i>	Connected to local network of endpoints.													
<i>wan</i>	Connected to Internet.													
<i>dmz</i>	Connected to server zone.													
<i>undefined</i>	Interface has no specific role.													
snmp-index	Permanent SNMP Index of the interface.	integer	Minimum value: 1 Maximum value: 2147483647	0										
secondary-IP	Enable/disable adding a secondary IP to this interface.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable secondary IP.</td></tr><tr><td><i>disable</i></td><td>Disable secondary IP.</td></tr></table>				Option	Description	<i>enable</i>	Enable secondary IP.	<i>disable</i>	Disable secondary IP.				
Option	Description													
<i>enable</i>	Enable secondary IP.													
<i>disable</i>	Disable secondary IP.													

Parameter	Description	Type	Size	Default
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
eap-supPLICant	Enable/disable EAP-SupPLICant.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable EAP SupPLICant.		
	<i>disable</i>	Disable EAP SupPLICant.		
eap-method	EAP method.	option	-	
	Option	Description		
	<i>tls</i>	TLS.		
	<i>peap</i>	PEAP.		
eap-identity	EAP identity.	string	Maximum length: 35	
eap-password	EAP password.	password	Not Specified	
eap-ca-cert	EAP CA certificate name.	string	Maximum length: 79	
eap-user-cert	EAP user certificate name.	string	Maximum length: 35	

config client-options

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
code	DHCP client option code.	integer	Minimum value: 0 Maximum value: 255	0
type	DHCP client option type.	option	-	hex

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>hex</i>	DHCP option in hex.		
	<i>string</i>	DHCP option in string.		
	<i>ip</i>	DHCP option in IP.		
	<i>fqdn</i>	DHCP option in domain search option format.		
value	DHCP client option value.	string	Maximum length: 312	
ip	DHCP option IPs.	user	Not Specified	

config secondaryip

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	Secondary IP address of the interface.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
allowaccess	Management access settings for the secondary IP address.	option	-	
	Option	Description		
	<i>ping</i>	PING access.		
	<i>https</i>	HTTPS access.		
	<i>ssh</i>	SSH access.		
	<i>snmp</i>	SNMP access.		
	<i>http</i>	HTTP access.		
	<i>telnet</i>	TELNET access.		
	<i>fgfm</i>	FortiManager access.		
	<i>radius-acct</i>	RADIUS accounting access.		
	<i>probe-response</i>	Probe access.		
	<i>fabric</i>	Security Fabric access.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ftm</i></td><td>FTM access.</td></tr><tr><td><i>speed-test</i></td><td>Speed test access.</td></tr></table>	Option	Description	<i>ftm</i>	FTM access.	<i>speed-test</i>	Speed test access.					
	Option	Description										
	<i>ftm</i>	FTM access.										
<i>speed-test</i>	Speed test access.											
gwdetect	Enable/disable detect gateway alive for first.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable detect gateway alive for first.</td></tr><tr><td><i>disable</i></td><td>Disable detect gateway alive for first.</td></tr></table>	Option	Description	<i>enable</i>	Enable detect gateway alive for first.	<i>disable</i>	Disable detect gateway alive for first.					
	Option	Description										
	<i>enable</i>	Enable detect gateway alive for first.										
<i>disable</i>	Disable detect gateway alive for first.											
ping-serv-status	PING server status.	integer	Minimum value: 0 Maximum value: 255	0								
detectserver	Gateway's ping server for this IP.	user	Not Specified									
detectprotocol	Protocols used to detect the server.	option	-	ping								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING.</td></tr><tr><td><i>tcp-echo</i></td><td>TCP echo.</td></tr><tr><td><i>udp-echo</i></td><td>UDP echo.</td></tr></table>	Option	Description	<i>ping</i>	PING.	<i>tcp-echo</i>	TCP echo.	<i>udp-echo</i>	UDP echo.			
	Option	Description										
	<i>ping</i>	PING.										
	<i>tcp-echo</i>	TCP echo.										
<i>udp-echo</i>	UDP echo.											
ha-priority	HA election priority for the PING server.	integer	Minimum value: 1 Maximum value: 50	1								

config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

config ipv6

Parameter	Description	Type	Size	Default										
ip6-mode	Addressing mode (static, DHCP, delegated).	option	-	static										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static</i></td><td>Static setting.</td></tr><tr><td><i>dhcp</i></td><td>DHCPv6 client mode.</td></tr><tr><td><i>pppoe</i></td><td>IPv6 over PPPoE mode.</td></tr><tr><td><i>delegated</i></td><td>IPv6 address with delegated prefix.</td></tr></table>	Option	Description	<i>static</i>	Static setting.	<i>dhcp</i>	DHCPv6 client mode.	<i>pppoe</i>	IPv6 over PPPoE mode.	<i>delegated</i>	IPv6 address with delegated prefix.			
Option	Description													
<i>static</i>	Static setting.													
<i>dhcp</i>	DHCPv6 client mode.													
<i>pppoe</i>	IPv6 over PPPoE mode.													
<i>delegated</i>	IPv6 address with delegated prefix.													
nd-mode	Neighbor discovery mode.	option	-	basic										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>basic</i></td><td>Do not support SEND.</td></tr><tr><td><i>SEND-compatible</i></td><td>Support SEND.</td></tr></table>	Option	Description	<i>basic</i>	Do not support SEND.	<i>SEND-compatible</i>	Support SEND.							
Option	Description													
<i>basic</i>	Do not support SEND.													
<i>SEND-compatible</i>	Support SEND.													
nd-cert	Neighbor discovery certificate.	string	Maximum length: 35											
nd-security-level	Neighbor discovery security level.	integer	Minimum value: 0 Maximum value: 7	0										
nd-timestamp-delta	Neighbor discovery timestamp delta value.	integer	Minimum value: 1 Maximum value: 3600	300										
nd-timestamp-fuzz	Neighbor discovery timestamp fuzz factor.	integer	Minimum value: 1 Maximum value: 60	1										
nd-cga-modifier	Neighbor discovery CGA modifier.	user	Not Specified											
ip6-dns-server-override	Enable/disable using the DNS server acquired by DHCP.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable using the DNS server acquired by DHCP.</td></tr><tr><td><i>disable</i></td><td>Disable using the DNS server acquired by DHCP.</td></tr></table>	Option	Description	<i>enable</i>	Enable using the DNS server acquired by DHCP.	<i>disable</i>	Disable using the DNS server acquired by DHCP.							
Option	Description													
<i>enable</i>	Enable using the DNS server acquired by DHCP.													
<i>disable</i>	Disable using the DNS server acquired by DHCP.													

Parameter	Description	Type	Size	Default																		
ip6-address	Primary IPv6 address prefix. Syntax: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx.	ipv6-prefix	Not Specified	::/0																		
ip6-allowaccess	Allow management access to the interface.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING access.</td></tr><tr><td><i>https</i></td><td>HTTPS access.</td></tr><tr><td><i>ssh</i></td><td>SSH access.</td></tr><tr><td><i>snmp</i></td><td>SNMP access.</td></tr><tr><td><i>http</i></td><td>HTTP access.</td></tr><tr><td><i>telnet</i></td><td>TELNET access.</td></tr><tr><td><i>fgfm</i></td><td>FortiManager access.</td></tr><tr><td><i>fabric</i></td><td>Fabric access.</td></tr></table>	Option	Description	<i>ping</i>	PING access.	<i>https</i>	HTTPS access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.	<i>http</i>	HTTP access.	<i>telnet</i>	TELNET access.	<i>fgfm</i>	FortiManager access.	<i>fabric</i>	Fabric access.			
Option	Description																					
<i>ping</i>	PING access.																					
<i>https</i>	HTTPS access.																					
<i>ssh</i>	SSH access.																					
<i>snmp</i>	SNMP access.																					
<i>http</i>	HTTP access.																					
<i>telnet</i>	TELNET access.																					
<i>fgfm</i>	FortiManager access.																					
<i>fabric</i>	Fabric access.																					
ip6-send-adv	Enable/disable sending advertisements about the interface.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending advertisements about this interface.</td></tr><tr><td><i>disable</i></td><td>Disable sending advertisements about this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending advertisements about this interface.	<i>disable</i>	Disable sending advertisements about this interface.															
Option	Description																					
<i>enable</i>	Enable sending advertisements about this interface.																					
<i>disable</i>	Disable sending advertisements about this interface.																					
icmp6-send-redirect	Enable/disable sending of ICMPv6 redirects.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending of ICMPv6 redirects.</td></tr><tr><td><i>disable</i></td><td>Disable sending of ICMPv6 redirects.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending of ICMPv6 redirects.	<i>disable</i>	Disable sending of ICMPv6 redirects.															
Option	Description																					
<i>enable</i>	Enable sending of ICMPv6 redirects.																					
<i>disable</i>	Disable sending of ICMPv6 redirects.																					
ip6-manage-flag	Enable/disable the managed flag.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the managed IPv6 flag.</td></tr><tr><td><i>disable</i></td><td>Disable the managed IPv6 flag.</td></tr></table>	Option	Description	<i>enable</i>	Enable the managed IPv6 flag.	<i>disable</i>	Disable the managed IPv6 flag.															
Option	Description																					
<i>enable</i>	Enable the managed IPv6 flag.																					
<i>disable</i>	Disable the managed IPv6 flag.																					
ip6-other-flag	Enable/disable the other IPv6 flag.	option	-	disable																		

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the other IPv6 flag.</td></tr><tr><td><i>disable</i></td><td>Disable the other IPv6 flag.</td></tr></table>	Option	Description	<i>enable</i>	Enable the other IPv6 flag.	<i>disable</i>	Disable the other IPv6 flag.			
	Option	Description								
	<i>enable</i>	Enable the other IPv6 flag.								
<i>disable</i>	Disable the other IPv6 flag.									
ip6-max-interval	IPv6 maximum interval (4 to 1800 sec).	integer	Minimum value: 4 Maximum value: 1800	600						
ip6-min-interval	IPv6 minimum interval (3 to 1350 sec).	integer	Minimum value: 3 Maximum value: 1350	198						
ip6-link-mtu	IPv6 link MTU.	integer	Minimum value: 1280 Maximum value: 16000	0						
ra-send-mtu	Enable/disable sending link MTU in RA packet.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending link MTU in RA packet.</td></tr><tr><td><i>disable</i></td><td>Disable sending link MTU in RA packet.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending link MTU in RA packet.	<i>disable</i>	Disable sending link MTU in RA packet.			
	Option	Description								
	<i>enable</i>	Enable sending link MTU in RA packet.								
<i>disable</i>	Disable sending link MTU in RA packet.									
ip6-reachable-time	IPv6 reachable time (milliseconds; 0 means unspecified).	integer	Minimum value: 0 Maximum value: 3600000	0						
ip6-retrans-time	IPv6 retransmit time (milliseconds; 0 means unspecified).	integer	Minimum value: 0 Maximum value: 4294967295	0						
ip6-default-life	Default life (sec).	integer	Minimum value: 0 Maximum value: 9000	1800						
ip6-hop-limit	Hop limit (0 means unspecified).	integer	Minimum value: 0 Maximum value: 255	0						

Parameter	Description	Type	Size	Default
autoconf	Enable/disable address auto config.	option	-	disable
	Option Description			
	<i>enable</i>	Enable auto-configuration.		
	<i>disable</i>	Disable auto-configuration.		
unique-autoconf-addr	Enable/disable unique auto config address.	option	-	disable
	Option Description			
	<i>enable</i>	Enable unique auto-configuration address.		
	<i>disable</i>	Disable unique auto-configuration address.		
interface-identifier	IPv6 interface identifier.	ipv6-address	Not Specified	::
ip6-prefix-mode	Assigning a prefix from DHCP or RA.	option	-	dhcp6
	Option Description			
	<i>dhcp6</i>	Use delegated prefix from a DHCPv6 client to form a delegated IPv6 address.		
	<i>ra</i>	Use prefix from RA to form a delegated IPv6 address.		
ip6-delegated-prefix-iaid	IAID of obtained delegated-prefix from the upstream interface.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip6-upstream-interface	Interface name providing delegated information.	string	Maximum length: 15	
ip6-subnet	Subnet to routing prefix. Syntax: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx.	ipv6-prefix	Not Specified	::/0
dhcp6-relay-service	Enable/disable DHCPv6 relay.	option	-	disable
	Option Description			
	<i>disable</i>	Disable DHCPv6 relay		
	<i>enable</i>	Enable DHCPv6 relay.		
dhcp6-relay-type	DHCPv6 relay type.	option	-	regular

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>regular</i></td><td>Regular DHCP relay.</td></tr></table>	Option	Description	<i>regular</i>	Regular DHCP relay.							
	Option	Description										
	<i>regular</i>	Regular DHCP relay.										
dhcp6-relay-source-interface	Enable/disable use of address on this interface as the source address of the relay message.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Use address of the egress interface as source address of the relay message.</td></tr><tr><td><i>enable</i></td><td>Use address of this interface as source address of the relay message.</td></tr></table>	Option	Description	<i>disable</i>	Use address of the egress interface as source address of the relay message.	<i>enable</i>	Use address of this interface as source address of the relay message.					
	Option	Description										
	<i>disable</i>	Use address of the egress interface as source address of the relay message.										
<i>enable</i>	Use address of this interface as source address of the relay message.											
dhcp6-relay-ip	DHCPv6 relay IP address.	user	Not Specified									
dhcp6-client-options	DHCPv6 client options.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rapid</i></td><td>Send rapid commit option.</td></tr><tr><td><i>iapd</i></td><td>Send including IA-PD option.</td></tr><tr><td><i>iana</i></td><td>Send including IA-NA option.</td></tr></table>	Option	Description	<i>rapid</i>	Send rapid commit option.	<i>iapd</i>	Send including IA-PD option.	<i>iana</i>	Send including IA-NA option.			
	Option	Description										
	<i>rapid</i>	Send rapid commit option.										
	<i>iapd</i>	Send including IA-PD option.										
<i>iana</i>	Send including IA-NA option.											
dhcp6-prefix-delegation	Enable/disable DHCPv6 prefix delegation.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DHCPv6 prefix delegation.</td></tr><tr><td><i>disable</i></td><td>Disable DHCPv6 prefix delegation.</td></tr></table>	Option	Description	<i>enable</i>	Enable DHCPv6 prefix delegation.	<i>disable</i>	Disable DHCPv6 prefix delegation.					
	Option	Description										
	<i>enable</i>	Enable DHCPv6 prefix delegation.										
<i>disable</i>	Disable DHCPv6 prefix delegation.											
dhcp6-information-request	Enable/disable DHCPv6 information request.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DHCPv6 information request.</td></tr><tr><td><i>disable</i></td><td>Disable DHCPv6 information request.</td></tr></table>	Option	Description	<i>enable</i>	Enable DHCPv6 information request.	<i>disable</i>	Disable DHCPv6 information request.					
	Option	Description										
	<i>enable</i>	Enable DHCPv6 information request.										
<i>disable</i>	Disable DHCPv6 information request.											
cli-conn6-status	CLI IPv6 connection status.	integer	Minimum value: 0 Maximum value: 4294967295	0								

config ip6-extra-addr

Parameter	Description	Type	Size	Default
prefix	IPv6 address prefix.	ipv6-prefix	Not Specified	::/0

config ip6-prefix-list

Parameter	Description	Type	Size	Default						
prefix	IPv6 prefix.	ipv6-network	Not Specified	::/0						
autonomous-flag	Enable/disable the autonomous flag.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable the autonomous flag.</td></tr><tr><td>disable</td><td>Disable the autonomous flag.</td></tr></table>				Option	Description	enable	Enable the autonomous flag.	disable	Disable the autonomous flag.
	Option	Description								
	enable	Enable the autonomous flag.								
disable	Disable the autonomous flag.									
onlink-flag	Enable/disable the onlink flag.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable the onlink flag.</td></tr><tr><td>disable</td><td>Disable the onlink flag.</td></tr></table>				Option	Description	enable	Enable the onlink flag.	disable	Disable the onlink flag.
	Option	Description								
	enable	Enable the onlink flag.								
disable	Disable the onlink flag.									
valid-life-time	Valid life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295	2592000						
preferred-life-time	Preferred life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295	604800						
rdnss	Recursive DNS server option.	user	Not Specified							
dnssl <domain>	DNS search list option. Domain name.	string	Maximum length: 79							

config ip6-delegated-prefix-list

Parameter	Description	Type	Size	Default								
prefix-id	Prefix ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
upstream-interface	Name of the interface that provides delegated information.	string	Maximum length: 15									
delegated-prefix-iaid	IAID of obtained delegated-prefix from the upstream interface.	integer	Minimum value: 0 Maximum value: 4294967295	0								
autonomous-flag	Enable/disable the autonomous flag.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the autonomous flag.</td></tr><tr><td><i>disable</i></td><td>Disable the autonomous flag.</td></tr></table>				Option	Description	<i>enable</i>	Enable the autonomous flag.	<i>disable</i>	Disable the autonomous flag.		
Option	Description											
<i>enable</i>	Enable the autonomous flag.											
<i>disable</i>	Disable the autonomous flag.											
onlink-flag	Enable/disable the onlink flag.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the onlink flag.</td></tr><tr><td><i>disable</i></td><td>Disable the onlink flag.</td></tr></table>				Option	Description	<i>enable</i>	Enable the onlink flag.	<i>disable</i>	Disable the onlink flag.		
Option	Description											
<i>enable</i>	Enable the onlink flag.											
<i>disable</i>	Disable the onlink flag.											
subnet	Add subnet ID to routing prefix.	ipv6-network	Not Specified	::/0								
rdnss-service	Recursive DNS service option.	option	-	specify								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>delegated</i></td><td>Delegated RDNSS settings.</td></tr><tr><td><i>default</i></td><td>System RDNSS settings.</td></tr><tr><td><i>specify</i></td><td>Specify recursive DNS servers.</td></tr></table>				Option	Description	<i>delegated</i>	Delegated RDNSS settings.	<i>default</i>	System RDNSS settings.	<i>specify</i>	Specify recursive DNS servers.
Option	Description											
<i>delegated</i>	Delegated RDNSS settings.											
<i>default</i>	System RDNSS settings.											
<i>specify</i>	Specify recursive DNS servers.											
rdnss	Recursive DNS server option.	user	Not Specified									

config dhcp6-iapd-list

Parameter	Description	Type	Size	Default
iaid	Identity association identifier.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix-hint	DHCPv6 prefix that will be used as a hint to the upstream DHCPv6 server.	ipv6-network	Not Specified	::/0
prefix-hint-plt	DHCPv6 prefix hint preferred life time (sec), 0 means unlimited lease time.	integer	Minimum value: 0 Maximum value: 4294967295	604800
prefix-hint-vlt	DHCPv6 prefix hint valid life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295	2592000

config system ip-conflict status

List interface names and IP addresses in conflict.

```
config system ip-conflict status
    Description: List interface names and IP addresses in conflict.
end
```

config system ipam

Configure IP address management services.

```
config system ipam
    Description: Configure IP address management services.
    set status [enable|disable]
    set server-type {option}
    config pools
        Description: Configure IPAM pools.
        edit <name>
            set description {string}
            set subnet {ipv4-classnet}
        next
    end
config rules
```

```

Description: Configure IPAM allocation rules.
edit <name>
    set description {string}
    set device <name1>, <name2>, ...
    set interface <name1>, <name2>, ...
    set role [any|lan|...]
    set pool <name1>, <name2>, ...
    set dhcp [enable|disable]
next
end
end

```

config system ipam

Parameter	Description	Type	Size	Default						
status	Enable/disable IP address management services.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable integration with IP address management services.</td></tr><tr><td><i>disable</i></td><td>Disable integration with IP address management services.</td></tr></table>				Option	Description	<i>enable</i>	Enable integration with IP address management services.	<i>disable</i>	Disable integration with IP address management services.
	Option	Description								
	<i>enable</i>	Enable integration with IP address management services.								
<i>disable</i>	Disable integration with IP address management services.									
server-type	Configure the type of IPAM server to use.	option	-	fabric-root						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fabric-root</i></td><td>Use the IPAM server running on the Security Fabric root.</td></tr></table>				Option	Description	<i>fabric-root</i>	Use the IPAM server running on the Security Fabric root.		
	Option	Description								
<i>fabric-root</i>	Use the IPAM server running on the Security Fabric root.									

config pools

Parameter	Description	Type	Size	Default
name	IPAM pool name.	string	Maximum length: 79	
description	Description.	string	Maximum length: 127	
subnet	Configure IPAM pool subnet, Class A - Class B subnet.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

config rules

Parameter	Description	Type	Size	Default
name	IPAM rule name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default												
description	Description.	string	Maximum length: 127													
device <name>	Configure serial number or wildcard of FortiGate to match. FortiGate serial number or wildcard.	string	Maximum length: 79													
interface <name>	Configure name or wildcard of interface to match. Interface name or wildcard.	string	Maximum length: 79													
role	Configure role of interface to match.	option	-	any												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>any</td><td>Match any interface role.</td></tr><tr><td>lan</td><td>Match interface role lan.</td></tr><tr><td>wan</td><td>Match interface role wan.</td></tr><tr><td>dmz</td><td>Match interface role dmz.</td></tr><tr><td>undefined</td><td>Match interface role undefined.</td></tr></table>				Option	Description	any	Match any interface role.	lan	Match interface role lan.	wan	Match interface role wan.	dmz	Match interface role dmz.	undefined	Match interface role undefined.
Option	Description															
any	Match any interface role.															
lan	Match interface role lan.															
wan	Match interface role wan.															
dmz	Match interface role dmz.															
undefined	Match interface role undefined.															
pool <name>	Configure name of IPAM pool to use. Ipam pool name.	string	Maximum length: 79													
dhcp	Enable/disable DHCP server for matching IPAM interfaces.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable DHCP server on matched IPAM interface.</td></tr><tr><td>disable</td><td>Disable DHCP server on matched IPAM interface.</td></tr></table>				Option	Description	enable	Enable DHCP server on matched IPAM interface.	disable	Disable DHCP server on matched IPAM interface.						
Option	Description															
enable	Enable DHCP server on matched IPAM interface.															
disable	Disable DHCP server on matched IPAM interface.															

config system ips-urlfilter-dns

Configure IPS URL filter DNS servers.

```

config system ips-urlfilter-dns
    Description: Configure IPS URL filter DNS servers.
    edit <address>
        set status [enable|disable]
        set ipv6-capability [enable|disable]
    next
end

```

config system ips-urlfilter-dns

Parameter	Description	Type	Size	Default
address	DNS server IP address.	ipv4-address	Not Specified	0.0.0.0
status	Enable/disable using this DNS server for IPS URL filter DNS queries.	option	-	enable
	Option	Description		
	enable	Enable this DNS server for IPS URL filter DNS queries.		
	disable	Disable this DNS server for IPS URL filter DNS queries.		
ipv6-capability	Enable/disable this server for IPv6 queries.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		

config system ips-urlfilter-dns6

Configure IPS URL filter IPv6 DNS servers.

```
config system ips-urlfilter-dns6
    Description: Configure IPS URL filter IPv6 DNS servers.
    edit <address6>
        set status [enable|disable]
    next
end
```

config system ips-urlfilter-dns6

Parameter	Description	Type	Size	Default
address6	IPv6 address of DNS server.	ipv6-address	Not Specified	::
status	Enable/disable this server for IPv6 DNS queries.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config system ips

Configure IPS system settings.

```
config system ips
    Description: Configure IPS system settings.
    set signature-hold-time {user}
    set override-signature-hold-by-id [enable|disable]
end
```

config system ips

Parameter	Description	Type	Size	Default
signature-hold-time	Time to hold and monitor IPS signatures. Format <#d##h>.	user	Not Specified	0h
override-signature-hold-by-id	Enable/disable override of hold of triggering signatures that are specified by IDs regardless of hold.	option	-	enable
		Option	Description	
		<i>enable</i>	Allow the signatures specified by IDs to be triggered even if they are on hold.	
		<i>disable</i>	Do not trigger the signatures that are on hold.	

config system ipv6-neighbor-cache

Configure IPv6 neighbor cache table.

```
config system ipv6-neighbor-cache
    Description: Configure IPv6 neighbor cache table.
    edit <id>
        set interface {string}
        set ipv6 {ipv6-address}
        set mac {mac-address}
    next
end
```

config system ipv6-neighbor-cache

Parameter	Description	Type	Size	Default
id	Unique integer ID of the entry.	integer	Minimum value: 0 Maximum value: 4294967295	0
interface	Select the associated interface name from available options.	string	Maximum length: 15	
ipv6	IPv6 address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::
mac	MAC address (format: xx:xx:xx:xx:xx:xx).	mac-address	Not Specified	00:00:00:00:00:00

config system link-monitor

Configure Link Health Monitor.

```
config system link-monitor
  Description: Configure Link Health Monitor.
  edit <name>
    set addr-mode [ipv4|ipv6]
    set srcintf {string}
    set server-config [default|individual]
    set server <address1>, <address2>, ...
    set protocol {option1}, {option2}, ...
    set port {integer}
    set gateway-ip {ipv4-address-any}
    set gateway-ip6 {ipv6-address}
    set route <subnet1>, <subnet2>, ...
    set source-ip {ipv4-address-any}
    set source-ip6 {ipv6-address}
    set http-get {string}
    set http-agent {string}
    set http-match {string}
    set interval {integer}
    set probe-timeout {integer}
    set failtime {integer}
    set recoverytime {integer}
    set probe-count {integer}
    set security-mode [none|authentication]
    set password {password}
    set packet-size {integer}
    set ha-priority {integer}
    set fail-weight {integer}
    set update-cascade-interface [enable|disable]
    set update-static-route [enable|disable]
```



```

set update-policy-route [enable|disable]
set status [enable|disable]
set diffservcode {user}
set class-id {integer}
set service-detection [enable|disable]
config server-list
    Description: Servers for link-monitor to monitor.
    edit <id>
        set dst {string}
        set protocol {option1}, {option2}, ...
        set port {integer}
        set weight {integer}
    next
end
next
end

```

config system link-monitor

Parameter	Description	Type	Size	Default								
name	Link monitor name.	string	Maximum length: 35									
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4</td><td>IPv4 mode.</td></tr><tr><td>ipv6</td><td>IPv6 mode.</td></tr></table>				Option	Description	ipv4	IPv4 mode.	ipv6	IPv6 mode.		
	Option	Description										
	ipv4	IPv4 mode.										
ipv6	IPv6 mode.											
srcintf	Interface that receives the traffic to be monitored.	string	Maximum length: 15									
server-config	Mode of server configuration.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>All servers share the same attributes.</td></tr><tr><td>individual</td><td>Some attributes can be specified for individual servers.</td></tr></table>				Option	Description	default	All servers share the same attributes.	individual	Some attributes can be specified for individual servers.		
	Option	Description										
	default	All servers share the same attributes.										
individual	Some attributes can be specified for individual servers.											
server <address>	IP address of the server(s) to be monitored. Server address.	string	Maximum length: 79									
protocol	Protocols used to monitor the server.	option	-	ping								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ping</td><td>PING link monitor.</td></tr><tr><td>tcp-echo</td><td>TCP echo link monitor.</td></tr><tr><td>udp-echo</td><td>UDP echo link monitor.</td></tr></table>				Option	Description	ping	PING link monitor.	tcp-echo	TCP echo link monitor.	udp-echo	UDP echo link monitor.
	Option	Description										
	ping	PING link monitor.										
	tcp-echo	TCP echo link monitor.										
udp-echo	UDP echo link monitor.											

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>HTTP-GET link monitor.</td></tr><tr><td><i>twamp</i></td><td>TWAMP link monitor.</td></tr></table>	Option	Description	<i>http</i>	HTTP-GET link monitor.	<i>twamp</i>	TWAMP link monitor.			
	Option	Description								
	<i>http</i>	HTTP-GET link monitor.								
<i>twamp</i>	TWAMP link monitor.									
port	Port number of the traffic to be used to monitor the server.	integer	Minimum value: 1 Maximum value: 65535	0						
gateway-ip	Gateway IP address used to probe the server.	ipv4-address-any	Not Specified	0.0.0.0						
gateway-ip6	Gateway IPv6 address used to probe the server.	ipv6-address	Not Specified	::						
route <subnet>	Subnet to monitor. IP and netmask (x.x.x.x/y).	string	Maximum length: 79							
source-ip	Source IP address used in packet to the server.	ipv4-address-any	Not Specified	0.0.0.0						
source-ip6	Source IPv6 address used in packet to the server.	ipv6-address	Not Specified	::						
http-get	If you are monitoring an HTML server you can send an HTTP-GET request with a custom string. Use this option to define the string.	string	Maximum length: 1024	/						
http-agent	String in the http-agent field in the HTTP header.	string	Maximum length: 1024	Chrome/ Safari/						
http-match	String that you expect to see in the HTTP-GET requests of the traffic to be monitored.	string	Maximum length: 1024							
interval	Detection interval in milliseconds.	integer	Minimum value: 20 Maximum value: 3600000	500						
probe-timeout	Time to wait before a probe packet is considered lost.	integer	Minimum value: 20 Maximum value: 5000	500						

Parameter	Description	Type	Size	Default						
failtime	Number of retry attempts before the server is considered down.	integer	Minimum value: 1 Maximum value: 3600	5						
recoverytime	Number of successful responses received before server is considered recovered.	integer	Minimum value: 1 Maximum value: 3600	5						
probe-count	Number of most recent probes that should be used to calculate latency and jitter.	integer	Minimum value: 5 Maximum value: 30	30						
security-mode	Twamp controller security mode.	option	-	none						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Unauthenticated mode.</td></tr><tr><td><i>authentication</i></td><td>Authenticated mode.</td></tr></table>				Option	Description	<i>none</i>	Unauthenticated mode.	<i>authentication</i>	Authenticated mode.
Option	Description									
<i>none</i>	Unauthenticated mode.									
<i>authentication</i>	Authenticated mode.									
password	TWAMP controller password in authentication mode.	password	Not Specified							
packet-size	Packet size of a TWAMP test session.	integer	Minimum value: 64 Maximum value: 1024	64						
ha-priority	HA election priority.	integer	Minimum value: 1 Maximum value: 50	1						
fail-weight	Threshold weight to trigger link failure alert.	integer	Minimum value: 0 Maximum value: 255	0						
update-cascade-interface	Enable/disable update cascade interface.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable update cascade interface.</td></tr><tr><td><i>disable</i></td><td>Disable update cascade interface.</td></tr></table>				Option	Description	<i>enable</i>	Enable update cascade interface.	<i>disable</i>	Disable update cascade interface.
Option	Description									
<i>enable</i>	Enable update cascade interface.									
<i>disable</i>	Disable update cascade interface.									

Parameter	Description	Type	Size	Default						
update-static-route	Enable/disable updating the static route.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable updating the static route.</td></tr><tr><td><i>disable</i></td><td>Disable updating the static route.</td></tr></table>	Option	Description	<i>enable</i>	Enable updating the static route.	<i>disable</i>	Disable updating the static route.			
Option	Description									
<i>enable</i>	Enable updating the static route.									
<i>disable</i>	Disable updating the static route.									
update-policy-route	Enable/disable updating the policy route.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable updating the policy route.</td></tr><tr><td><i>disable</i></td><td>Disable updating the policy route.</td></tr></table>	Option	Description	<i>enable</i>	Enable updating the policy route.	<i>disable</i>	Disable updating the policy route.			
Option	Description									
<i>enable</i>	Enable updating the policy route.									
<i>disable</i>	Disable updating the policy route.									
status	Enable/disable this link monitor.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this link monitor.</td></tr><tr><td><i>disable</i></td><td>Disable this link monitor.</td></tr></table>	Option	Description	<i>enable</i>	Enable this link monitor.	<i>disable</i>	Disable this link monitor.			
Option	Description									
<i>enable</i>	Enable this link monitor.									
<i>disable</i>	Disable this link monitor.									
diffservcode	Differentiated services code point (DSCP) in the IP header of the probe packet.	user	Not Specified							
class-id	Traffic class ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
service-detection	Only use monitor to read quality values. If enabled, static routes and cascade interfaces will not be updated.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Only use monitor for service-detection.</td></tr><tr><td><i>disable</i></td><td>Monitor will update routes/interfaces on link failure.</td></tr></table>	Option	Description	<i>enable</i>	Only use monitor for service-detection.	<i>disable</i>	Monitor will update routes/interfaces on link failure.			
Option	Description									
<i>enable</i>	Only use monitor for service-detection.									
<i>disable</i>	Monitor will update routes/interfaces on link failure.									

config server-list

Parameter	Description	Type	Size	Default
id	Server ID.	integer	Minimum value: 1 Maximum value: 32	0
dst	IP address of the server to be monitored.	string	Maximum length: 64	
protocol	Protocols used to monitor the server.	option	-	ping
	Option	Description		
	ping	PING link monitor.		
	tcp-echo	TCP echo link monitor.		
	udp-echo	UDP echo link monitor.		
	http	HTTP-GET link monitor.		
	twamp	TWAMP link monitor.		
port	Port number of the traffic to be used to monitor the server.	integer	Minimum value: 1 Maximum value: 65535	0
weight	Weight of the monitor to this dst.	integer	Minimum value: 0 Maximum value: 255	0

config system management-tunnel

Management tunnel configuration.

```

config system management-tunnel
    Description: Management tunnel configuration.
    set status [enable|disable]
    set allow-config-restore [enable|disable]
    set allow-push-configuration [enable|disable]
    set allow-push-firmware [enable|disable]
    set allow-collect-statistics [enable|disable]
    set authorized-manager-only [enable|disable]
    set serial-number {user}
end

```

config system management-tunnel

Parameter	Description	Type	Size	Default
status	Enable/disable FGFM tunnel.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable management tunnel.		
	<i>disable</i>	Disable management tunnel.		
allow-config-restore	Enable/disable allow config restore.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable allow config restore.		
	<i>disable</i>	Disable allow config restore.		
allow-push-configuration	Enable/disable push configuration.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable push configuration.		
	<i>disable</i>	Disable push configuration.		
allow-push-firmware	Enable/disable push firmware.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable push firmware.		
	<i>disable</i>	Disable push firmware.		
allow-collect-statistics	Enable/disable collection of run time statistics.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable collection of run time statistics.		
	<i>disable</i>	Disable collection of run time statistics.		
authorized-manager-only	Enable/disable restriction of authorized manager only.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable restriction of authorized manager only.		
	<i>disable</i>	Disable restriction of authorized manager only.		

Parameter	Description	Type	Size	Default
serial-number	Serial number.	user	Not Specified	

config system mgmt-csum

System checksum for FortiManager use only.

```
config system mgmt-csum
  Description: System checksum for FortiManager use only.
end
```

config system nethsm

Configure system nethsm.

```
config system nethsm
  Description: Configure system nethsm.
  set status [enable|disable]
  set vendor [safenet|primus]
  set interface {string}
  set receivetimeout {integer}
  config servers
    Description: NetHSM server list.
    edit <name>
      set server {string}
      set port {integer}
      set server-cert {user}
      set htl [enable|disable]
    next
  end
  config slots
    Description: NetHSM slot list.
    edit <name>
      set id {integer}
      set password {password}
      set for-ha [yes|no]
    next
  end
  set ha [enable|disable]
  set ha-status-pulling-interval {integer}
  config hagroups
    Description: NetHSM HA group list.
    edit <name>
      set member <name1>, <name2>, ...
    next
  end
  set rsa-mech-remap [enable|disable]
  set primus-cfg {user}
```

```

set secret-content {varlen_password}
config partitions
    Description: Set Hardware Security Module partition information.
    edit <name>
        set slot-id {integer}
        set pkcs11-pin {password}
    next
end
end

```

config system nethsm

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable system network HSM.		
	<i>disable</i>	Disable system network HSM.		
vendor	Vendor.	option	-	safenet
	Option	Description		
	<i>safenet</i>	SafeNet HSM.		
	<i>primus</i>	Securosys Primus HSM.		
interface	Outgoing interface	string	Maximum length: 15	
receivetimeout	Receive timeout, specified in ms.	integer	Minimum value: 0 Maximum value: 4294967295	20000
ha	HA option.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable HA.		
	<i>disable</i>	Disable HA.		
ha-status-pulling-interval	Interval to pull HA status in minutes.	integer	Minimum value: 0 Maximum value: 60	1

Parameter	Description	Type	Size	Default						
rsa-mech-remap	RSA Mechanism Remap option. Enable it if Luna server is running in FIPS mode and firmware version is 6.22.* or greater.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable RSA Mechanism Remap.</td></tr><tr><td><i>disable</i></td><td>Disable RSA Mechanism Remap.</td></tr></table>				Option	Description	<i>enable</i>	Enable RSA Mechanism Remap.	<i>disable</i>	Disable RSA Mechanism Remap.
Option	Description									
<i>enable</i>	Enable RSA Mechanism Remap.									
<i>disable</i>	Disable RSA Mechanism Remap.									
primus-cfg	Set primus.cfg file content	user	Not Specified							
secret-content	Set secret content	varlen_ password	Not Specified							

config servers

Parameter	Description	Type	Size	Default						
name	NetHSM server name.	string	Maximum length: 35							
server	{<name_str ip_str>} NetHSM server domain name or IP.	string	Maximum length: 63							
port	NetHSM server port.	integer	Minimum value: 1 Maximum value: 65535	1792						
server-cert	NetHSM server certificate.	user	Not Specified							
htl	HTL option.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTL.</td></tr><tr><td><i>disable</i></td><td>Disable HTL.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTL.	<i>disable</i>	Disable HTL.			
Option	Description									
<i>enable</i>	Enable HTL.									
<i>disable</i>	Disable HTL.									

config slots

Parameter	Description	Type	Size	Default
name	NetHSM slot name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
id	NetHSM slot ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
password	NetHSM slot access password.	password	Not Specified	
for-ha	HA option.	option	-	no
	Option	Description		
	yes	HA slot.		
	no	Regular slot.		

config hagroups

Parameter	Description	Type	Size	Default
name	NetHSM HA group name.	string	Maximum length: 35	
member <name>	HA group members. NetHSM HA group member (slot names).	string	Maximum length: 79	

config partitions

Parameter	Description	Type	Size	Default
name	Name of the Hardware Security Module partition.	string	Maximum length: 35	
slot-id	Slot ID number of the Hardware Security Module partition.	integer	Minimum value: 0 Maximum value: 4294967295	0
pkcs11-pin	PKCS#11 PIN for the Hardware Security Module partition.	password	Not Specified	

config system network-visibility

Configure network visibility settings.

```

config system network-visibility
    Description: Configure network visibility settings.
    set destination-visibility [disable|enable]
    set source-location [disable|enable]
    set destination-hostname-visibility [disable|enable]
    set hostname-ttl {integer}
    set hostname-limit {integer}
    set destination-location [disable|enable]
end

```

config system network-visibility

Parameter	Description	Type	Size	Default
destination-visibility	Enable/disable logging of destination visibility.	option	-	enable
	Option	Description		
	disable	Disable logging of destination visibility.		
	enable	Enable logging of destination visibility.		
source-location	Enable/disable logging of source geographical location visibility.	option	-	enable
	Option	Description		
	disable	Disable logging of source geographical location visibility.		
	enable	Enable logging of source geographical location visibility.		
destination-hostname-visibility	Enable/disable logging of destination hostname visibility.	option	-	enable
	Option	Description		
	disable	Disable logging of destination hostname visibility.		
	enable	Enable logging of destination hostname visibility.		
hostname-ttl	TTL of hostname table entries.	integer	Minimum value: 60 Maximum value: 86400	86400
hostname-limit	Limit of the number of hostname table entries.	integer	Minimum value: 0 Maximum value: 50000	5000

Parameter	Description	Type	Size	Default
destination-location	Enable/disable logging of destination geographical location visibility.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable logging of destination geographical location visibility.		
	<i>enable</i>	Enable logging of destination geographical location visibility.		

config system ntp

Configure system NTP information.

```
config system ntp
    Description: Configure system NTP information.
    set ntpsync [enable|disable]
    set type [fortiguard|custom]
    set syncinterval {integer}
    config ntpserver
        Description: Configure the FortiProxy to connect to any available third-party NTP
server.
        edit <id>
            set server {string}
            set ntpv3 [enable|disable]
            set authentication [enable|disable]
            set key {password}
            set key-id {integer}
            set interface-select-method [auto|specify]
            set interface {string}
        next
    end
    set source-ip {ipv4-address}
    set source-ip6 {ipv6-address}
    set server-mode [enable|disable]
    set authentication [enable|disable]
    set key-type [MD5|SHA1]
    set key {password}
    set key-id {integer}
    set interface <interface-name1>, <interface-name2>, ...
end
```

config system ntp

Parameter	Description	Type	Size	Default
ntpsync	Enable/disable setting the FortiProxy system time by synchronizing with an NTP Server.	option	-	disable

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable synchronization with NTP Server.</td></tr><tr><td><i>disable</i></td><td>Disable synchronization with NTP Server.</td></tr></table>	Option	Description	<i>enable</i>	Enable synchronization with NTP Server.	<i>disable</i>	Disable synchronization with NTP Server.			
	Option	Description								
	<i>enable</i>	Enable synchronization with NTP Server.								
<i>disable</i>	Disable synchronization with NTP Server.									
type	Use the FortiGuard NTP server or any other available NTP Server.	option	-	fortiguard						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortiguard</i></td><td>Use the FortiGuard NTP server.</td></tr><tr><td><i>custom</i></td><td>Use any other available NTP server.</td></tr></table>	Option	Description	<i>fortiguard</i>	Use the FortiGuard NTP server.	<i>custom</i>	Use any other available NTP server.			
	Option	Description								
	<i>fortiguard</i>	Use the FortiGuard NTP server.								
<i>custom</i>	Use any other available NTP server.									
syncinterval	NTP synchronization interval.	integer	Minimum value: 1 Maximum value: 1440	60						
source-ip	Source IP address for communication to the NTP server.	ipv4-address	Not Specified	0.0.0.0						
source-ip6	Source IPv6 address for communication to the NTP server.	ipv6-address	Not Specified	::						
server-mode	Enable/disable FortiProxy NTP Server Mode. Your FortiProxy becomes an NTP server for other devices on your network. The FortiProxy relays NTP requests to its configured NTP server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiProxy NTP Server Mode.</td></tr><tr><td><i>disable</i></td><td>Disable FortiProxy NTP Server Mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiProxy NTP Server Mode.	<i>disable</i>	Disable FortiProxy NTP Server Mode.			
	Option	Description								
	<i>enable</i>	Enable FortiProxy NTP Server Mode.								
<i>disable</i>	Disable FortiProxy NTP Server Mode.									
authentication	Enable/disable authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable authentication.</td></tr><tr><td><i>disable</i></td><td>Disable authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable authentication.	<i>disable</i>	Disable authentication.			
	Option	Description								
	<i>enable</i>	Enable authentication.								
<i>disable</i>	Disable authentication.									
key-type	Key type for authentication (MD5, SHA1).	option	-	MD5						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>MD5</i></td><td>Use MD5 to authenticate the message.</td></tr><tr><td><i>SHA1</i></td><td>Use SHA1 to authenticate the message.</td></tr></table>	Option	Description	<i>MD5</i>	Use MD5 to authenticate the message.	<i>SHA1</i>	Use SHA1 to authenticate the message.			
	Option	Description								
	<i>MD5</i>	Use MD5 to authenticate the message.								
<i>SHA1</i>	Use SHA1 to authenticate the message.									

Parameter	Description	Type	Size	Default
key	Key for authentication.	password	Not Specified	
key-id	Key ID for authentication.	integer	Minimum value: 0 Maximum value: 4294967295	0
interface <interface-name>	FortiProxy interface(s) with NTP server mode enabled. Devices on your network can contact these interfaces for NTP services. Interface name.	string	Maximum length: 79	

config ntpserver

Parameter	Description	Type	Size	Default						
id	NTP server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
server	IP address or hostname of the NTP Server.	string	Maximum length: 63							
ntp3	Enable to use NTPv3 instead of NTPv4.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable NTPv3.</td></tr><tr><td>disable</td><td>Disable NTPv3 (use NTPv4).</td></tr></table>				Option	Description	enable	Enable NTPv3.	disable	Disable NTPv3 (use NTPv4).
	Option	Description								
	enable	Enable NTPv3.								
disable	Disable NTPv3 (use NTPv4).									
authentication	Enable/disable MD5(NTPv3)/SHA1(NTPv4) authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable MD5(NTPv3)/SHA1(NTPv4) authentication.</td></tr><tr><td>disable</td><td>Disable MD5(NTPv3)/SHA1(NTPv4) authentication.</td></tr></table>				Option	Description	enable	Enable MD5(NTPv3)/SHA1(NTPv4) authentication.	disable	Disable MD5(NTPv3)/SHA1(NTPv4) authentication.
	Option	Description								
	enable	Enable MD5(NTPv3)/SHA1(NTPv4) authentication.								
disable	Disable MD5(NTPv3)/SHA1(NTPv4) authentication.									
key	Key for MD5(NTPv3)/SHA1(NTPv4) authentication.	password	Not Specified							
key-id	Key ID for authentication.	integer	Minimum value: 0 Maximum value: 4294967295	0						

Parameter	Description	Type	Size	Default
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config system object-tagging

Configure object tagging.

```
config system object-tagging
  Description: Configure object tagging.
  edit <category>
    set address [disable|mandatory|...]
    set device [disable|mandatory|...]
    set interface [disable|mandatory|...]
    set multiple [enable|disable]
    set color {integer}
    set tags <name1>, <name2>, ...
  next
end
```

config system object-tagging

Parameter	Description	Type	Size	Default
category	Tag Category.	string	Maximum length: 63	
address	Address.	option	-	optional
	Option	Description		
	<i>disable</i>	Disable.		
	<i>mandatory</i>	Mandatory.		
	<i>optional</i>	Optional.		
device	Device.	option	-	optional

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable.		
	<i>mandatory</i>	Mandatory.		
	<i>optional</i>	Optional.		
interface	Interface.	option	-	optional
	Option	Description		
	<i>disable</i>	Disable.		
	<i>mandatory</i>	Mandatory.		
	<i>optional</i>	Optional.		
multiple	Allow multiple tag selection.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable multi-tagging.		
	<i>disable</i>	Disable multi-tagging.		
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
tags <name>	Tags. Tag name.	string	Maximum length: 79	

config system password-policy-guest-admin

Configure the password policy for guest administrators.

```

config system password-policy-guest-admin
    Description: Configure the password policy for guest administrators.
    set status [enable|disable]
    set apply-to {option1}, {option2}, ...
    set minimum-length {integer}
    set min-lower-case-letter {integer}
    set min-upper-case-letter {integer}
    set min-non-alphanumeric {integer}
    set min-number {integer}
    set min-change-characters {integer}
    set expire-status [enable|disable]
    set expire-day {integer}
    set reuse-password [enable|disable]

```



```

set password-history {integer}
end

```

config system password-policy-guest-admin

Parameter	Description	Type	Size	Default						
status	Enable/disable setting a password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable password policy.</td></tr><tr><td><i>disable</i></td><td>Disable password policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable password policy.	<i>disable</i>	Disable password policy.			
Option	Description									
<i>enable</i>	Enable password policy.									
<i>disable</i>	Disable password policy.									
apply-to	Guest administrator to which this password policy applies.	option	-	guest-admin-password						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>guest-admin-password</i></td><td>Apply to guest administrator password.</td></tr></table>	Option	Description	<i>guest-admin-password</i>	Apply to guest administrator password.					
Option	Description									
<i>guest-admin-password</i>	Apply to guest administrator password.									
minimum-length	Minimum password length.	integer	Minimum value: 8 Maximum value: 128	8						
min-lower-case-letter	Minimum number of lowercase characters in password.	integer	Minimum value: 0 Maximum value: 128	0						
min-upper-case-letter	Minimum number of uppercase characters in password.	integer	Minimum value: 0 Maximum value: 128	0						
min-non-alphanumeric	Minimum number of non-alphanumeric characters in password.	integer	Minimum value: 0 Maximum value: 128	0						
min-number	Minimum number of numeric characters in password.	integer	Minimum value: 0 Maximum value: 128	0						

Parameter	Description	Type	Size	Default
min-change-characters	Minimum number of unique characters in new password which do not exist in old password.	integer	Minimum value: 0 Maximum value: 128	0
expire-status	Enable/disable password expiration.	option	-	disable
	Option	Description		
	<i>enable</i>	Passwords expire after expire-day days.		
	<i>disable</i>	Passwords do not expire.		
expire-day	Number of days after which passwords expire.	integer	Minimum value: 1 Maximum value: 999	90
reuse-password	Enable/disable reuse of password. If both reuse-password and min-change-characters are enabled, min-change-characters overrides.	option	-	enable
	Option	Description		
	<i>enable</i>	Administrators are allowed to reuse the same password.		
	<i>disable</i>	Administrators must create a new password.		
password-history	Number of previous passwords that cannot be reused.	integer	Minimum value: 2 Maximum value: 20	2

config system password-policy

Configure password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.

```
config system password-policy
    Description: Configure password policy for locally defined administrator passwords and
    IPsec VPN pre-shared keys.
    set status [enable|disable]
    set apply-to {option1}, {option2}, ...
    set minimum-length {integer}
    set min-lower-case-letter {integer}
    set min-upper-case-letter {integer}
    set min-non-alphanumeric {integer}
    set min-number {integer}
    set min-change-characters {integer}
    set expire-status [enable|disable]
    set expire-day {integer}
```

```

set reuse-password [enable|disable]
set password-history {integer}
end

```

config system password-policy

Parameter	Description	Type	Size	Default						
status	Enable/disable setting a password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable password policy.</td></tr><tr><td><i>disable</i></td><td>Disable password policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable password policy.	<i>disable</i>	Disable password policy.			
	Option	Description								
	<i>enable</i>	Enable password policy.								
<i>disable</i>	Disable password policy.									
apply-to	Apply password policy to administrator passwords or IPsec pre-shared keys or both. Separate entries with a space.	option	-	admin-password						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>admin-password</i></td><td>Apply to administrator passwords.</td></tr><tr><td><i>ipsec-preshared-key</i></td><td>Apply to IPsec pre-shared keys.</td></tr></table>	Option	Description	<i>admin-password</i>	Apply to administrator passwords.	<i>ipsec-preshared-key</i>	Apply to IPsec pre-shared keys.			
	Option	Description								
	<i>admin-password</i>	Apply to administrator passwords.								
<i>ipsec-preshared-key</i>	Apply to IPsec pre-shared keys.									
minimum-length	Minimum password length.	integer	Minimum value: 8 Maximum value: 128	8						
min-lower-case-letter	Minimum number of lowercase characters in password.	integer	Minimum value: 0 Maximum value: 128	0						
min-upper-case-letter	Minimum number of uppercase characters in password.	integer	Minimum value: 0 Maximum value: 128	0						
min-non-alphanumeric	Minimum number of non-alphanumeric characters in password.	integer	Minimum value: 0 Maximum value: 128	0						

Parameter	Description	Type	Size	Default						
min-number	Minimum number of numeric characters in password.	integer	Minimum value: 0 Maximum value: 128	0						
min-change-characters	Minimum number of unique characters in new password which do not exist in old password.	integer	Minimum value: 0 Maximum value: 128	0						
expire-status	Enable/disable password expiration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Passwords expire after expire-day days.</td></tr><tr><td><i>disable</i></td><td>Passwords do not expire.</td></tr></table>				Option	Description	<i>enable</i>	Passwords expire after expire-day days.	<i>disable</i>	Passwords do not expire.
	Option	Description								
	<i>enable</i>	Passwords expire after expire-day days.								
<i>disable</i>	Passwords do not expire.									
expire-day	Number of days after which passwords expire.	integer	Minimum value: 1 Maximum value: 999	90						
reuse-password	Enable/disable reuse of password. If both reuse-password and min-change-characters are enabled, min-change-characters overrides.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Administrators are allowed to reuse the same password.</td></tr><tr><td><i>disable</i></td><td>Administrators must create a new password.</td></tr></table>				Option	Description	<i>enable</i>	Administrators are allowed to reuse the same password.	<i>disable</i>	Administrators must create a new password.
	Option	Description								
	<i>enable</i>	Administrators are allowed to reuse the same password.								
<i>disable</i>	Administrators must create a new password.									
password-history	Number of previous passwords that cannot be reused.	integer	Minimum value: 2 Maximum value: 20	2						

config system performance status

System performance status.

```
config system performance status
    Description: System performance status.
end
```

config system performance top

Display information about the top CPU processes.

```
config system performance top
    Description: Display information about the top CPU processes.
    set <delay> {string}
end
```

config system performance top

Parameter	Description	Type	Size	Default
<delay>	Delay in seconds.	string	Maximum length: -	

config system probe-response

Configure system probe response.

```
config system probe-response
    Description: Configure system probe response.
    set port {integer}
    set http-probe-value {string}
    set ttl-mode [reinit|decrease|...]
    set mode [none|http-probe|...]
    set security-mode [none|authentication]
    set password {password}
    set timeout {integer}
end
```

config system probe-response

Parameter	Description	Type	Size	Default
port	Port number to response.	integer	Minimum value: 1 Maximum value: 65535	8008
http-probe-value	Value to respond to the monitoring server.	string	Maximum length: 1024	OK
ttl-mode	Mode for TWAMP packet TTL modification.	option	-	retain

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>reinit</i>	Reinitialize TTL.		
	<i>decrease</i>	Decrease TTL.		
	<i>retain</i>	Retain TTL.		
mode	SLA response mode.	option	-	none
	Option	Description		
	<i>none</i>	Disable probe.		
	<i>http-probe</i>	HTTP probe.		
	<i>twamp</i>	Two way active measurement protocol.		
security-mode	TWAMP responder security mode.	option	-	none
	Option	Description		
	<i>none</i>	Unauthenticated mode.		
	<i>authentication</i>	Authenticated mode.		
password	TWAMP responder password in authentication mode.	password	Not Specified	
timeout	An inactivity timer for a twamp test session.	integer	Minimum value: 10 Maximum value: 3600	300

config system proxy-arp

Configure proxy-ARP.

```

config system proxy-arp
    Description: Configure proxy-ARP.
    edit <id>
        set interface {string}
        set ip {ipv4-address}
        set end-ip {ipv4-address}
    next
end

```

config system proxy-arp

Parameter	Description	Type	Size	Default
id	Unique integer ID of the entry.	integer	Minimum value: 0 Maximum value: 4294967295	0
interface	Interface acting proxy-ARP.	string	Maximum length: 15	
ip	IP address or start IP to be proxied.	ipv4-address	Not Specified	0.0.0.0
end-ip	End IP of IP range to be proxied.	ipv4-address	Not Specified	0.0.0.0

config system ptp

Configure system PTP information.

```

config system ptp
    Description: Configure system PTP information.
    set status [enable|disable]
    set mode [multicast|hybrid]
    set delay-mechanism [E2E|P2P]
    set request-interval {integer}
    set interface {string}
    set server-mode [enable|disable]
    config server-interface
        Description: FortiGate interface(s) with PTP server mode enabled. Devices on your
network can contact these interfaces for PTP services.
        edit <id>
            set server-interface-name {string}
            set delay-mechanism [E2E|P2P]
        next
    end
end

```

config system ptp

Parameter	Description	Type	Size	Default
status	Enable/disable setting the FortiProxy system time by synchronizing with an PTP Server.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable synchronization with PTP Server.		
	<i>disable</i>	Disable synchronization with PTP Server.		
mode	Multicast transmission or hybrid transmission.	option	-	multicast
	Option	Description		
	<i>multicast</i>	Send PTP packets with multicast.		
	<i>hybrid</i>	Send PTP packets with unicast and multicast.		
delay-mechanism	End to end delay detection or peer to peer delay detection.	option	-	E2E
	Option	Description		
	<i>E2E</i>	End to end delay detection.		
	<i>P2P</i>	Peer to peer delay detection.		
request-interval	The delay request value is the logarithmic mean interval in seconds between the delay request messages sent by the slave to the master.	integer	Minimum value: 1 Maximum value: 6	1
interface	PTP client will reply through this interface.	string	Maximum length: 15	
server-mode	Enable/disable FortiGate PTP server mode. Your FortiGate becomes an PTP server for other devices on your network.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FortiGate PTP server mode.		
	<i>disable</i>	Disable FortiGate PTP server mode.		

config server-interface

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default						
server-interface-name	Interface name.	string	Maximum length: 15							
delay-mechanism	End to end delay detection or peer to peer delay detection.	option	-	E2E						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>E2E</td><td>End to end delay detection.</td></tr><tr><td>P2P</td><td>Peer to peer delay detection.</td></tr></table>				Option	Description	E2E	End to end delay detection.	P2P	Peer to peer delay detection.
Option	Description									
E2E	End to end delay detection.									
P2P	Peer to peer delay detection.									

config system replacemsg-group

Configure replacement message groups.

```
config system replacemsg-group
  Description: Configure replacement message groups.
  edit <name>
    set comment {var-string}
    set group-type [default|utm|...]
    config mail
      Description: Replacement message table entries.
      edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
      next
    end
  config http
    Description: Replacement message table entries.
    edit <msg-type>
      set buffer {var-string}
      set header [none|http|...]
      set format [none|text|...]
    next
  end
  config webproxy
    Description: Replacement message table entries.
    edit <msg-type>
      set buffer {var-string}
      set header [none|http|...]
      set format [none|text|...]
    next
  end
  config ftp
    Description: Replacement message table entries.
    edit <msg-type>
      set buffer {var-string}
      set header [none|http|...]
```

```
        set format [none|text|...]
    next
end
config fortiguard-wf
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config spam
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config alertmail
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config admin
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config auth
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config sslvpn
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config nac-quar
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
```

```

        set format [none|text|...]
    next
end
config traffic-quota
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config utm
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config custom-message
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config icap
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config automation
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
next
end

```

config system replacemsg-group

Parameter	Description	Type	Size	Default
name	Group name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
group-type	Group type.	option	-	default
	Option	Description		
	default	Per-vdom replacement messages.		
	utm	For use with UTM settings in firewall policies.		
	auth	For use with authentication pages in firewall policies.		

config mail

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		

config http

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		

config webproxy

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option Description			
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option Description			
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config ftp

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config fortiguard-wf

Parameter	Description	Type	Size	Default								
msg-type	Message type.	string	Maximum length: 28									
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></table>				Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.
	Option	Description										
	<i>none</i>	No header type.										
	<i>http</i>	HTTP										
<i>8bit</i>	8 bit.											
format	Format flag.	option	-	none								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config spam

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config alertmail

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	

Parameter	Description	Type	Size	Default
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config admin

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config auth

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config sslvpn

Parameter	Description	Type	Size	Default								
msg-type	Message type.	string	Maximum length: 28									
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></table>				Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.
	Option	Description										
	<i>none</i>	No header type.										
	<i>http</i>	HTTP										
<i>8bit</i>	8 bit.											
format	Format flag.	option	-	none								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config nac-quar

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config traffic-quota

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	

Parameter	Description	Type	Size	Default
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config utm

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config custom-message

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config icap

Parameter	Description	Type	Size	Default								
msg-type	Message type.	string	Maximum length: 28									
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></table>				Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.
	Option	Description										
	<i>none</i>	No header type.										
	<i>http</i>	HTTP										
<i>8bit</i>	8 bit.											
format	Format flag.	option	-	none								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config automation

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config system replacemsg-image

Configure replacement message images.

```
config system replacemsg-image
  Description: Configure replacement message images.
  edit <name>
    set image-type [gif|jpg|...]
    set image-base64 {var-string}
  next
end
```

config system replacemsg-image

Parameter	Description	Type	Size	Default
name	Image name.	string	Maximum length: 23	
image-type	Image type.	option	-	png
	Option	Description		
	<i>gif</i>	GIF image.		
	<i>jpg</i>	JPEG image.		
	<i>tiff</i>	TIFF image.		
	<i>png</i>	PNG image.		
image-base64	Image data.	var-string	Maximum length: 32768	

config system replacemsg admin

Replacement messages.

```
config system replacemsg admin
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg admin

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config system replacemsg alertmail

Replacement messages.

```
config system replacemsg alertmail
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
```

config system replacemsg alertmail

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config system replacemsg auth

Replacement messages.

```
config system replacemsg auth
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
```

config system replacemsg auth

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config system replacemsg automation

Replacement messages.

```
config system replacemsg automation
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg automation

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config system replacemsg custom-message

Replacement messages.

```
config system replacemsg custom-message
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg custom-message

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config system replacemsg fortiguard-wf

Replacement messages.

```
config system replacemsg fortiguard-wf
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg fortiguard-wf

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		

config system replacemsg ftp

Replacement messages.

```
config system replacemsg ftp
  Description: Replacement messages.
  edit <msg-type>
```

```

        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end

```

config system replacemsg ftp

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config system replacemsg http

Replacement messages.

```

config system replacemsg http
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end

```

config system replacemsg http

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	OptionDescription			
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
format	Format flag.	option	-	none
	OptionDescription			
	none	No format type.		
	text	Text format.		
	html	HTML format.		

config system replacemsg icap

Replacement messages.

```
config system replacemsg icap
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg icap

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		

config system replacemsg mail

Replacement messages.

```
config system replacemsg mail
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
```

config system replacemsg mail

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config system replacemsg nac-quar

Replacement messages.

```
config system replacemsg nac-quar
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg nac-quar

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config system replacemsg spam

Replacement messages.

```
config system replacemsg spam
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg spam

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config system replacemsg sslvpn

Replacement messages.

```
config system replacemsg sslvpn
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
```

config system replacemsg sslvpn

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config system replacemsg traffic-quota

Replacement messages.

```
config system replacemsg traffic-quota
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg traffic-quota

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

config system replacemsg utm

Replacement messages.

```
config system replacemsg utm
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set header [none|http|...]
    set format [none|text|...]
  next
end
```

config system replacemsg utm

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	Option	Description		
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
format	Format flag.	option	-	none
	Option	Description		
	none	No format type.		
	text	Text format.		
	html	HTML format.		

config system replacemsg webproxy

Replacement messages.

```
config system replacemsg webproxy
  Description: Replacement messages.
  edit <msg-type>
```

```

        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end

```

config system replacemsg webproxy

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	OptionDescription			
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
format	Format flag.	option	-	none
	OptionDescription			
	none	No format type.		
	text	Text format.		
	html	HTML format.		

config system resource-limits

Configure resource limits.

```

config system resource-limits
    Description: Configure resource limits.
    set ipsec-phase1-interface {integer}
    set ipsec-phase2-interface {integer}
    set firewall-policy {integer}
    set firewall-address {integer}
    set firewall-addrgrp {integer}
    set custom-service {integer}
    set service-group {integer}
    set onetime-schedule {integer}
    set recurring-schedule {integer}

```

```

set user {integer}
set user-group {integer}
set proxy {integer}
set log-disk-quota {integer}
end

```

config system resource-limits

Parameter	Description	Type	Size	Default
ipsec-phase1-interface	Maximum number of VPN IPsec phase1 interface tunnels.	integer	Minimum value: 0 Maximum value: 4294967295	
ipsec-phase2-interface	Maximum number of VPN IPsec phase2 interface tunnels.	integer	Minimum value: 0 Maximum value: 4294967295	
firewall-policy	Maximum number of firewall policies (policy, DoS-policy4, DoS-policy6, multicast).	integer	Minimum value: 0 Maximum value: 4294967295	
firewall-address	Maximum number of firewall addresses (IPv4, IPv6, multicast).	integer	Minimum value: 0 Maximum value: 4294967295	
firewall-addgrp	Maximum number of firewall address groups (IPv4, IPv6).	integer	Minimum value: 0 Maximum value: 4294967295	
custom-service	Maximum number of firewall custom services.	integer	Minimum value: 0 Maximum value: 4294967295	
service-group	Maximum number of firewall service groups.	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default
onetime-schedule	Maximum number of firewall one-time schedules.	integer	Minimum value: 0 Maximum value: 4294967295	
recurring-schedule	Maximum number of firewall recurring schedules.	integer	Minimum value: 0 Maximum value: 4294967295	
user	Maximum number of local users.	integer	Minimum value: 0 Maximum value: 4294967295	
user-group	Maximum number of user groups.	integer	Minimum value: 0 Maximum value: 4294967295	
proxy	Maximum number of concurrent proxy users.	integer	Minimum value: 0 Maximum value: 4294967295	
log-disk-quota	Log disk quota in megabytes (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0

config system saml

Global settings for SAML authentication.

```
config system saml
    Description: Global settings for SAML authentication.
    set status [enable|disable]
    set role [identity-provider|service-provider]
    set default-login-page [normal|sso]
    set default-profile {string}
    set cert {string}
    set binding-protocol [post|redirect]
    set portal-url {string}
```

```

set entity-id {string}
set single-sign-on-url {string}
set single-logout-url {string}
set idp-entity-id {string}
set idp-single-sign-on-url {string}
set idp-single-logout-url {string}
set idp-cert {string}
set server-address {string}
set tolerance {integer}
set life {integer}
config service-providers
    Description: Authorized service providers.
    edit <name>
        set prefix {string}
        set sp-binding-protocol [post|redirect]
        set sp-cert {string}
        set sp-entity-id {string}
        set sp-single-sign-on-url {string}
        set sp-single-logout-url {string}
        set sp-portal-url {string}
        set idp-entity-id {string}
        set idp-single-sign-on-url {string}
        set idp-single-logout-url {string}
        config assertion-attributes
            Description: Customized SAML attributes to send along with assertion.
            edit <name>
                set type [username|email|...]
            next
        end
    next
end
end

```

config system saml

Parameter	Description	Type	Size	Default
status	Enable/disable SAML authentication.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable SAML authentication.		
	<i>disable</i>	Disable SAML authentication.		
role	SAML role.	option	-	service-provider
	Option	Description		
	<i>identity-provider</i>	Identity Provider.		
	<i>service-provider</i>	Service Provider.		

Parameter	Description	Type	Size	Default						
default-login-page	Choose default login page.	option	-	normal						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>normal</i></td><td>Use local login page as default.</td></tr><tr><td><i>sso</i></td><td>Use IdP's Single Sign-On page as default.</td></tr></table>	Option	Description	<i>normal</i>	Use local login page as default.	<i>sso</i>	Use IdP's Single Sign-On page as default.			
Option	Description									
<i>normal</i>	Use local login page as default.									
<i>sso</i>	Use IdP's Single Sign-On page as default.									
default-profile	Default profile for new SSO admin.	string	Maximum length: 35							
cert	Certificate to sign SAML messages.	string	Maximum length: 35							
binding-protocol	IdP Binding protocol.	option	-	redirect						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>post</i></td><td>HTTP POST binding.</td></tr><tr><td><i>redirect</i></td><td>HTTP Redirect binding.</td></tr></table>	Option	Description	<i>post</i>	HTTP POST binding.	<i>redirect</i>	HTTP Redirect binding.			
Option	Description									
<i>post</i>	HTTP POST binding.									
<i>redirect</i>	HTTP Redirect binding.									
portal-url	SP portal URL.	string	Maximum length: 255							
entity-id	SP entity ID.	string	Maximum length: 255							
single-sign-on-url	SP single sign-on URL.	string	Maximum length: 255							
single-logout-url	SP single logout URL.	string	Maximum length: 255							
idp-entity-id	IDP entity ID.	string	Maximum length: 255							
idp-single-sign-on-url	IDP single sign-on URL.	string	Maximum length: 255							
idp-single-logout-url	IDP single logout URL.	string	Maximum length: 255							
idp-cert	IDP certificate name.	string	Maximum length: 35							
server-address	Server address.	string	Maximum length: 63							

Parameter	Description	Type	Size	Default
tolerance	Tolerance to the range of time when the assertion is valid (in minutes).	integer	Minimum value: 0 Maximum value: 4294967295	5
life	Length of the range of time when the assertion is valid (in minutes).	integer	Minimum value: 0 Maximum value: 4294967295	30

config service-providers

Parameter	Description	Type	Size	Default						
name	Name.	string	Maximum length: 35							
prefix	Prefix.	string	Maximum length: 35							
sp-binding-protocol	SP binding protocol.	option	-	post						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>post</i></td><td>HTTP POST binding.</td></tr><tr><td><i>redirect</i></td><td>HTTP Redirect binding.</td></tr></table>	Option	Description	<i>post</i>	HTTP POST binding.	<i>redirect</i>	HTTP Redirect binding.			
Option	Description									
<i>post</i>	HTTP POST binding.									
<i>redirect</i>	HTTP Redirect binding.									
sp-cert	SP certificate name.	string	Maximum length: 35							
sp-entity-id	SP entity ID.	string	Maximum length: 255							
sp-single-sign-on-url	SP single sign-on URL.	string	Maximum length: 255							
sp-single-logout-url	SP single logout URL.	string	Maximum length: 255							
sp-portal-url	SP portal URL.	string	Maximum length: 255							
idp-entity-id	IDP entity ID.	string	Maximum length: 255							
idp-single-sign-on-url	IDP single sign-on URL.	string	Maximum length: 255							
idp-single-logout-url	IDP single logout URL.	string	Maximum length: 255							

config assertion-attributes

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
type	Type.	option	-	username
	Option	Description		
	username	User Name.		
	email	Email Address.		
	profile-name	Profile Name.		

config system sdn-connector

Configure connection to SDN Connector.

```

config system sdn-connector
  Description: Configure connection to SDN Connector.
  edit <name>
    set status [disable|enable]
    set type [aci|alicloud|...]
    set use-metadata-iam [disable|enable]
    set ha-status [disable|enable]
    set verify-certificate [disable|enable]
    set server {string}
    set server-list <ip1>, <ip2>, ...
    set server-port {integer}
    set username {string}
    set password {password_aes256}
    set vcenter-server {string}
    set vcenter-username {string}
    set vcenter-password {password_aes256}
    set access-key {string}
    set secret-key {password}
    set region {string}
    set vpc-id {string}
    set alt-resource-ip [disable|enable]
    config external-account-list
      Description: Configure AWS external account list.
      edit <role-arn>
        set external-id {string}
        set region-list <region1>, <region2>, ...
      next
    end
    set tenant-id {string}
    set client-id {string}
    set client-secret {password}
    set subscription-id {string}
  
```

```
set resource-group {string}
set login-endpoint {string}
set resource-url {string}
set azure-region [global|china|...]
config nic
    Description: Configure Azure network interface.
    edit <name>
        config ip
            Description: Configure IP configuration.
            edit <name>
                set public-ip {string}
                set resource-group {string}
            next
        end
    next
end
config route-table
    Description: Configure Azure route table.
    edit <name>
        set subscription-id {string}
        set resource-group {string}
        config route
            Description: Configure Azure route.
            edit <name>
                set next-hop {string}
            next
        end
    next
end
set user-id {string}
set compartment-id {string}
set oci-region {string}
set oci-region-type [commercial|government]
set oci-cert {string}
set oci-fingerprint {string}
config external-ip
    Description: Configure GCP external IP.
    edit <name>
    next
end
config route
    Description: Configure GCP route.
    edit <name>
    next
end
config gcp-project-list
    Description: Configure GCP project list.
    edit <id>
        set gcp-zone-list <name1>, <name2>, ...
    next
end
config forwarding-rule
    Description: Configure GCP forwarding rule.
    edit <rule-name>
        set target {string}
    next
```

```

end
set service-account {string}
set private-key {user}
set secret-token {user}
set domain {string}
set group-name {string}
set server-cert {string}
set server-ca-cert {string}
set api-key {password}
set compute-generation {integer}
set ibm-region [dallas|washington-dc|...]
set update-interval {integer}
next
end

```

config system sdn-connector

Parameter	Description	Type	Size	Default
name	SDN connector name.	string	Maximum length: 35	
status	Enable/disable connection to the remote SDN connector.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable connection to this SDN Connector.		
	<i>enable</i>	Enable connection to this SDN Connector.		
type	Type of SDN connector.	option	-	aws
	Option	Description		
	<i>aci</i>	Application Centric Infrastructure (ACI).		
	<i>alicloud</i>	AliCloud Service (ACS).		
	<i>aws</i>	Amazon Web Services (AWS).		
	<i>azure</i>	Microsoft Azure.		
	<i>gcp</i>	Google Cloud Platform (GCP).		
	<i>nsx</i>	VMware NSX.		
	<i>nuage</i>	Nuage VSP.		
	<i>oci</i>	Oracle Cloud Infrastructure.		
	<i>openstack</i>	OpenStack.		
	<i>kubernetes</i>	Kubernetes.		
	<i>vmware</i>	VMware vSphere (vCenter & ESXi).		

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sepm</i></td><td>Symantec Endpoint Protection Manager.</td></tr><tr><td><i>aci-direct</i></td><td>Application Centric Infrastructure (ACI Direct Connection).</td></tr><tr><td><i>ibm</i></td><td>IBM Cloud Infrastructure.</td></tr><tr><td><i>nutanix</i></td><td>Nutanix Prism Central.</td></tr><tr><td><i>sap</i></td><td>SAP Control.</td></tr></table>	Option	Description	<i>sepm</i>	Symantec Endpoint Protection Manager.	<i>aci-direct</i>	Application Centric Infrastructure (ACI Direct Connection).	<i>ibm</i>	IBM Cloud Infrastructure.	<i>nutanix</i>	Nutanix Prism Central.	<i>sap</i>	SAP Control.			
	Option	Description														
	<i>sepm</i>	Symantec Endpoint Protection Manager.														
	<i>aci-direct</i>	Application Centric Infrastructure (ACI Direct Connection).														
	<i>ibm</i>	IBM Cloud Infrastructure.														
	<i>nutanix</i>	Nutanix Prism Central.														
<i>sap</i>	SAP Control.															
use-metadata-iam	Enable/disable use of IAM role from metadata to call API.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable using IAM role to call API.</td></tr><tr><td><i>enable</i></td><td>Enable using IAM role to call API.</td></tr></table>	Option	Description	<i>disable</i>	Disable using IAM role to call API.	<i>enable</i>	Enable using IAM role to call API.									
	Option	Description														
	<i>disable</i>	Disable using IAM role to call API.														
<i>enable</i>	Enable using IAM role to call API.															
ha-status	Enable/disable use for FortiProxy HA service.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use for FortiProxy HA service.</td></tr><tr><td><i>enable</i></td><td>Enable use for FortiProxy HA service.</td></tr></table>	Option	Description	<i>disable</i>	Disable use for FortiProxy HA service.	<i>enable</i>	Enable use for FortiProxy HA service.									
	Option	Description														
	<i>disable</i>	Disable use for FortiProxy HA service.														
<i>enable</i>	Enable use for FortiProxy HA service.															
verify-certificate	Enable/disable server certificate verification.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable server certificate verification.</td></tr><tr><td><i>enable</i></td><td>Enable server certificate verification.</td></tr></table>	Option	Description	<i>disable</i>	Disable server certificate verification.	<i>enable</i>	Enable server certificate verification.									
	Option	Description														
	<i>disable</i>	Disable server certificate verification.														
<i>enable</i>	Enable server certificate verification.															
server	Server address of the remote SDN connector.	string	Maximum length: 127													
server-list <ip>	Server address list of the remote SDN connector. IPv4 address.	string	Maximum length: 15													
server-port	Port number of the remote SDN connector.	integer	Minimum value: 0 Maximum value: 65535	0												
username	Username of the remote SDN connector as login credentials.	string	Maximum length: 64													
password	Password of the remote SDN connector as login credentials.	password_aes256	Not Specified													

Parameter	Description	Type	Size	Default						
vcenter-server	vCenter server address for NSX quarantine.	string	Maximum length: 127							
vcenter-username	vCenter server username for NSX quarantine.	string	Maximum length: 64							
vcenter-password	vCenter server password for NSX quarantine.	password_aes256	Not Specified							
access-key	AWS / ACS access key ID.	string	Maximum length: 31							
secret-key	AWS / ACS secret access key.	password	Not Specified							
region	AWS / ACS region name.	string	Maximum length: 31							
vpc-id	AWS VPC ID.	string	Maximum length: 31							
alt-resource-ip	Enable/disable AWS alternative resource IP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable AWS alternative resource IP.</td></tr><tr><td>enable</td><td>Enable AWS alternative resource IP.</td></tr></table>				Option	Description	disable	Disable AWS alternative resource IP.	enable	Enable AWS alternative resource IP.
Option	Description									
disable	Disable AWS alternative resource IP.									
enable	Enable AWS alternative resource IP.									
tenant-id	Tenant ID (directory ID).	string	Maximum length: 127							
client-id	Azure client ID (application ID).	string	Maximum length: 63							
client-secret	Azure client secret (application key).	password	Not Specified							
subscription-id	Azure subscription ID.	string	Maximum length: 63							
resource-group	Azure resource group.	string	Maximum length: 63							
login-endpoint	Azure Stack login endpoint.	string	Maximum length: 127							
resource-url	Azure Stack resource URL.	string	Maximum length: 127							
azure-region	Azure server region.	option	-	global						

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Global Azure Server.</td></tr><tr><td><i>china</i></td><td>China Azure Server.</td></tr><tr><td><i>germany</i></td><td>Germany Azure Server.</td></tr><tr><td><i>usgov</i></td><td>US Government Azure Server.</td></tr><tr><td><i>local</i></td><td>Azure Stack Local Server.</td></tr></table>	Option	Description	<i>global</i>	Global Azure Server.	<i>china</i>	China Azure Server.	<i>germany</i>	Germany Azure Server.	<i>usgov</i>	US Government Azure Server.	<i>local</i>	Azure Stack Local Server.			
	Option	Description														
	<i>global</i>	Global Azure Server.														
	<i>china</i>	China Azure Server.														
	<i>germany</i>	Germany Azure Server.														
	<i>usgov</i>	US Government Azure Server.														
	<i>local</i>	Azure Stack Local Server.														
user-id	User ID.	string	Maximum length: 127													
compartment-id	Compartment ID.	string	Maximum length: 127													
oci-region	OCI server region.	string	Maximum length: 31													
oci-region-type	OCI region type.	option	-	commercial												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>commercial</i></td><td>Commercial region.</td></tr><tr><td><i>government</i></td><td>Government region.</td></tr></table>	Option	Description	<i>commercial</i>	Commercial region.	<i>government</i>	Government region.									
	Option	Description														
	<i>commercial</i>	Commercial region.														
<i>government</i>	Government region.															
oci-cert	OCI certificate.	string	Maximum length: 63													
oci-fingerprint	OCI pubkey fingerprint.	string	Maximum length: 63													
service-account	GCP service account email.	string	Maximum length: 127													
private-key	Private key of GCP service account.	user	Not Specified													
secret-token	Secret token of Kubernetes service account.	user	Not Specified													
domain	Domain name.	string	Maximum length: 127													
group-name	Full path group name of computers.	string	Maximum length: 127													
server-cert	Trust servers that contain this certificate only.	string	Maximum length: 127													
server-ca-cert	Trust only those servers whose certificate is directly/indirectly signed by this certificate.	string	Maximum length: 127													

Parameter	Description	Type	Size	Default																				
api-key	IBM cloud API key or service ID API key.	password	Not Specified																					
compute-generation	Compute generation for IBM cloud infrastructure.	integer	Minimum value: 1 Maximum value: 2	2																				
ibm-region	IBM cloud region name.	option	-	dallas																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>dallas</td><td>US South (Dallas) Public Endpoint.</td></tr><tr><td>washington-dc</td><td>US East (Washington DC) Public Endpoint.</td></tr><tr><td>london</td><td>United Kingdom (London) Public Endpoint.</td></tr><tr><td>frankfurt</td><td>Germany (Frankfurt) Public Endpoint.</td></tr><tr><td>sydney</td><td>Australia (Sydney) Public Endpoint.</td></tr><tr><td>tokyo</td><td>Japan (Tokyo) Public Endpoint.</td></tr><tr><td>osaka</td><td>Japan (Osaka) Public Endpoint.</td></tr><tr><td>toronto</td><td>Canada (Toronto) Public Endpoint.</td></tr><tr><td>sao-paulo</td><td>Brazil (Sao Paulo) Public Endpoint.</td></tr></table>				Option	Description	dallas	US South (Dallas) Public Endpoint.	washington-dc	US East (Washington DC) Public Endpoint.	london	United Kingdom (London) Public Endpoint.	frankfurt	Germany (Frankfurt) Public Endpoint.	sydney	Australia (Sydney) Public Endpoint.	tokyo	Japan (Tokyo) Public Endpoint.	osaka	Japan (Osaka) Public Endpoint.	toronto	Canada (Toronto) Public Endpoint.	sao-paulo	Brazil (Sao Paulo) Public Endpoint.
	Option	Description																						
	dallas	US South (Dallas) Public Endpoint.																						
	washington-dc	US East (Washington DC) Public Endpoint.																						
	london	United Kingdom (London) Public Endpoint.																						
	frankfurt	Germany (Frankfurt) Public Endpoint.																						
	sydney	Australia (Sydney) Public Endpoint.																						
	tokyo	Japan (Tokyo) Public Endpoint.																						
	osaka	Japan (Osaka) Public Endpoint.																						
	toronto	Canada (Toronto) Public Endpoint.																						
sao-paulo	Brazil (Sao Paulo) Public Endpoint.																							
update-interval	Dynamic object update interval.	integer	Minimum value: 0 Maximum value: 3600	60																				

config external-account-list

Parameter	Description	Type	Size	Default
role-arn	AWS role ARN to assume.	string	Maximum length: 2047	
external-id	AWS external ID.	string	Maximum length: 1399	
region-list <region>	AWS region name list. AWS region name.	string	Maximum length: 31	

config nic

Parameter	Description	Type	Size	Default
name	Network interface name.	string	Maximum length: 63	

config ip

Parameter	Description	Type	Size	Default
name	IP configuration name.	string	Maximum length: 63	
public-ip	Public IP name.	string	Maximum length: 63	
resource-group	Resource group of Azure public IP.	string	Maximum length: 63	

config route-table

Parameter	Description	Type	Size	Default
name	Route table name.	string	Maximum length: 63	
subscription-id	Subscription ID of Azure route table.	string	Maximum length: 63	
resource-group	Resource group of Azure route table.	string	Maximum length: 63	

config route

Parameter	Description	Type	Size	Default
name	Route name.	string	Maximum length: 63	
next-hop	Next hop address.	string	Maximum length: 127	

config route

Parameter	Description	Type	Size	Default
name	Route name.	string	Maximum length: 63	

config external-ip

Parameter	Description	Type	Size	Default
name	External IP name.	string	Maximum length: 63	

config route

Parameter	Description	Type	Size	Default
name	Route name.	string	Maximum length: 63	
next-hop	Next hop address.	string	Maximum length: 127	

config route

Parameter	Description	Type	Size	Default
name	Route name.	string	Maximum length: 63	

config gcp-project-list

Parameter	Description	Type	Size	Default
id	GCP project ID.	string	Maximum length: 127	
gcp-zone-list <name>	Configure GCP zone list. GCP zone name.	string	Maximum length: 127	

config forwarding-rule

Parameter	Description	Type	Size	Default
rule-name	Forwarding rule name.	string	Maximum length: 63	
target	Target instance name.	string	Maximum length: 63	

config system session-ttl

Configure global session TTL timers for this FortiProxy.

```
config system session-ttl
  Description: Configure global session TTL timers for this FortiProxy.
  set default {user}
  config port
    Description: Session TTL port.
    edit <id>
      set protocol {integer}
      set start-port {integer}
      set end-port {integer}
      set timeout {user}
    next
  end
end
```

config system session-ttl

Parameter	Description	Type	Size	Default
default	Default timeout.	user	Not Specified	

config port

Parameter	Description	Type	Size	Default
id	Table entry ID.	integer	Minimum value: 0 Maximum value: 65535	0
protocol	Protocol.	integer	Minimum value: 0 Maximum value: 255	0
start-port	Start port number.	integer	Minimum value: 0 Maximum value: 65535	0

Parameter	Description	Type	Size	Default
end-port	End port number.	integer	Minimum value: 0 Maximum value: 65535	0
timeout	Session timeout (TTL).	user	Not Specified	

config system session

System IPv4 session.

```
config system session
    Description: System IPv4 session.
end
```

config system session6

System IPv6 session.

```
config system session6
    Description: System IPv6 session.
end
```

config system settings

Configure VDOM settings.

```
config system settings
    Description: Configure VDOM settings.
    set comments {var-string}
    set opmode [nat|transparent]
    set forward-domain [enable|disable]
    set http-external-dest [fortiweb|forticache]
    set firewall-session-dirty [check-all|check-new|...]
    set manageip {user}
    set gateway {ipv4-address}
    set ip {ipv4-classnet-host}
    set manageip6 {ipv6-prefix}
    set gateway6 {ipv6-address}
    set ip6 {ipv6-prefix}
    set device {string}
    set utf8-spam-tagging [enable|disable]
```

```
set wccp-cache-engine [enable|disable]
set wccp-local-route [enable|disable]
set vpn-stats-log {option1}, {option2}, ...
set vpn-stats-period {integer}
set mac-ttl {integer}
set fw-session-hairpin [enable|disable]
set prp-trailer-action [enable|disable]
set snat-hairpin-traffic [enable|disable]
set dhcp-proxy [enable|disable]
set dhcp-proxy-interface-select-method [auto|specify]
set dhcp-proxy-interface {string}
set dhcp-server-ip {user}
set dhcp6-server-ip {user}
set gui-default-policy-columns <name1>, <name2>, ...
set link-down-access [enable|disable]
set asymroute [enable|disable]
set asymroute-icmp [enable|disable]
set tcp-session-without-syn [enable|disable]
set ses-denied-traffic [enable|disable]
set strict-src-check [enable|disable]
set allow-linkdown-path [enable|disable]
set asymroute6 [enable|disable]
set asymroute6-icmp [enable|disable]
set sctp-session-without-init [enable|disable]
set status [enable|disable]
set allow-subnet-overlap [enable|disable]
set deny-tcp-with-icmp [enable|disable]
set discovered-device-timeout {integer}
set email-portal-check-dns [disable|enable]
set gui-icap [enable|disable]
set gui-implicit-policy [enable|disable]
set gui-dns-database [enable|disable]
set gui-proxy-inspection [enable|disable]
set gui-multicast-policy [enable|disable]
set gui-dos-policy [enable|disable]
set gui-object-colors [enable|disable]
set gui-voip-profile [enable|disable]
set gui-security-profile-group [enable|disable]
set gui-wanopt-cache [enable|disable]
set gui-explicit-proxy [enable|disable]
set gui-policy-based-ipsec [enable|disable]
set gui-threat-weight [enable|disable]
set gui-spamfilter [enable|disable]
set gui-file-filter [enable|disable]
set gui-application-control [enable|disable]
set gui-ips [enable|disable]
set gui-dhcp-advanced [enable|disable]
set gui-vpn [enable|disable]
set gui-webfilter-advanced [enable|disable]
set gui-traffic-shaping [enable|disable]
set gui-antivirus [enable|disable]
set gui-webfilter [enable|disable]
set gui-videofilter [enable|disable]
set gui-dnsfilter [enable|disable]
set gui-advanced-policy [enable|disable]
set gui-allow-unnamed-policy [enable|disable]
```

```

set gui-email-collection [enable|disable]
set gui-multiple-interface-policy [enable|disable]
set gui-policy-disclaimer [enable|disable]
set gui-ztna [enable|disable]
set gui-ot [enable|disable]
set block-land-attack [disable|enable]
set default-app-port-as-service [enable|disable]
set application-bandwidth-tracking [disable|enable]
set default-policy-expiry-days {integer}
set gui-enforce-change-summary [disable|require|...]
set internet-service-database-cache [disable|enable]

```

```
end
```

config system settings

Parameter	Description	Type	Size	Default						
comments	VDOM comments.	var-string	Maximum length: 255							
opmode	Firewall operation mode (NAT or Transparent).	option	-	nat						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>nat</i></td><td>Change to NAT mode.</td></tr><tr><td><i>transparent</i></td><td>Change to transparent mode.</td></tr></table>	Option	Description	<i>nat</i>	Change to NAT mode.	<i>transparent</i>	Change to transparent mode.			
Option	Description									
<i>nat</i>	Change to NAT mode.									
<i>transparent</i>	Change to transparent mode.									
forward-domain	Enable/disable forward domain.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward domain.</td></tr><tr><td><i>disable</i></td><td>Disable forward domain.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward domain.	<i>disable</i>	Disable forward domain.			
Option	Description									
<i>enable</i>	Enable forward domain.									
<i>disable</i>	Disable forward domain.									
http-external-dest	Offload HTTP traffic to FortiWeb or FortiCache.	option	-	fortiweb						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortiweb</i></td><td>Offload HTTP traffic to FortiWeb for Web Application Firewall inspection.</td></tr><tr><td><i>forticache</i></td><td>Offload HTTP traffic to FortiCache for external web caching and WAN optimization.</td></tr></table>	Option	Description	<i>fortiweb</i>	Offload HTTP traffic to FortiWeb for Web Application Firewall inspection.	<i>forticache</i>	Offload HTTP traffic to FortiCache for external web caching and WAN optimization.			
Option	Description									
<i>fortiweb</i>	Offload HTTP traffic to FortiWeb for Web Application Firewall inspection.									
<i>forticache</i>	Offload HTTP traffic to FortiCache for external web caching and WAN optimization.									
firewall-session-dirty	Select how to manage sessions affected by firewall policy configuration changes.	option	-	check-all						

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>check-all</i></td><td>All sessions affected by a firewall policy change are flushed from the session table. When new packets are received they are re-evaluated by stateful inspection and re-added to the session table.</td></tr><tr><td><i>check-new</i></td><td>Established sessions for changed firewall policies continue without being affected by the policy configuration change. New sessions are evaluated according to the new firewall policy configuration.</td></tr><tr><td><i>check-policy-option</i></td><td>Sessions are managed individually depending on the firewall policy. Some sessions may restart. Some may continue.</td></tr></table>				Option	Description	<i>check-all</i>	All sessions affected by a firewall policy change are flushed from the session table. When new packets are received they are re-evaluated by stateful inspection and re-added to the session table.	<i>check-new</i>	Established sessions for changed firewall policies continue without being affected by the policy configuration change. New sessions are evaluated according to the new firewall policy configuration.	<i>check-policy-option</i>	Sessions are managed individually depending on the firewall policy. Some sessions may restart. Some may continue.
	Option	Description										
	<i>check-all</i>	All sessions affected by a firewall policy change are flushed from the session table. When new packets are received they are re-evaluated by stateful inspection and re-added to the session table.										
	<i>check-new</i>	Established sessions for changed firewall policies continue without being affected by the policy configuration change. New sessions are evaluated according to the new firewall policy configuration.										
<i>check-policy-option</i>	Sessions are managed individually depending on the firewall policy. Some sessions may restart. Some may continue.											
manageip	Transparent mode IPv4 management IP address and netmask.	user	Not Specified									
gateway	Transparent mode IPv4 default gateway IP address.	ipv4-address	Not Specified	0.0.0.0								
ip	IP address and netmask.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0								
manageip6	Transparent mode IPv6 management IP address and netmask.	ipv6-prefix	Not Specified	::/0								
gateway6	Transparent mode IPv4 default gateway IP address.	ipv6-address	Not Specified	::								
ip6	IPv6 address prefix for NAT mode.	ipv6-prefix	Not Specified	::/0								
device	Interface to use for management access for NAT mode.	string	Maximum length: 35									
utf8-spam-tagging	Enable/disable converting antispam tags to UTF-8 for better non-ASCII character support.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Convert antispam tags to UTF-8.</td></tr><tr><td><i>disable</i></td><td>Do not convert antispam tags.</td></tr></table>				Option	Description	<i>enable</i>	Convert antispam tags to UTF-8.	<i>disable</i>	Do not convert antispam tags.		
	Option	Description										
	<i>enable</i>	Convert antispam tags to UTF-8.										
<i>disable</i>	Do not convert antispam tags.											
wccp-cache-engine	Enable/disable WCCP cache engine.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WCCP cache engine.</td></tr><tr><td><i>disable</i></td><td>Disable WCCP cache engine.</td></tr></table>				Option	Description	<i>enable</i>	Enable WCCP cache engine.	<i>disable</i>	Disable WCCP cache engine.		
	Option	Description										
	<i>enable</i>	Enable WCCP cache engine.										
<i>disable</i>	Disable WCCP cache engine.											

Parameter	Description	Type	Size	Default
wccp-local-route	Enable/disable WCCP to use local route.	option	-	disable
	Option Description			
	enable Enable WCCP to use local route.			
	disable Disable WCCP to use local route.			
vpn-stats-log	Enable/disable periodic VPN log statistics for one or more types of VPN. Separate names with a space.	option	-	ipsec pptp l2tp
	Option Description			
	ipsec IPsec.			
	pptp PPTP.			
	l2tp L2TP.			
vpn-stats-period	Period to send VPN log statistics.	integer	Minimum value: 0 Maximum value: 4294967295	600
mac-ttl	Duration of MAC addresses in Transparent mode.	integer	Minimum value: 300 Maximum value: 8640000	300
fw-session-hairpin	Enable/disable checking for a matching policy each time hairpin traffic goes through the FortiProxy.	option	-	disable
	Option Description			
	enable Perform a policy check every time.			
	disable Perform a policy check only the first time the session is received.			
prp-trailer-action	Enable/disable action to take on PRP trailer.	option	-	disable
	Option Description			
	enable Try to keep PRP trailer.			
	disable Trim PRP trailer.			
snat-hairpin-traffic	Enable/disable source NAT (SNAT) for hairpin traffic.	option	-	enable

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable SNAT for hairpin traffic.		
	<i>disable</i>	Disable SNAT for hairpin traffic.		
dhcp-proxy	Enable/disable the DHCP Proxy.	option	-	disable
	Option Description			
	<i>enable</i>	Enable the DHCP proxy.		
	<i>disable</i>	Disable the DHCP proxy.		
dhcp-proxy-interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option Description			
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
dhcp-proxy-interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
dhcp-server-ip	DHCP Server IPv4 address.	user	Not Specified	
dhcp6-server-ip	DHCPv6 server IPv6 address.	user	Not Specified	
gui-default-policy-columns <name>	Default columns to display for policy lists on GUI. Select column name.	string	Maximum length: 79	
link-down-access	Enable/disable link down access traffic.	option	-	enable
	Option Description			
	<i>enable</i>	Allow link down access traffic.		
	<i>disable</i>	Block link down access traffic.		
asymroute	Enable/disable IPv4 asymmetric routing.	option	-	disable
	Option Description			
	<i>enable</i>	Enable IPv4 asymmetric routing.		
	<i>disable</i>	Disable IPv4 asymmetric routing.		

Parameter	Description	Type	Size	Default						
asymroute-icmp	Enable/disable ICMP asymmetric routing.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ICMP asymmetric routing.</td></tr><tr><td><i>disable</i></td><td>Disable ICMP asymmetric routing.</td></tr></table>	Option	Description	<i>enable</i>	Enable ICMP asymmetric routing.	<i>disable</i>	Disable ICMP asymmetric routing.			
Option	Description									
<i>enable</i>	Enable ICMP asymmetric routing.									
<i>disable</i>	Disable ICMP asymmetric routing.									
tcp-session-without-syn	Enable/disable allowing TCP session without SYN flags.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow TCP session without SYN flags.</td></tr><tr><td><i>disable</i></td><td>Do not allow TCP session without SYN flags.</td></tr></table>	Option	Description	<i>enable</i>	Allow TCP session without SYN flags.	<i>disable</i>	Do not allow TCP session without SYN flags.			
Option	Description									
<i>enable</i>	Allow TCP session without SYN flags.									
<i>disable</i>	Do not allow TCP session without SYN flags.									
ses-denied-traffic	Enable/disable including denied session in the session table.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Include denied sessions in the session table.</td></tr><tr><td><i>disable</i></td><td>Do not add denied sessions to the session table.</td></tr></table>	Option	Description	<i>enable</i>	Include denied sessions in the session table.	<i>disable</i>	Do not add denied sessions to the session table.			
Option	Description									
<i>enable</i>	Include denied sessions in the session table.									
<i>disable</i>	Do not add denied sessions to the session table.									
strict-src-check	Enable/disable strict source verification.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable strict source verification.</td></tr><tr><td><i>disable</i></td><td>Disable strict source verification.</td></tr></table>	Option	Description	<i>enable</i>	Enable strict source verification.	<i>disable</i>	Disable strict source verification.			
Option	Description									
<i>enable</i>	Enable strict source verification.									
<i>disable</i>	Disable strict source verification.									
allow-linkdown-path	Enable/disable link down path.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow link down path.</td></tr><tr><td><i>disable</i></td><td>Do not allow link down path.</td></tr></table>	Option	Description	<i>enable</i>	Allow link down path.	<i>disable</i>	Do not allow link down path.			
Option	Description									
<i>enable</i>	Allow link down path.									
<i>disable</i>	Do not allow link down path.									
asymroute6	Enable/disable asymmetric IPv6 routing.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable asymmetric IPv6 routing.</td></tr><tr><td><i>disable</i></td><td>Disable asymmetric IPv6 routing.</td></tr></table>	Option	Description	<i>enable</i>	Enable asymmetric IPv6 routing.	<i>disable</i>	Disable asymmetric IPv6 routing.			
Option	Description									
<i>enable</i>	Enable asymmetric IPv6 routing.									
<i>disable</i>	Disable asymmetric IPv6 routing.									

Parameter	Description	Type	Size	Default						
asymroute6-icmp	Enable/disable asymmetric ICMPv6 routing.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable asymmetric ICMPv6 routing.</td></tr><tr><td><i>disable</i></td><td>Disable asymmetric ICMPv6 routing.</td></tr></table>	Option	Description	<i>enable</i>	Enable asymmetric ICMPv6 routing.	<i>disable</i>	Disable asymmetric ICMPv6 routing.			
Option	Description									
<i>enable</i>	Enable asymmetric ICMPv6 routing.									
<i>disable</i>	Disable asymmetric ICMPv6 routing.									
sctp-session-without-init	Enable/disable SCTP session creation without SCTP INIT.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SCTP session creation without SCTP INIT.</td></tr><tr><td><i>disable</i></td><td>Disable SCTP session creation without SCTP INIT.</td></tr></table>	Option	Description	<i>enable</i>	Enable SCTP session creation without SCTP INIT.	<i>disable</i>	Disable SCTP session creation without SCTP INIT.			
Option	Description									
<i>enable</i>	Enable SCTP session creation without SCTP INIT.									
<i>disable</i>	Disable SCTP session creation without SCTP INIT.									
status	Enable/disable this VDOM.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this VDOM.</td></tr><tr><td><i>disable</i></td><td>Disable this VDOM.</td></tr></table>	Option	Description	<i>enable</i>	Enable this VDOM.	<i>disable</i>	Disable this VDOM.			
Option	Description									
<i>enable</i>	Enable this VDOM.									
<i>disable</i>	Disable this VDOM.									
allow-subnet-overlap	Enable/disable allowing interface subnets to use overlapping IP addresses.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable overlapping subnets.</td></tr><tr><td><i>disable</i></td><td>Disable overlapping subnets.</td></tr></table>	Option	Description	<i>enable</i>	Enable overlapping subnets.	<i>disable</i>	Disable overlapping subnets.			
Option	Description									
<i>enable</i>	Enable overlapping subnets.									
<i>disable</i>	Disable overlapping subnets.									
deny-tcp-with-icmp	Enable/disable denying TCP by sending an ICMP communication prohibited packet.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Deny TCP with ICMP.</td></tr><tr><td><i>disable</i></td><td>Disable denying TCP with ICMP.</td></tr></table>	Option	Description	<i>enable</i>	Deny TCP with ICMP.	<i>disable</i>	Disable denying TCP with ICMP.			
Option	Description									
<i>enable</i>	Deny TCP with ICMP.									
<i>disable</i>	Disable denying TCP with ICMP.									
discovered-device-timeout	Timeout for discovered devices.	integer	Minimum value: 1 Maximum value: 365	28						
email-portal-check-dns	Enable/disable using DNS to validate email addresses collected by a captive portal.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable email address checking with DNS.		
	<i>enable</i>	Enable email address checking with DNS.		
gui-icap	Enable/disable ICAP on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable ICAP on the GUI.		
	<i>disable</i>	Disable ICAP on the GUI.		
gui-implicit-policy	Enable/disable implicit firewall policies on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable implicit firewall policies on the GUI.		
	<i>disable</i>	Disable implicit firewall policies on the GUI.		
gui-dns-database	Enable/disable DNS database settings on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable DNS database settings on the GUI.		
	<i>disable</i>	Disable DNS database settings on the GUI.		
gui-proxy-inspection	Enable/disable the proxy features on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable the proxy features on the GUI.		
	<i>disable</i>	Disable the proxy features on the GUI.		
gui-multicast-policy	Enable/disable multicast firewall policies on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable multicast firewall policies on the GUI.		
	<i>disable</i>	Disable multicast firewall policies on the GUI.		
gui-dos-policy	Enable/disable DoS policies on the GUI.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable DoS policies on the GUI.		
	<i>disable</i>	Disable DoS policies on the GUI.		
gui-object-colors	Enable/disable object colors on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable object colors on the GUI.		
	<i>disable</i>	Disable object colors on the GUI.		
gui-voip-profile	Enable/disable VoIP profiles on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable VoIP profiles on the GUI.		
	<i>disable</i>	Disable VoIP profiles on the GUI.		
gui-security-profile-group	Enable/disable Security Profile Groups on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Security Profile Groups on the GUI.		
	<i>disable</i>	Disable Security Profile Groups on the GUI.		
gui-wanopt-cache	Enable/disable WAN Optimization and Web Caching on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable WAN Optimization and Web Caching on the GUI.		
	<i>disable</i>	Disable WAN Optimization and Web Caching on the GUI.		
gui-explicit-proxy	Enable/disable the explicit proxy on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable the explicit proxy on the GUI.		
	<i>disable</i>	Disable the explicit proxy on the GUI.		
gui-policy-based-ipsec	Enable/disable policy-based IPsec VPN on the GUI.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable policy-based IPsec VPN on the GUI.		
	<i>disable</i>	Disable policy-based IPsec VPN on the GUI.		
gui-threat-weight	Enable/disable threat weight on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable threat weight on the GUI.		
	<i>disable</i>	Disable threat weight on the GUI.		
gui-spamfilter	Enable/disable Antispam on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Antispam on the GUI.		
	<i>disable</i>	Disable Antispam on the GUI.		
gui-file-filter	Enable/disable File-filter on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable File-filter on the GUI.		
	<i>disable</i>	Disable File-filter on the GUI.		
gui-application-control	Enable/disable application control on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable application control on the GUI.		
	<i>disable</i>	Disable application control on the GUI.		
gui-ips	Enable/disable IPS on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable IPS on the GUI.		
	<i>disable</i>	Disable IPS on the GUI.		
gui-dhcp-advanced	Enable/disable advanced DHCP options on the GUI.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable advanced DHCP options on the GUI.		
	<i>disable</i>	Disable advanced DHCP options on the GUI.		
gui-vpn	Enable/disable VPN tunnels on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable VPN tunnels on the GUI.		
	<i>disable</i>	Disable VPN tunnels on the GUI.		
gui-webfilter-advanced	Enable/disable advanced web filtering on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable advanced web filtering on the GUI.		
	<i>disable</i>	Disable advanced web filtering on the GUI.		
gui-traffic-shaping	Enable/disable traffic shaping on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable traffic shaping on the GUI.		
	<i>disable</i>	Disable traffic shaping on the GUI.		
gui-antivirus	Enable/disable AntiVirus on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable AntiVirus on the GUI.		
	<i>disable</i>	Disable AntiVirus on the GUI.		
gui-webfilter	Enable/disable Web filtering on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Web filtering on the GUI.		
	<i>disable</i>	Disable Web filtering on the GUI.		
gui-videofilter	Enable/disable Video filtering on the GUI.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable Video filtering on the GUI.		
	<i>disable</i>	Disable Video filtering on the GUI.		
gui-dnsfilter	Enable/disable DNS Filtering on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable DNS Filtering on the GUI.		
	<i>disable</i>	Disable DNS Filtering on the GUI.		
gui-advanced-policy	Enable/disable advanced policy configuration on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable advanced policy configuration on the GUI.		
	<i>disable</i>	Disable advanced policy configuration on the GUI.		
gui-allow-unnamed-policy	Enable/disable the requirement for policy naming on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable the requirement for policy naming on the GUI.		
	<i>disable</i>	Disable the requirement for policy naming on the GUI.		
gui-email-collection	Enable/disable email collection on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable email collection on the GUI.		
	<i>disable</i>	Disable email collection on the GUI.		
gui-multiple-interface-policy	Enable/disable adding multiple interfaces to a policy on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable adding multiple interfaces to a policy on the GUI.		
	<i>disable</i>	Disable adding multiple interfaces to a policy on the GUI.		

Parameter	Description	Type	Size	Default
gui-policy-disclaimer	Enable/disable policy disclaimer on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable policy disclaimer on the GUI.		
	<i>disable</i>	Disable policy disclaimer on the GUI.		
gui-ztna	Enable/disable Zero Trust Network Access features on the GUI.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable Zero Trust Network Access features on the GUI.		
	<i>disable</i>	Disable Zero Trust Network Access features on the GUI.		
gui-ot	Enable/disable Operational technology features on the GUI.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable Operational technology features on the GUI.		
	<i>disable</i>	Disable Operational technology features on the GUI.		
block-land-attack	Enable/disable blocking of land attacks.	option	-	disable
	Option	Description		
	<i>disable</i>	Do not block land attack.		
	<i>enable</i>	Block land attack.		
default-app-port-as-service	Enable/disable policy service enforcement based on application default ports.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
application-bandwidth-tracking	Enable/disable application bandwidth tracking.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable application bandwidth tracking.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable application bandwidth tracking.		
default-policy-expiry-days	Default policy expiry in days.	integer	Minimum value: 0 Maximum value: 365	30
gui-enforce-change-summary	Enforce change summaries for select tables in the GUI.	option	-	require
	Option	Description		
	<i>disable</i>	No change summary requirement.		
	<i>require</i>	Change summary required.		
	<i>optional</i>	Change summary optional.		
internet-service-database-cache	Enable/disable Internet Service database caching.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable Internet Service database caching.		
	<i>enable</i>	Enable Internet Service database caching.		

config system sms-server

Configure SMS server for sending SMS messages to support user authentication.

```

config system sms-server
    Description: Configure SMS server for sending SMS messages to support user
authentication.
    edit <name>
        set mail-server {string}
    next
end

```

config system sms-server

Parameter	Description	Type	Size	Default
name	Name of SMS server.	string	Maximum length: 35	
mail-server	Email-to-SMS server domain name.	string	Maximum length: 63	

config system snmp community

SNMP community configuration.

```

config system snmp community
  Description: SNMP community configuration.
  edit <id>
    set name {string}
    set status [enable|disable]
    config hosts
      Description: Configure IPv4 SNMP managers (hosts).
      edit <id>
        set source-ip {ipv4-address}
        set ip {user}
        set ha-direct [enable|disable]
        set host-type [any|query|...]
      next
    end
  config hosts6
    Description: Configure IPv6 SNMP managers.
    edit <id>
      set source-ipv6 {ipv6-address}
      set ipv6 {ipv6-prefix}
      set ha-direct [enable|disable]
      set host-type [any|query|...]
    next
  end
  set query-v1-status [enable|disable]
  set query-v1-port {integer}
  set query-v2c-status [enable|disable]
  set query-v2c-port {integer}
  set trap-v1-status [enable|disable]
  set trap-v1-lport {integer}
  set trap-v1-rport {integer}
  set trap-v2c-status [enable|disable]
  set trap-v2c-lport {integer}
  set trap-v2c-rport {integer}
  set events {option1}, {option2}, ...
  set mib-view {string}
  set vdoms <name1>, <name2>, ...
next
end

```

config system snmp community

Parameter	Description	Type	Size	Default						
id	Community ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
name	Community name.	string	Maximum length: 35							
status	Enable/disable this SNMP community.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
query-v1-status	Enable/disable SNMP v1 queries.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
query-v1-port	SNMP v1 query port.	integer	Minimum value: 1 Maximum value: 65535	161						
query-v2c-status	Enable/disable SNMP v2c queries.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
query-v2c-port	SNMP v2c query port.	integer	Minimum value: 0 Maximum value: 65535	161						
trap-v1-status	Enable/disable SNMP v1 traps.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.					
Option	Description									
<i>enable</i>	Enable setting.									

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>disable</i>	Disable setting.					
	Option	Description								
<i>disable</i>	Disable setting.									
trap-v1-lport	SNMP v1 trap local port.	integer	Minimum value: 1 Maximum value: 65535	162						
trap-v1-rport	SNMP v1 trap remote port.	integer	Minimum value: 1 Maximum value: 65535	162						
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
trap-v2c-lport	SNMP v2c trap local port.	integer	Minimum value: 1 Maximum value: 65535	162						
trap-v2c-rport	SNMP v2c trap remote port.	integer	Minimum value: 1 Maximum value: 65535	162						

Parameter	Description	Type	Size	Default
events	SNMP trap events.	option	-	cpu-high mem-low log- full intf-ip vpn- tun-up vpn- tun-down ha- switch ha-hb- failure ips- signature ips- anomaly av- virus av- oversize av- pattern av- fragmented fm-if-change ha-member- up ha- member- down ent- conf-change av-conserve av-bypass av- oversize- passed av- oversize- blocked ips- pkg-update ips-fail-open faz- disconnect load-balance- real-server- down per- cpu-high dhcp pool- usage cert- expiry
Option		Description		
<i>cpu-high</i>		Send a trap when CPU usage is high.		
<i>mem-low</i>		Send a trap when available memory is low.		
<i>log-full</i>		Send a trap when log disk space becomes low.		
<i>intf-ip</i>		Send a trap when an interface IP address is changed.		
<i>vpn-tun-up</i>		Send a trap when a VPN tunnel comes up.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>vpn-tun-down</i>	Send a trap when a VPN tunnel goes down.		
	<i>ha-switch</i>	Send a trap after an HA failover when the backup unit has taken over.		
	<i>ha-hb-failure</i>	Send a trap when HA heartbeats are not received.		
	<i>ips-signature</i>	Send a trap when IPS detects an attack.		
	<i>ips-anomaly</i>	Send a trap when IPS finds an anomaly.		
	<i>av-virus</i>	Send a trap when AntiVirus finds a virus.		
	<i>av-oversize</i>	Send a trap when AntiVirus finds an oversized file.		
	<i>av-pattern</i>	Send a trap when AntiVirus finds file matching pattern.		
	<i>av-fragmented</i>	Send a trap when AntiVirus finds a fragmented file.		
	<i>fm-if-change</i>	Send a trap when FortiManager interface changes. Send a FortiManager trap.		
	<i>fm-conf-change</i>	Send a trap when a configuration change is made by a FortiProxy administrator and the FortiProxy is managed by FortiManager.		
	<i>ha-member-up</i>	Send a trap when an HA cluster member goes up.		
	<i>ha-member-down</i>	Send a trap when an HA cluster member goes down.		
	<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).		
	<i>av-conserve</i>	Send a trap when the FortiProxy enters conserve mode.		
	<i>av-bypass</i>	Send a trap when the FortiProxy enters bypass mode.		
	<i>av-oversize-passed</i>	Send a trap when AntiVirus passes an oversized file.		
	<i>av-oversize-blocked</i>	Send a trap when AntiVirus blocks an oversized file.		
	<i>ips-pkg-update</i>	Send a trap when the IPS signature database or engine is updated.		
	<i>ips-fail-open</i>	Send a trap when the IPS network buffer is full.		
	<i>faz-disconnect</i>	Send a trap when a FortiAnalyzer disconnects from the FortiProxy.		
	<i>load-balance-real-server-down</i>	Send a trap when a server load balance real server goes down.		
	<i>device-new</i>	Send a trap when a new device is found.		
<i>per-cpu-high</i>	Send a trap when per-CPU usage is high.			
<i>dhcp</i>	Send a trap when the DHCP server exhausts the IP pool, an IP address already is in use, or a DHCP client interface received a DHCP-NAK.			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>pool-usage</i>	Send a trap about ippool usage.		
	<i>cert-expiry</i>	Send a trap when a local certificate is near expiry.		
mib-view	SNMP access control MIB view.	string	Maximum length: 32	
vdoms <name>	SNMP access control VDOMs. VDOM name.	string	Maximum length: 79	

config hosts

Parameter	Description	Type	Size	Default
id	Host entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
source-ip	Source IPv4 address for SNMP traps.	ipv4-address	Not Specified	0.0.0.0
ip	IPv4 address of the SNMP manager (host).	user	Not Specified	
ha-direct	Enable/disable direct management of HA cluster members.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
host-type	Control whether the SNMP manager sends SNMP queries, receives SNMP traps, or both. No traps will be sent when IP type is subnet.	option	-	any
	Option	Description		
	<i>any</i>	Accept queries from and send traps to this SNMP manager.		
	<i>query</i>	Accept queries from this SNMP manager but do not send traps.		
	<i>trap</i>	Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.		

config hosts6

Parameter	Description	Type	Size	Default								
id	Host6 entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
source-ipv6	Source IPv6 address for SNMP traps.	ipv6-address	Not Specified	::								
ipv6	SNMP manager IPv6 address prefix.	ipv6-prefix	Not Specified	::/0								
ha-direct	Enable/disable direct management of HA cluster members.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
host-type	Control whether the SNMP manager sends SNMP queries, receives SNMP traps, or both.	option	-	any								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Accept queries from and send traps to this SNMP manager.</td></tr><tr><td><i>query</i></td><td>Accept queries from this SNMP manager but do not send traps.</td></tr><tr><td><i>trap</i></td><td>Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.</td></tr></table>				Option	Description	<i>any</i>	Accept queries from and send traps to this SNMP manager.	<i>query</i>	Accept queries from this SNMP manager but do not send traps.	<i>trap</i>	Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.
	Option	Description										
	<i>any</i>	Accept queries from and send traps to this SNMP manager.										
	<i>query</i>	Accept queries from this SNMP manager but do not send traps.										
<i>trap</i>	Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.											

config system snmp mib-view

SNMP Access Control MIB View configuration.

```

config system snmp mib-view
    Description: SNMP Access Control MIB View configuration.
    edit <name>
        set include {string}
        set exclude {string}
    next
end

```

config system snmp mib-view

Parameter	Description	Type	Size	Default
name	MIB view name.	string	Maximum length: 32	
include	OID subtrees to be included in the view. Maximum 16 allowed.	string	Maximum length: 79	
exclude	OID subtrees to be excluded in the view. Maximum 64 allowed.	string	Maximum length: 79	

config system snmp sysinfo

SNMP system info configuration.

```
config system snmp sysinfo
    Description: SNMP system info configuration.
    set status [enable|disable]
    set engine-id-type [text|hex|...]
    set engine-id {string}
    set description {var-string}
    set contact-info {var-string}
    set location {var-string}
    set trap-high-cpu-threshold {integer}
    set trap-low-memory-threshold {integer}
    set trap-log-full-threshold {integer}
    set append-index [enable|disable]
end
```

config system snmp sysinfo

Parameter	Description	Type	Size	Default						
status	Enable/disable SNMP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
engine-id-type	Local SNMP engineID type (text/hex/mac).	option	-	text						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>text</i></td><td>Text format.</td></tr></table>				Option	Description	<i>text</i>	Text format.		
	Option	Description								
<i>text</i>	Text format.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>hex</i>	Octets format.		
	<i>mac</i>	MAC address format.		
engine-id	Local SNMP engineID string (maximum 27 characters).	string	Maximum length: 54	
description	System description.	var-string	Maximum length: 255	
contact-info	Contact information.	var-string	Maximum length: 255	
location	System location.	var-string	Maximum length: 255	
trap-high-cpu-threshold	CPU usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100	80
trap-low-memory-threshold	Memory usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100	80
trap-log-full-threshold	Log disk usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100	90
append-index	Enable/disable allowance of appending VDOM or interface index in some RFC tables.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config system snmp user

SNMP user configuration.

```
config system snmp user
  Description: SNMP user configuration.
  edit <name>
    set status [enable|disable]
    set trap-status [enable|disable]
```

```

set trap-lport {integer}
set trap-rport {integer}
set queries [enable|disable]
set query-port {integer}
set notify-hosts {ipv4-address}
set notify-hosts6 {ipv6-address}
set source-ip {ipv4-address}
set source-ipv6 {ipv6-address}
set ha-direct [enable|disable]
set events {option1}, {option2}, ...
set mib-view {string}
set vdoms <name1>, <name2>, ...
set security-level [no-auth-no-priv|auth-no-priv|...]
set auth-proto [md5|sha|...]
set auth-pwd {password}
set priv-proto [aes|des|...]
set priv-pwd {password}
next
end

```

config system snmp user

Parameter	Description	Type	Size	Default						
name	SNMP user name.	string	Maximum length: 32							
status	Enable/disable this SNMP user.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
trap-status	Enable/disable traps for this SNMP user.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
trap-lport	SNMPv3 local trap port.	integer	Minimum value: 1 Maximum value: 65535	162						

Parameter	Description	Type	Size	Default
trap-rport	SNMPv3 trap remote port.	integer	Minimum value: 1 Maximum value: 65535	162
queries	Enable/disable SNMP queries for this user.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
query-port	SNMPv3 query port.	integer	Minimum value: 1 Maximum value: 65535	161
notify-hosts	SNMP managers to send notifications (traps) to.	ipv4-address	Not Specified	
notify-hosts6	IPv6 SNMP managers to send notifications (traps) to.	ipv6-address	Not Specified	
source-ip	Source IP for SNMP trap.	ipv4-address	Not Specified	0.0.0.0
source-ipv6	Source IPv6 for SNMP trap.	ipv6-address	Not Specified	::
ha-direct	Enable/disable direct management of HA cluster members.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		

Parameter	Description	Type	Size	Default
events	SNMP notifications (traps) to send.	option	-	cpu-high mem-low log- full intf-ip vpn- tun-up vpn- tun-down ha- switch ha-hb- failure ips- signature ips- anomaly av- virus av- oversize av- pattern av- fragmented fm-if-change ha-member- up ha- member- down ent- conf-change av-conserve av-bypass av- oversize- passed av- oversize- blocked ips- pkg-update ips-fail-open faz- disconnect load-balance- real-server- down per- cpu-high dhcp pool- usage cert- expiry
Option		Description		
<i>cpu-high</i>		Send a trap when CPU usage is high.		
<i>mem-low</i>		Send a trap when available memory is low.		
<i>log-full</i>		Send a trap when log disk space becomes low.		
<i>intf-ip</i>		Send a trap when an interface IP address is changed.		
<i>vpn-tun-up</i>		Send a trap when a VPN tunnel comes up.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>vpn-tun-down</i>	Send a trap when a VPN tunnel goes down.		
	<i>ha-switch</i>	Send a trap after an HA failover when the backup unit has taken over.		
	<i>ha-hb-failure</i>	Send a trap when HA heartbeats are not received.		
	<i>ips-signature</i>	Send a trap when IPS detects an attack.		
	<i>ips-anomaly</i>	Send a trap when IPS finds an anomaly.		
	<i>av-virus</i>	Send a trap when AntiVirus finds a virus.		
	<i>av-oversize</i>	Send a trap when AntiVirus finds an oversized file.		
	<i>av-pattern</i>	Send a trap when AntiVirus finds file matching pattern.		
	<i>av-fragmented</i>	Send a trap when AntiVirus finds a fragmented file.		
	<i>fm-if-change</i>	Send a trap when FortiManager interface changes. Send a FortiManager trap.		
	<i>fm-conf-change</i>	Send a trap when a configuration change is made by a FortiProxy administrator and the FortiProxy is managed by FortiManager.		
	<i>ha-member-up</i>	Send a trap when an HA cluster member goes up.		
	<i>ha-member-down</i>	Send a trap when an HA cluster member goes down.		
	<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).		
	<i>av-conserve</i>	Send a trap when the FortiProxy enters conserve mode.		
	<i>av-bypass</i>	Send a trap when the FortiProxy enters bypass mode.		
	<i>av-oversize-passed</i>	Send a trap when AntiVirus passes an oversized file.		
	<i>av-oversize-blocked</i>	Send a trap when AntiVirus blocks an oversized file.		
	<i>ips-pkg-update</i>	Send a trap when the IPS signature database or engine is updated.		
	<i>ips-fail-open</i>	Send a trap when the IPS network buffer is full.		
	<i>faz-disconnect</i>	Send a trap when a FortiAnalyzer disconnects from the FortiProxy.		
	<i>load-balance-real-server-down</i>	Send a trap when a server load balance real server goes down.		
	<i>device-new</i>	Send a trap when a new device is found.		
	<i>per-cpu-high</i>	Send a trap when per-CPU usage is high.		
	<i>dhcp</i>	Send a trap when the DHCP server exhausts the IP pool, an IP address already is in use, or a DHCP client interface received a DHCP-NAK.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>pool-usage</i>	Send a trap about ippool usage.		
	<i>cert-expiry</i>	Send a trap when a local certificate is near expiry.		
mib-view	SNMP access control MIB view.	string	Maximum length: 32	
vdoms <name>	SNMP access control VDOMs. VDOM name.	string	Maximum length: 79	
security-level	Security level for message authentication and encryption.	option	-	no-auth-no-priv
	Option	Description		
	<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).		
	<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).		
	<i>auth-priv</i>	Message with authentication and privacy (encryption).		
auth-proto	Authentication protocol.	option	-	sha
	Option	Description		
	<i>md5</i>	HMAC-MD5-96 authentication protocol.		
	<i>sha</i>	HMAC-SHA-96 authentication protocol.		
	<i>sha224</i>	HMAC-SHA224 authentication protocol.		
	<i>sha256</i>	HMAC-SHA256 authentication protocol.		
	<i>sha384</i>	HMAC-SHA384 authentication protocol.		
	<i>sha512</i>	HMAC-SHA512 authentication protocol.		
auth-pwd	Password for authentication protocol.	password	Not Specified	
priv-proto	Privacy (encryption) protocol.	option	-	aes
	Option	Description		
	<i>aes</i>	CFB128-AES-128 symmetric encryption protocol.		
	<i>des</i>	CBC-DES symmetric encryption protocol.		
	<i>aes256</i>	CFB128-AES-256 symmetric encryption protocol.		
	<i>aes256cisco</i>	CFB128-AES-256 symmetric encryption protocol compatible with CISCO.		
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified	

config system source-ip status

Show configured service source-IP.

```
config system source-ip status
    Description: Show configured service source-IP.
end
```

config system span-port

Configure SPAN port.

```
config system span-port
    Description: Configure SPAN port.
    edit <id>
        set status [disable|enable]
        set span-source-port {string}
        set span-dest-port {string}
        set span-direction [rx|tx|...]
    next
end
```

config system span-port

Parameter	Description	Type	Size	Default
id	SPAN port id.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Enable/disable SPAN.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable SPAN.		
	<i>enable</i>	Enable SPAN.		
span-source-port	SPAN source ports.	string	Maximum length: 15	
span-dest-port	SPAN destination port.	string	Maximum length: 15	
span-direction	SPAN direction.	option	-	both

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>rx</i>	Span receive direction only.		
	<i>tx</i>	Span transmit direction only.		
	<i>both</i>	Span both directions.		

config system speed-test-schedule

Speed test schedule for each interface.

```

config system speed-test-schedule
    Description: Speed test schedule for each interface.
    edit <interface>
        set status [disable|enable]
        set diffserv {user}
        set server-name {string}
        set mode [UDP|TCP|...]
        set schedules <name1>, <name2>, ...
        set dynamic-server [disable|enable]
        set update-inbandwidth [disable|enable]
        set update-outbandwidth [disable|enable]
        set update-inbandwidth-maximum {integer}
        set update-inbandwidth-minimum {integer}
        set update-outbandwidth-maximum {integer}
        set update-outbandwidth-minimum {integer}
    next
end

```

config system speed-test-schedule

Parameter	Description	Type	Size	Default
interface	Interface name.	string	Maximum length: 35	
status	Enable/disable scheduled speed test.	option	-	enable
	Option	Description		
	<i>disable</i>	Disable scheduled speed test.		
	<i>enable</i>	Enable scheduled speed test.		
diffserv	DSCP used for speed test.	user	Not Specified	

Parameter	Description	Type	Size	Default								
server-name	Speed test server name.	string	Maximum length: 35									
mode	Protocol Auto, TCP or UDP used for speed test.	option	-	Auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>UDP</td><td>Protocol UDP for speed test.</td></tr><tr><td>TCP</td><td>Protocol TCP for speed test.</td></tr><tr><td>Auto</td><td>Dynamically selects TCP or UDP based on the speed test setting</td></tr></table>	Option	Description	UDP	Protocol UDP for speed test.	TCP	Protocol TCP for speed test.	Auto	Dynamically selects TCP or UDP based on the speed test setting			
Option	Description											
UDP	Protocol UDP for speed test.											
TCP	Protocol TCP for speed test.											
Auto	Dynamically selects TCP or UDP based on the speed test setting											
schedules <name>	Schedules for the interface. Name of a firewall recurring schedule.	string	Maximum length: 31									
dynamic-server	Enable/disable dynamic server option.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable dynamic server.</td></tr><tr><td>enable</td><td>Enable dynamic server. The speed test server will be found automatically.</td></tr></table>	Option	Description	disable	Disable dynamic server.	enable	Enable dynamic server. The speed test server will be found automatically.					
Option	Description											
disable	Disable dynamic server.											
enable	Enable dynamic server. The speed test server will be found automatically.											
update-inbandwidth	Enable/disable bypassing interface's inbound bandwidth setting.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Honor interface's inboundbandwidth shaping.</td></tr><tr><td>enable</td><td>Ignore interface's inboundbandwidth shaping.</td></tr></table>	Option	Description	disable	Honor interface's inboundbandwidth shaping.	enable	Ignore interface's inboundbandwidth shaping.					
Option	Description											
disable	Honor interface's inboundbandwidth shaping.											
enable	Ignore interface's inboundbandwidth shaping.											
update-outbandwidth	Enable/disable bypassing interface's outbound bandwidth setting.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Honor interface's outbandwidth shaping.</td></tr><tr><td>enable</td><td>Ignore updating interface's outbandwidth shaping.</td></tr></table>	Option	Description	disable	Honor interface's outbandwidth shaping.	enable	Ignore updating interface's outbandwidth shaping.					
Option	Description											
disable	Honor interface's outbandwidth shaping.											
enable	Ignore updating interface's outbandwidth shaping.											
update-inbandwidth-maximum	Maximum downloading bandwidth (kbps) to be used in a speed test.	integer	Minimum value: 0 Maximum value: 16776000	0								
update-inbandwidth-minimum	Minimum downloading bandwidth (kbps) to be considered effective.	integer	Minimum value: 0 Maximum value: 16776000	0								

Parameter	Description	Type	Size	Default
update-outbandwidth-maximum	Maximum uploading bandwidth (kbps) to be used in a speed test.	integer	Minimum value: 0 Maximum value: 16776000	0
update-outbandwidth-minimum	Minimum uploading bandwidth (kbps) to be considered effective.	integer	Minimum value: 0 Maximum value: 16776000	0

config system speed-test-server

Configure speed test server list.

```
config system speed-test-server
    Description: Configure speed test server list.
    edit <name>
        set timestamp {integer}
        config host
            Description: Hosts of the server.
            edit <id>
                set ip {ipv4-address}
                set port {integer}
                set user {string}
                set password {password}
                set longitude {string}
                set latitude {string}
                set distance {integer}
            next
        next
    end
next
end
```

config system speed-test-server

Parameter	Description	Type	Size	Default
name	Speed test server name.	string	Maximum length: 35	
timestamp	Speed test server timestamp.	integer	Minimum value: 0 Maximum value: 4294967295	0

config host

Parameter	Description	Type	Size	Default
id	Server host ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	Server host IPv4 address.	ipv4-address	Not Specified	0.0.0.0
port	Server host port number to communicate with client.	integer	Minimum value: 1 Maximum value: 65535	5204
user	Speed test host user name.	string	Maximum length: 64	
password	Speed test host password.	password	Not Specified	
longitude	Speed test host longitude.	string	Maximum length: 7	
latitude	Speed test host latitude.	string	Maximum length: 7	
distance	Speed test host distance.	integer	Minimum value: 0 Maximum value: 4294967295	0

config system speed-test-setting

Configure speed test setting.

```
config system speed-test-setting
    Description: Configure speed test setting.
    set latency-threshold {integer}
    set multiple-tcp-stream {integer}
end
```

config system speed-test-setting

Parameter	Description	Type	Size	Default
latency-threshold	Speed test latency threshold in milliseconds for the Auto mode. If the latency exceeds this threshold, the speed test will use the UDP protocol; otherwise, it will use the TCP protocol.	integer	Minimum value: 0 Maximum value: 2000	60
multiple-tcp-stream	Number of parallel client streams for the TCP protocol to run during the speed test.	integer	Minimum value: 1 Maximum value: 64	4

config system sso-admin

Configure SSO admin users.

```
config system sso-admin
  Description: Configure SSO admin users.
  edit <name>
    set accprofile {string}
    set vdom <name1>, <name2>, ...
  next
end
```

config system sso-admin

Parameter	Description	Type	Size	Default
name	SSO admin name.	string	Maximum length: 64	
accprofile	SSO admin user access profile.	string	Maximum length: 35	
vdom <name>	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79	

config system sso-forticloud-admin

Configure FortiCloud SSO admin users.

```
config system sso-forticloud-admin
  Description: Configure FortiCloud SSO admin users.
  edit <name>
```

```
        set accprofile {string}
        set vdom <name1>, <name2>, ...
    next
end
```

config system sso-forticloud-admin

Parameter	Description	Type	Size	Default
name	FortiCloud SSO admin name.	string	Maximum length: 64	
accprofile	FortiCloud SSO admin user access profile.	string	Maximum length: 35	
vdom <name>	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79	

config system sso-fortigate-cloud-admin

Configure FortiCloud SSO admin users.

```
config system sso-fortigate-cloud-admin
    Description: Configure FortiCloud SSO admin users.
    edit <name>
        set accprofile {string}
        set vdom <name1>, <name2>, ...
    next
end
```

config system sso-fortigate-cloud-admin

Parameter	Description	Type	Size	Default
name	FortiCloud SSO admin name.	string	Maximum length: 64	
accprofile	FortiCloud SSO admin user access profile.	string	Maximum length: 35	
vdom <name>	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79	

config system startup-error-log

Display startup config error on console.

```
config system startup-error-log
    Description: Display startup config error on console.
end
```

config system status

System status.

```
config system status
    Description: System status.
end
```

config system storage

Configure logical storage.

```
config system storage
    Description: Configure logical storage.
    edit <name>
        set status [enable|disable]
        set media-status [enable|disable|...]
        set order {integer}
        set partition {string}
        set device {string}
        set size {integer}
        set usage [log|wanopt]
        set wanopt-mode [mix|wanopt|...]
    next
end
```

config system storage

Parameter	Description	Type	Size	Default
name	Storage name.	string	Maximum length: 35	default_n
status	Enable/disable storage.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
media-status	The physical status of current media.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Storage is enabled.		
	<i>disable</i>	Storage is disabled.		
	<i>fail</i>	Storage have some fail sector.		
order	Set storage order.	integer	Minimum value: 0 Maximum value: 255	0
partition	Label of underlying partition.	string	Maximum length: 16	<unknown>
device	Partition device.	string	Maximum length: 19	?
size	Partition size.	integer	Minimum value: 0 Maximum value: 4294967295	0
usage	Use hard disk for logging or WAN Optimization.	option	-	log
	Option	Description		
	<i>log</i>	Use hard disk for logging.		
	<i>wanopt</i>	Use hard disk for WAN Optimization.		
wanopt-mode	WAN Optimization mode	option	-	webcache
	Option	Description		
	<i>mix</i>	Use hard disk for WAN Optimization mix mode.		
	<i>wanopt</i>	Use hard disk for WAN Optimization wanopt mode.		
	<i>webcache</i>	Use hard disk for WAN Optimization webcache mode.		

config system vdom-dns

Configure DNS servers for a non-management VDOM.

```
config system vdom-dns
  Description: Configure DNS servers for a non-management VDOM.
  set vdom-dns [enable|disable]
  set primary {ipv4-address}
  set secondary {ipv4-address}
```

```

set protocol {option1}, {option2}, ...
set ssl-certificate {string}
set server-hostname <hostname1>, <hostname2>, ...
set ip6-primary {ipv6-address}
set ip6-secondary {ipv6-address}
set source-ip {ipv4-address}
set interface-select-method [auto|specify]
set interface {string}
set server-select-method [least-rtt|failover]
set alt-primary {ipv4-address}
set alt-secondary {ipv4-address}

```

```
end
```

config system vdom-dns

Parameter	Description	Type	Size	Default								
vdom-dns	Enable/disable configuring DNS servers for the current VDOM.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable configuring DNS servers for the current VDOM.</td></tr><tr><td><i>disable</i></td><td>Disable configuring DNS servers for the current VDOM.</td></tr></table>	Option	Description	<i>enable</i>	Enable configuring DNS servers for the current VDOM.	<i>disable</i>	Disable configuring DNS servers for the current VDOM.					
Option	Description											
<i>enable</i>	Enable configuring DNS servers for the current VDOM.											
<i>disable</i>	Disable configuring DNS servers for the current VDOM.											
primary	Primary DNS server IP address for the VDOM.	ipv4-address	Not Specified	0.0.0.0								
secondary	Secondary DNS server IP address for the VDOM.	ipv4-address	Not Specified	0.0.0.0								
protocol	DNS transport protocols.	option	-	cleartext								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>cleartext</i></td><td>DNS over UDP/53, DNS over TCP/53.</td></tr><tr><td><i>dot</i></td><td>DNS over TLS/853.</td></tr><tr><td><i>doh</i></td><td>DNS over HTTPS/443.</td></tr></table>	Option	Description	<i>cleartext</i>	DNS over UDP/53, DNS over TCP/53.	<i>dot</i>	DNS over TLS/853.	<i>doh</i>	DNS over HTTPS/443.			
Option	Description											
<i>cleartext</i>	DNS over UDP/53, DNS over TCP/53.											
<i>dot</i>	DNS over TLS/853.											
<i>doh</i>	DNS over HTTPS/443.											
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory								
server-hostname <hostname>	DNS server host name list. DNS server host name list separated by space (maximum 4 domains).	string	Maximum length: 127									
ip6-primary	Primary IPv6 DNS server IP address for the VDOM.	ipv6-address	Not Specified	::								
ip6-secondary	Secondary IPv6 DNS server IP address for the VDOM.	ipv6-address	Not Specified	::								

Parameter	Description	Type	Size	Default
source-ip	Source IP for communications with the DNS server.	ipv4-address	Not Specified	0.0.0.0
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
server-select-method	Specify how configured servers are prioritized.	option	-	least-rtt
	Option	Description		
	<i>least-rtt</i>	Select servers based on least round trip time.		
	<i>failover</i>	Select servers based on the order they are configured.		
alt-primary	Alternate primary DNS server. This is not used as a failover DNS server.	ipv4-address	Not Specified	0.0.0.0
alt-secondary	Alternate secondary DNS server. This is not used as a failover DNS server.	ipv4-address	Not Specified	0.0.0.0

config system vdom-exception

Global configuration objects that can be configured independently across different ha peers for all VDOMs or for the defined VDOM scope.

```

config system vdom-exception
    Description: Global configuration objects that can be configured independently across
different ha peers for all VDOMs or for the defined VDOM scope.
    edit <id>
        set object [log.fortianalyzer.setting|log.fortianalyzer.override-setting|...]
        set scope [all|inclusive|...]
        set vdom <name1>, <name2>, ...
    next
end

```

config system vdom-exception

Parameter	Description	Type	Size	Default
id	Index.	integer	Minimum value: 1 Maximum value: 4096	0
object	Name of the configuration object that can be configured independently for all VDOMs.	option	-	

Option	Description
<i>log.fortianalyzer.setting</i>	log.fortianalyzer.setting
<i>log.fortianalyzer.override-setting</i>	log.fortianalyzer.override-setting
<i>log.fortianalyzer2.setting</i>	log.fortianalyzer2.setting
<i>log.fortianalyzer2.override-setting</i>	log.fortianalyzer2.override-setting
<i>log.fortianalyzer3.setting</i>	log.fortianalyzer3.setting
<i>log.fortianalyzer3.override-setting</i>	log.fortianalyzer3.override-setting
<i>log.fortianalyzer-cloud.setting</i>	log.fortianalyzer-cloud.setting
<i>log.fortianalyzer-cloud.override-setting</i>	log.fortianalyzer-cloud.override-setting
<i>log.syslogd.setting</i>	log.syslogd.setting
<i>log.syslogd.override-setting</i>	log.syslogd.override-setting
<i>log.syslogd2.setting</i>	log.syslogd2.setting
<i>log.syslogd2.override-setting</i>	log.syslogd2.override-setting
<i>log.syslogd3.setting</i>	log.syslogd3.setting
<i>log.syslogd3.override-setting</i>	log.syslogd3.override-setting
<i>log.syslogd4.setting</i>	log.syslogd4.setting
<i>log.syslogd4.override-setting</i>	log.syslogd4.override-setting
<i>system.gre-tunnel</i>	system.gre-tunnel
<i>system.central-management</i>	system.central-management
<i>system.csf</i>	system.csf
<i>user.radius</i>	user.radius

Parameter	Description	Type	Size	Default																																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>system.snmp.sysinfo</i></td><td>system.snmp.sysinfo</td></tr><tr><td><i>system.snmp.community</i></td><td>system.snmp.community</td></tr><tr><td><i>system.snmp.user</i></td><td>system.snmp.user</td></tr><tr><td><i>system.interface</i></td><td>system.interface</td></tr><tr><td><i>vpn.ipsec.phase1-interface</i></td><td>vpn.ipsec.phase1-interface</td></tr><tr><td><i>vpn.ipsec.phase2-interface</i></td><td>vpn.ipsec.phase2-interface</td></tr><tr><td><i>router.bgp</i></td><td>router.bgp</td></tr><tr><td><i>router.route-map</i></td><td>router.route-map</td></tr><tr><td><i>router.prefix-list</i></td><td>router.prefix-list</td></tr><tr><td><i>firewall.ippool</i></td><td>firewall.ippool</td></tr><tr><td><i>firewall.ippool6</i></td><td>firewall.ippool6</td></tr><tr><td><i>router.static</i></td><td>router.static</td></tr><tr><td><i>router.static6</i></td><td>router.static6</td></tr><tr><td><i>firewall.vip</i></td><td>firewall.vip</td></tr><tr><td><i>firewall.vip6</i></td><td>firewall.vip6</td></tr><tr><td><i>system.sdwan</i></td><td>system.sdwan</td></tr><tr><td><i>system.saml</i></td><td>system.saml</td></tr><tr><td><i>router.policy</i></td><td>router.policy</td></tr><tr><td><i>router.policy6</i></td><td>router.policy6</td></tr><tr><td><i>log.syslogd.setting</i></td><td>log.syslogd.setting</td></tr><tr><td><i>log.syslogd.override-setting</i></td><td>log.syslogd.override-setting</td></tr></table>	Option	Description	<i>system.snmp.sysinfo</i>	system.snmp.sysinfo	<i>system.snmp.community</i>	system.snmp.community	<i>system.snmp.user</i>	system.snmp.user	<i>system.interface</i>	system.interface	<i>vpn.ipsec.phase1-interface</i>	vpn.ipsec.phase1-interface	<i>vpn.ipsec.phase2-interface</i>	vpn.ipsec.phase2-interface	<i>router.bgp</i>	router.bgp	<i>router.route-map</i>	router.route-map	<i>router.prefix-list</i>	router.prefix-list	<i>firewall.ippool</i>	firewall.ippool	<i>firewall.ippool6</i>	firewall.ippool6	<i>router.static</i>	router.static	<i>router.static6</i>	router.static6	<i>firewall.vip</i>	firewall.vip	<i>firewall.vip6</i>	firewall.vip6	<i>system.sdwan</i>	system.sdwan	<i>system.saml</i>	system.saml	<i>router.policy</i>	router.policy	<i>router.policy6</i>	router.policy6	<i>log.syslogd.setting</i>	log.syslogd.setting	<i>log.syslogd.override-setting</i>	log.syslogd.override-setting			
	Option	Description																																														
	<i>system.snmp.sysinfo</i>	system.snmp.sysinfo																																														
	<i>system.snmp.community</i>	system.snmp.community																																														
	<i>system.snmp.user</i>	system.snmp.user																																														
	<i>system.interface</i>	system.interface																																														
	<i>vpn.ipsec.phase1-interface</i>	vpn.ipsec.phase1-interface																																														
	<i>vpn.ipsec.phase2-interface</i>	vpn.ipsec.phase2-interface																																														
	<i>router.bgp</i>	router.bgp																																														
	<i>router.route-map</i>	router.route-map																																														
	<i>router.prefix-list</i>	router.prefix-list																																														
	<i>firewall.ippool</i>	firewall.ippool																																														
	<i>firewall.ippool6</i>	firewall.ippool6																																														
	<i>router.static</i>	router.static																																														
	<i>router.static6</i>	router.static6																																														
	<i>firewall.vip</i>	firewall.vip																																														
	<i>firewall.vip6</i>	firewall.vip6																																														
	<i>system.sdwan</i>	system.sdwan																																														
	<i>system.saml</i>	system.saml																																														
	<i>router.policy</i>	router.policy																																														
<i>router.policy6</i>	router.policy6																																															
<i>log.syslogd.setting</i>	log.syslogd.setting																																															
<i>log.syslogd.override-setting</i>	log.syslogd.override-setting																																															
scope	Determine whether the configuration object can be configured separately for all VDOMs or if some VDOMs share the same configuration.	option	-	all																																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Object configuration independent for all VDOMs.</td></tr><tr><td><i>inclusive</i></td><td>Object configuration independent for the listed VDOMs. Other VDOMs use the global configuration.</td></tr><tr><td><i>exclusive</i></td><td>Use the global object configuration for the listed VDOMs. Other VDOMs can be configured independently.</td></tr></table>	Option	Description	<i>all</i>	Object configuration independent for all VDOMs.	<i>inclusive</i>	Object configuration independent for the listed VDOMs. Other VDOMs use the global configuration.	<i>exclusive</i>	Use the global object configuration for the listed VDOMs. Other VDOMs can be configured independently.																																							
	Option	Description																																														
	<i>all</i>	Object configuration independent for all VDOMs.																																														
	<i>inclusive</i>	Object configuration independent for the listed VDOMs. Other VDOMs use the global configuration.																																														
<i>exclusive</i>	Use the global object configuration for the listed VDOMs. Other VDOMs can be configured independently.																																															

Parameter	Description	Type	Size	Default
vdom <name>	Names of the VDOMs. VDOM name.	string	Maximum length: 79	

config system vdom-link

Configure VDOM links.

```
config system vdom-link
  Description: Configure VDOM links.
  edit <name>
    next
  end
```

config system vdom-link

Parameter	Description	Type	Size	Default
name	VDOM link name (maximum = 11 characters).	string	Maximum length: 11	

config system vdom-property

Configure VDOM property.

```
config system vdom-property
  Description: Configure VDOM property.
  edit <name>
    set description {string}
    set snmp-index {integer}
    set ipsec-phase1-interface {user}
    set ipsec-phase2-interface {user}
    set firewall-policy {user}
    set firewall-address {user}
    set firewall-addrgrp {user}
    set custom-service {user}
    set service-group {user}
    set onetime-schedule {user}
    set recurring-schedule {user}
    set user {user}
    set user-group {user}
    set proxy {user}
    set log-disk-quota {user}
  next
end
```

config system vdom-property

Parameter	Description	Type	Size	Default
name	VDOM name.	string	Maximum length: 31	
description	Description.	string	Maximum length: 127	
snmp-index	Permanent SNMP Index of the virtual domain.	integer	Minimum value: 1 Maximum value: 2147483647	0
ipsec-phase1-interface	Maximum guaranteed number of VPN IPsec phase1 interface tunnels.	user	Not Specified	
ipsec-phase2-interface	Maximum guaranteed number of VPN IPsec phase2 interface tunnels.	user	Not Specified	
firewall-policy	Maximum guaranteed number of firewall policies (policy, DoS-policy4, DoS-policy6, multicast).	user	Not Specified	
firewall-address	Maximum guaranteed number of firewall addresses (IPv4, IPv6, multicast).	user	Not Specified	
firewall-addgrp	Maximum guaranteed number of firewall address groups (IPv4, IPv6).	user	Not Specified	
custom-service	Maximum guaranteed number of firewall custom services.	user	Not Specified	
service-group	Maximum guaranteed number of firewall service groups.	user	Not Specified	
onetime-schedule	Maximum guaranteed number of firewall one-time schedules.	user	Not Specified	
recurring-schedule	Maximum guaranteed number of firewall recurring schedules.	user	Not Specified	
user	Maximum guaranteed number of local users.	user	Not Specified	
user-group	Maximum guaranteed number of user groups.	user	Not Specified	
proxy	Maximum guaranteed number of concurrent proxy users.	user	Not Specified	
log-disk-quota	Log disk quota in megabytes (MB). Range depends on how much disk space is available.	user	Not Specified	

config system vdom-radius-server

Configure a RADIUS server to use as a RADIUS Single Sign On (RSSO) server for this VDOM.

```
config system vdom-radius-server
  Description: Configure a RADIUS server to use as a RADIUS Single Sign On (RSSO) server
for this VDOM.
  edit <name>
    set status [enable|disable]
    set radius-server-vdom {string}
  next
end
```

config system vdom-radius-server

Parameter	Description	Type	Size	Default
name	Name of the VDOM that you are adding the RADIUS server to.	string	Maximum length: 31	
status	Enable/disable the RSSO RADIUS server for this VDOM.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable the RSSO RADIUS server for this VDOM.		
	<i>disable</i>	Disable the RSSO RADIUS server for this VDOM.		
radius-server-vdom	Use this option to select another VDOM containing a VDOM RSSO RADIUS server to use for the current VDOM.	string	Maximum length: 31	

config system vdom

Configure virtual domain.

```
config system vdom
  Description: Configure virtual domain.
  edit <name>
    set short-name {string}
    set vcluster-id {integer}
    set flag {integer}
  next
end
```


config system vdom

Parameter	Description	Type	Size	Default
name	VDOM name.	string	Maximum length: 31	
short-name	VDOM short name.	string	Maximum length: 11	
vcluster-id	Virtual cluster ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
flag	Flag.	integer	Minimum value: 0 Maximum value: 4294967295	0

config system vne-tunnel

Configure virtual network enabler tunnel.

```
config system vne-tunnel
  Description: Configure virtual network enabler tunnel.
  set status [enable|disable]
  set interface {string}
  set ssl-certificate {string}
  set bmr-hostname {password}
  set ipv4-address {ipv4-classnet-host}
  set br {string}
  set update-url {string}
  set mode [map-e|fixed-ip|...]
  set http-username {string}
  set http-password {password}
end
```

config system vne-tunnel

Parameter	Description	Type	Size	Default
status	Enable/disable VNE tunnel.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable VNE tunnel.		
	<i>disable</i>	Disable VNE tunnel.		
interface	Interface name.	string	Maximum length: 15	
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory
bmr-hostname	BMR hostname.	password	Not Specified	
ipv4-address	Tunnel IPv4 address and netmask.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
br	IPv6 address or FQDN of the border relay.	string	Maximum length: 255	
update-url	URL of provisioning server.	string	Maximum length: 511	
mode	VNE tunnel mode.	option	-	map-e
	Option	Description		
	<i>map-e</i>	Map-e mode.		
	<i>fixed-ip</i>	Fixed-ip mode.		
	<i>ds-lite</i>	DS-Lite mode.		
http-username	HTTP authentication user name.	string	Maximum length: 64	
http-password	HTTP authentication password.	password	Not Specified	

config system vxlan

Configure VXLAN devices.

```
config system vxlan
  Description: Configure VXLAN devices.
  edit <name>
    set interface {string}
    set vni {integer}
    set ip-version [ipv4-unicast|ipv6-unicast]
    set remote-ip <ip1>, <ip2>, ...
```

```

    set remote-ip6 <ip61>, <ip62>, ...
    set dstport {integer}
    set multicast-ttl {integer}
next
end

```

config system vxlan

Parameter	Description	Type	Size	Default
name	VXLAN device or interface name. Must be a unique interface name.	string	Maximum length: 15	
interface	Outgoing interface for VXLAN encapsulated traffic.	string	Maximum length: 15	
vni	VXLAN network ID.	integer	Minimum value: 1 Maximum value: 16777215	0
ip-version	IP version to use for the VXLAN interface and so for communication over the VXLAN. IPv4 or IPv6 unicast.	option	-	ipv4-unicast
	Option	Description		
	ipv4-unicast	Use IPv4 unicast addressing over the VXLAN.		
	ipv6-unicast	Use IPv6 unicast addressing over the VXLAN.		
remote-ip <ip>	IPv4 address of the VXLAN interface on the device at the remote end of the VXLAN. IPv4 address.	string	Maximum length: 15	
remote-ip6 <ip6>	IPv6 IP address of the VXLAN interface on the device at the remote end of the VXLAN. IPv6 address.	string	Maximum length: 45	
dstport	VXLAN destination port.	integer	Minimum value: 1 Maximum value: 65535	4789
multicast-ttl	VXLAN multicast TTL.	integer	Minimum value: 1 Maximum value: 255	0

config system wccp

Configure WCCP.

```
config system wccp
  Description: Configure WCCP.
  edit <service-id>
    set router-id {ipv4-address}
    set cache-id {ipv4-address}
    set group-address {ipv4-address-multicast}
    set server-list {user}
    set router-list {user}
    set ports-defined [source|destination]
    set server-type [forward|proxy]
    set ports {user}
    set authentication [enable|disable]
    set password {password}
    set forward-method [GRE|L2|...]
    set cache-engine-method [GRE|L2]
    set service-type [auto|standard|...]
    set primary-hash {option1}, {option2}, ...
    set priority {integer}
    set protocol {integer}
    set assignment-weight {integer}
    set assignment-bucket-format [wccp-v2|cisco-implementation]
    set return-method [GRE|L2|...]
    set assignment-method [HASH|MASK|...]
    set assignment-srcaddr-mask {ipv4-netmask-any}
    set assignment-dstaddr-mask {ipv4-netmask-any}
  next
end
```

config system wccp

Parameter	Description	Type	Size	Default
service-id	Service ID.	string	Maximum length: 3	
router-id	IP address known to all cache engines. If all cache engines connect to the same FortiProxy interface, use the default 0.0.0.0.	ipv4-address	Not Specified	0.0.0.0
cache-id	IP address known to all routers. If the addresses are the same, use the default 0.0.0.0.	ipv4-address	Not Specified	0.0.0.0
group-address	IP multicast address used by the cache routers. For the FortiProxy to ignore multicast WCCP traffic, use the default 0.0.0.0.	ipv4-address-multicast	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default								
server-list	IP addresses and netmasks for up to four cache servers.	user	Not Specified									
router-list	IP addresses of one or more WCCP routers.	user	Not Specified									
ports-defined	Match method.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>source</i></td><td>Source port match.</td></tr><tr><td><i>destination</i></td><td>Destination port match.</td></tr></table>	Option	Description	<i>source</i>	Source port match.	<i>destination</i>	Destination port match.					
Option	Description											
<i>source</i>	Source port match.											
<i>destination</i>	Destination port match.											
server-type	Cache server type.	option	-	forward								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>forward</i></td><td>Forward server.</td></tr><tr><td><i>proxy</i></td><td>Proxy server.</td></tr></table>	Option	Description	<i>forward</i>	Forward server.	<i>proxy</i>	Proxy server.					
Option	Description											
<i>forward</i>	Forward server.											
<i>proxy</i>	Proxy server.											
ports	Service ports.	user	Not Specified									
authentication	Enable/disable MD5 authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable MD5 authentication.</td></tr><tr><td><i>disable</i></td><td>Disable MD5 authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable MD5 authentication.	<i>disable</i>	Disable MD5 authentication.					
Option	Description											
<i>enable</i>	Enable MD5 authentication.											
<i>disable</i>	Disable MD5 authentication.											
password	Password for MD5 authentication.	password	Not Specified									
forward-method	Method used to forward traffic to the cache servers.	option	-	GRE								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>GRE</i></td><td>GRE encapsulation.</td></tr><tr><td><i>L2</i></td><td>L2 rewrite.</td></tr><tr><td><i>any</i></td><td>GRE or L2.</td></tr></table>	Option	Description	<i>GRE</i>	GRE encapsulation.	<i>L2</i>	L2 rewrite.	<i>any</i>	GRE or L2.			
Option	Description											
<i>GRE</i>	GRE encapsulation.											
<i>L2</i>	L2 rewrite.											
<i>any</i>	GRE or L2.											
cache-engine-method	Method used to forward traffic to the routers or to return to the cache engine.	option	-	GRE								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>GRE</i></td><td>GRE encapsulation.</td></tr><tr><td><i>L2</i></td><td>L2 rewrite.</td></tr></table>	Option	Description	<i>GRE</i>	GRE encapsulation.	<i>L2</i>	L2 rewrite.					
Option	Description											
<i>GRE</i>	GRE encapsulation.											
<i>L2</i>	L2 rewrite.											

Parameter	Description	Type	Size	Default										
service-type	WCCP service type used by the cache server for logical interception and redirection of traffic.	option	-	auto										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>auto</td></tr><tr><td><i>standard</i></td><td>Standard service.</td></tr><tr><td><i>dynamic</i></td><td>Dynamic service.</td></tr></table>	Option	Description	<i>auto</i>	auto	<i>standard</i>	Standard service.	<i>dynamic</i>	Dynamic service.					
Option	Description													
<i>auto</i>	auto													
<i>standard</i>	Standard service.													
<i>dynamic</i>	Dynamic service.													
primary-hash	Hash method.	option	-	dst-ip										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>src-ip</i></td><td>Source IP hash.</td></tr><tr><td><i>dst-ip</i></td><td>Destination IP hash.</td></tr><tr><td><i>src-port</i></td><td>Source port hash.</td></tr><tr><td><i>dst-port</i></td><td>Destination port hash.</td></tr></table>	Option	Description	<i>src-ip</i>	Source IP hash.	<i>dst-ip</i>	Destination IP hash.	<i>src-port</i>	Source port hash.	<i>dst-port</i>	Destination port hash.			
Option	Description													
<i>src-ip</i>	Source IP hash.													
<i>dst-ip</i>	Destination IP hash.													
<i>src-port</i>	Source port hash.													
<i>dst-port</i>	Destination port hash.													
priority	Service priority.	integer	Minimum value: 0 Maximum value: 255	0										
protocol	Service protocol.	integer	Minimum value: 0 Maximum value: 255	0										
assignment-weight	Assignment of hash weight/ratio for the WCCP cache engine.	integer	Minimum value: 0 Maximum value: 255	0										
assignment-bucket-format	Assignment bucket format for the WCCP cache engine.	option	-	cisco-implementation										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>wccp-v2</i></td><td>WCCP-v2 bucket format.</td></tr><tr><td><i>cisco-implementation</i></td><td>Cisco bucket format.</td></tr></table>	Option	Description	<i>wccp-v2</i>	WCCP-v2 bucket format.	<i>cisco-implementation</i>	Cisco bucket format.							
Option	Description													
<i>wccp-v2</i>	WCCP-v2 bucket format.													
<i>cisco-implementation</i>	Cisco bucket format.													
return-method	Method used to decline a redirected packet and return it to the FortiProxy unit.	option	-	GRE										

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>GRE</i></td><td>GRE encapsulation.</td></tr><tr><td><i>L2</i></td><td>L2 rewrite.</td></tr><tr><td><i>any</i></td><td>GRE or L2.</td></tr></table>	Option	Description	<i>GRE</i>	GRE encapsulation.	<i>L2</i>	L2 rewrite.	<i>any</i>	GRE or L2.			
	Option	Description										
	<i>GRE</i>	GRE encapsulation.										
	<i>L2</i>	L2 rewrite.										
	<i>any</i>	GRE or L2.										
assignment-method	Hash key assignment preference.	option	-	HASH								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>HASH</i></td><td>HASH assignment method.</td></tr><tr><td><i>MASK</i></td><td>MASK assignment method.</td></tr><tr><td><i>any</i></td><td>HASH or MASK.</td></tr></table>	Option	Description	<i>HASH</i>	HASH assignment method.	<i>MASK</i>	MASK assignment method.	<i>any</i>	HASH or MASK.			
	Option	Description										
	<i>HASH</i>	HASH assignment method.										
	<i>MASK</i>	MASK assignment method.										
	<i>any</i>	HASH or MASK.										
assignment-srcaddr-mask	Assignment source address mask.	ipv4-netmask-any	Not Specified	0.0.23.65								
assignment-dstaddr-mask	Assignment destination address mask.	ipv4-netmask-any	Not Specified	0.0.0.0								

config system zone

Configure zones to group two or more interfaces. When a zone is created you can configure policies for the zone instead of individual interfaces in the zone.

```

config system zone
    Description: Configure zones to group two or more interfaces. When a zone is created you
    can configure policies for the zone instead of individual interfaces in the zone.
    edit <name>
        config tagging
            Description: Config object tagging.
            edit <name>
                set category {string}
                set tags <name1>, <name2>, ...
            next
        end
        set description {string}
        set interface <interface-name1>, <interface-name2>, ...
    next
end

```

config system zone

Parameter	Description	Type	Size	Default
name	Zone name.	string	Maximum length: 35	
description	Description.	string	Maximum length: 127	
interface <interface-name>	Add interfaces to this zone. Interfaces must not be assigned to another zone or have firewall policies defined. Select interfaces to add to the zone.	string	Maximum length: 79	

config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

test

This section includes syntax for the following commands:

- [config test acd on page 978](#)
- [config test acsd on page 979](#)
- [config test autod on page 979](#)
- [config test awsd on page 980](#)
- [config test azd on page 980](#)
- [config test bfd on page 980](#)
- [config test csfd on page 981](#)
- [config test ddnsd on page 981](#)
- [config test dhcp6c on page 981](#)
- [config test dhcp6r on page 982](#)
- [config test dhcprelay on page 982](#)
- [config test dlpfingerprint on page 983](#)
- [config test dlpfpcache on page 983](#)
- [config test dnsproxy on page 983](#)
- [config test dsd on page 984](#)
- [config test eap_supp on page 984](#)
- [config test fas on page 984](#)
- [config test fcnacd on page 985](#)
- [config test fds_notify on page 985](#)
- [config test fgtlogd on page 986](#)
- [config test fnbamd on page 986](#)
- [config test forticldd on page 986](#)
- [config test forticron on page 987](#)
- [config test fsd on page 987](#)
- [config test fsvrd on page 987](#)
- [config test gcpd on page 988](#)
- [config test harelay on page 988](#)
- [config test hasync on page 989](#)
- [config test hataalk on page 989](#)
- [config test ibmd on page 989](#)
- [config test imap on page 990](#)
- [config test init on page 990](#)
- [config test iotd on page 990](#)
- [config test ipamd on page 991](#)
- [config test ipamsd on page 991](#)
- [config test ipldbd on page 992](#)
- [config test ipsengine on page 992](#)

- [config test ipsmonitor on page 992](#)
- [config test ipsufd on page 993](#)
- [config test kubed on page 993](#)
- [config test l2tpcd on page 993](#)
- [config test lnkmttd on page 994](#)
- [config test locallogd on page 994](#)
- [config test miglogd on page 995](#)
- [config test mrd on page 995](#)
- [config test netxd on page 995](#)
- [config test nntp on page 996](#)
- [config test ocid on page 996](#)
- [config test openstackd on page 996](#)
- [config test ovrd on page 997](#)
- [config test pop3 on page 997](#)
- [config test pptpcd on page 998](#)
- [config test quarantined on page 998](#)
- [config test radius-das on page 998](#)
- [config test radiusd on page 999](#)
- [config test radvd on page 999](#)
- [config test reportd on page 999](#)
- [config test rt_router on page 1000](#)
- [config test sdncd on page 1000](#)
- [config test sdnd on page 1001](#)
- [config test sepmd on page 1001](#)
- [config test sessionsync on page 1001](#)
- [config test sfupgraded on page 1002](#)
- [config test smtp on page 1002](#)
- [config test snmpd on page 1002](#)
- [config test syslogd on page 1003](#)
- [config test updated on page 1003](#)
- [config test uploadd on page 1004](#)
- [config test urlfilter on page 1004](#)
- [config test vned on page 1004](#)
- [config test wad on page 1005](#)
- [config test wccpd on page 1005](#)
- [config test wf_monitor on page 1005](#)
- [config test wiredapd on page 1006](#)

config test acd

Aggregate Controller.

```
config test acd
    Description: Aggregate Controller.
    set <Integer> {string}
end
```

config test acd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test acsd

Ali Cloud Service daemon.

```
config test acsd
    Description: Ali Cloud Service daemon.
    set <Integer> {string}
end
```

config test acsd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test autod

Automation daemon.

```
config test autod
    Description: Automation daemon.
    set <Integer> {string}
end
```

config test autod

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test awsd

Amazon Web Services (AWS) daemon.

```
config test awsd
    Description: Amazon Web Services (AWS) daemon.
    set <Integer> {string}
end
```

config test awsd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test azd

Microsoft Azure daemon.

```
config test azd
    Description: Microsoft Azure daemon.
    set <Integer> {string}
end
```

config test azd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test bfd

BFD daemon.

```
config test bfd
    Description: BFD daemon.
    set <Integer> {string}
end
```

config test bfd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test csfd

Security Fabric daemon.

```
config test csfd
  Description: Security Fabric daemon.
  set <Integer> {string}
end
```

config test csfd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test ddnsd

DDNS client daemon.

```
config test ddnsd
  Description: DDNS client daemon.
  set <Integer> {string}
end
```

config test ddnsd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test dhcp6c

DHCP6 client daemon.

```
config test dhcp6c
    Description: DHCP6 client daemon.
    set <Integer> {string}
end
```

config test dhcp6c

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test dhcp6r

DHCP6 relay daemon.

```
config test dhcp6r
    Description: DHCP6 relay daemon.
    set <Integer> {string}
end
```

config test dhcp6r

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test dhcprelay

DHCP relay daemon.

```
config test dhcprelay
    Description: DHCP relay daemon.
    set <Integer> {string}
end
```

config test dhcprelay

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test dlpfingerprint

DLP fingerprint daemon.

```
config test dlpfingerprint
    Description: DLP fingerprint daemon.
    set <Integer> {string}
end
```

config test dlpfingerprint

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test dlpfpcache

DLP fingerprint cache daemon.

```
config test dlpfpcache
    Description: DLP fingerprint cache daemon.
    set <Integer> {string}
end
```

config test dlpfpcache

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test dnsproxy

DNS proxy.

```
config test dnsproxy
    Description: DNS proxy.
    set <Integer> {string}
end
```

config test dnspoxy

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test dsd

DLP Statistics daemon.

```
config test dsd
    Description: DLP Statistics daemon.
    set <Integer> {string}
end
```

config test dsd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test eap_supp

EAP Supplicant daemon.

```
config test eap_supp
    Description: EAP Supplicant daemon.
    set <Integer> {string}
end
```

config test eap_supp

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test fas

FortiToken Cloud daemon.


```
config test fas
  Description: FortiToken Cloud daemon.
  set <Integer> {string}
end
```

config test fas

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test fcnacd

FortiClient NAC daemon.

```
config test fcnacd
  Description: FortiClient NAC daemon.
  set <Integer> {string}
end
```

config test fcnacd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test fds_notify

Update Notification daemon.

```
config test fds_notify
  Description: Update Notification daemon.
  set <Integer> {string}
end
```

config test fds_notify

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test fgtlogd

Fgtlog daemon.

```
config test fgtlogd
    Description: Fgtlog daemon.
    set <Integer> {string}
end
```

config test fgtlogd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test fnbamd

Fortiproxy non-blocking auth daemon.

```
config test fnbamd
    Description: Fortiproxy non-blocking auth daemon.
    set <Integer> {string}
end
```

config test fnbamd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test forticldd

FortiCloud daemon.

```
config test forticldd
    Description: FortiCloud daemon.
    set <Integer> {string}
end
```

config test forticldd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test forticron

Forticron daemon.

```
config test forticron
  Description: Forticron daemon.
  set <Integer> {string}
end
```

config test forticron

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test fsd

FortiExplorer daemon.

```
config test fsd
  Description: FortiExplorer daemon.
  set <Integer> {string}
end
```

config test fsd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test fsvrd

FortiService daemon.

```
config test fsvr
  Description: FortiService daemon.
  set <Integer> {string}
end
```

config test fsvr

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test gcpd

Google Cloud Platform (GCP) daemon.

```
config test gcpd
  Description: Google Cloud Platform (GCP) daemon.
  set <Integer> {string}
end
```

config test gcpd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test harelay

HA relay daemon.

```
config test harelay
  Description: HA relay daemon.
  set <Integer> {string}
end
```

config test harelay

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test hasync

HA sync daemon.

```
config test hasync
    Description: HA sync daemon.
    set <Integer> {string}
end
```

config test hasync

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test hatalk

HA talk daemon.

```
config test hatalk
    Description: HA talk daemon.
    set <Integer> {string}
end
```

config test hatalk

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test ibmd

IBM Cloud Infrastructure daemon.

```
config test ibmd
    Description: IBM Cloud Infrastructure daemon.
    set <Integer> {string}
end
```

config test ibmd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test imap

IMAP proxy.

```
config test imap
    Description: IMAP proxy.
    set <Integer> {string}
end
```

config test imap

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test init

init process.

```
config test init
    Description: init process.
    set <Integer> {string}
end
```

config test init

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test iotd

IoT device info daemon.

```
config test iotd
    Description: IoT device info daemon.
    set <Integer> {string}
end
```

config test iotd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test ipamd

IP Address Management daemon.

```
config test ipamd
    Description: IP Address Management daemon.
    set <Integer> {string}
end
```

config test ipamd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test ipamsd

IPAM server daemon.

```
config test ipamsd
    Description: IPAM server daemon.
    set <Integer> {string}
end
```

config test ipamsd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test ipldbd

IP load balancing daemon.

```
config test ipldbd
    Description: IP load balancing daemon.
    set <Integer> {string}
end
```

config test ipldbd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test ipsengine

IPS sensor.

```
config test ipsengine
    Description: IPS sensor.
    set <Integer> {string}
end
```

config test ipsengine

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test ipsmonitor

IPS monitor.

```
config test ipsmonitor
    Description: IPS monitor.
    set <Integer> {string}
end
```


config test ipsmonitor

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test ipsufd

IPS urlfilter daemon.

```
config test ipsufd
    Description: IPS urlfilter daemon.
    set <Integer> {string}
end
```

config test ipsufd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test kubed

Kubernetes daemon.

```
config test kubed
    Description: Kubernetes daemon.
    set <Integer> {string}
end
```

config test kubed

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test l2tpcd

L2TP client daemon.

```
config test l2tpcd
    Description: L2TP client daemon.
    set <Integer> {string}
end
```

config test l2tpcd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test lnkmttd

Link monitor daemon.

```
config test lnkmttd
    Description: Link monitor daemon.
    set <Integer> {string}
end
```

config test lnkmttd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test locallogd

Locallogd daemon.

```
config test locallogd
    Description: Locallogd daemon.
    set <Integer> {string}
end
```

config test locallogd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test miglogd

Miglog logging daemon.

```
config test miglogd
    Description: Miglog logging daemon.
    set <Integer> {string}
end
```

config test miglogd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test mrd

Mobile router daemon.

```
config test mrd
    Description: Mobile router daemon.
    set <Integer> {string}
end
```

config test mrd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test netxd

VMWare NetX service manager daemon.

```
config test netxd
    Description: VMWare NetX service manager daemon.
    set <Integer> {string}
end
```

config test netxd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test nntp

NNTP proxy.

```
config test nntp
    Description: NNTP proxy.
    set <Integer> {string}
end
```

config test nntp

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test ocid

Oracle Cloud Infrastructure.

```
config test ocid
    Description: Oracle Cloud Infrastructure.
    set <Integer> {string}
end
```

config test ocid

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test openstackd

OpenStack SDN connector daemon.

```
config test openstackd
    Description: OpenStack SDN connector daemon.
    set <Integer> {string}
end
```

config test openstackd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test ovrd

Override daemon.

```
config test ovrd
    Description: Override daemon.
    set <Integer> {string}
end
```

config test ovrd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test pop3

POP3 proxy.

```
config test pop3
    Description: POP3 proxy.
    set <Integer> {string}
end
```

config test pop3

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test pptpcd

PPTP client.

```
config test pptpcd
    Description: PPTP client.
    set <Integer> {string}
end
```

config test pptpcd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test quarantined

Quarantine daemon.

```
config test quarantined
    Description: Quarantine daemon.
    set <Integer> {string}
end
```

config test quarantined

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test radius-das

Radius-das daemon.

```
config test radius-das
    Description: Radius-das daemon.
    set <Integer> {string}
end
```

config test radius-das

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test radiusd

RADIUS daemon.

```
config test radiusd
  Description: RADIUS daemon.
  set <Integer> {string}
end
```

config test radiusd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test radvd

radvd daemon.

```
config test radvd
  Description: radvd daemon.
  set <Integer> {string}
end
```

config test radvd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test reportd

Report daemon.

```
config test reportd
    Description: Report daemon.
    set <Integer> {string}
end
```

config test reportd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test rt_router

```
Router daemon
config test rt_router
    Description: Router daemon
    set <Integer> {string}
end
```

config test rt_router

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test sdncd

```
SDN Connector daemon.
config test sdncd
    Description: SDN Connector daemon.
    set <Integer> {string}
end
```

config test sdncd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test sdnd

SDN connector daemon.

```
config test sdnd
    Description: SDN connector daemon.
    set <Integer> {string}
end
```

config test sdnd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test sepmd

Symantec Endpoint Protection Manager daemon.

```
config test sepmd
    Description: Symantec Endpoint Protection Manager daemon.
    set <Integer> {string}
end
```

config test sepmd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test sessionsync

Session sync daemon.

```
config test sessionsync
    Description: Session sync daemon.
    set <Integer> {string}
end
```

config test sessionsync

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test sfupgraded

Security Fabric Upgrade daemon.

```
config test sfupgraded
  Description: Security Fabric Upgrade daemon.
  set <Integer> {string}
end
```

config test sfupgraded

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test smtp

SMTP proxy.

```
config test smtp
  Description: SMTP proxy.
  set <Integer> {string}
end
```

config test smtp

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test snmpd

SNMP daemon.

```
config test snmpd
    Description: SNMP daemon.
    set <Integer> {string}
end
```

config test snmpd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test syslogd

Syslog daemon.

```
config test syslogd
    Description: Syslog daemon.
    set <Integer> {string}
end
```

config test syslogd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test updated

Update daemon.

```
config test updated
    Description: Update daemon.
    set <Integer> {string}
end
```

config test updated

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test uploadd

Upload daemon.

```
config test uploadd
  Description: Upload daemon.
  set <Integer> {string}
end
```

config test uploadd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test urlfilter

URL filter daemon.

```
config test urlfilter
  Description: URL filter daemon.
  set <Integer> {string}
end
```

config test urlfilter

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test vned

Virtual network enabler daemon.

```
config test vned
  Description: Virtual network enabler daemon.
  set <Integer> {string}
end
```

config test vned

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test wad

WAD related processes.

```
config test wad
    Description: WAD related processes.
    set <Integer> {string}
end
```

config test wad

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test wccpd

WCCP daemon.

```
config test wccpd
    Description: WCCP daemon.
    set <Integer> {string}
end
```

config test wccpd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test wf_monitor

WF monitor.

```
config test wf_monitor
  Description: WF monitor.
  set <Integer> {string}
end
```

config test wf_monitor

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

config test wiredapd

Wiredapd daemon.

```
config test wiredapd
  Description: Wiredapd daemon.
  set <Integer> {string}
end
```

config test wiredapd

Parameter	Description	Type	Size	Default
<Integer>	Test level.	string	Maximum length: -	

user

This section includes syntax for the following commands:

- [config user adgrp on page 1007](#)
- [config user certificate on page 1008](#)
- [config user domain-controller on page 1009](#)
- [config user exchange on page 1013](#)
- [config user external-identity-provider on page 1015](#)
- [config user fortitoken on page 1017](#)
- [config user fsso-polling on page 1018](#)
- [config user fsso on page 1020](#)
- [config user group on page 1024](#)
- [config user krb-keytab on page 1029](#)
- [config user ldap on page 1030](#)
- [config user local on page 1037](#)
- [config user password-policy on page 1041](#)
- [config user peer on page 1042](#)
- [config user peergrp on page 1044](#)
- [config user pop3 on page 1044](#)
- [config user radius on page 1045](#)
- [config user saml on page 1058](#)
- [config user security-exempt-list on page 1062](#)
- [config user setting on page 1063](#)
- [config user tacacs+ on page 1067](#)

config user adgrp

Configure FSSO groups.

```
config user adgrp
    Description: Configure FSSO groups.
    edit <name>
        set server-name {string}
        set connector-source {string}
        set id {integer}
    next
end
```

config user adgrp

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 511	
server-name	FSSO agent name.	string	Maximum length: 35	
connector-source	FSSO connector source.	string	Maximum length: 35	
id	Group ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config user certificate

Configure certificate users.

```
config user certificate
  Description: Configure certificate users.
  edit <name>
    set id {integer}
    set status [enable|disable]
    set type [single-certificate|trusted-issuer]
    set common-name {string}
    set issuer {string}
  next
end
```

config user certificate

Parameter	Description	Type	Size	Default
name	User name.	string	Maximum length: 64	
id	User ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Enable/disable allowing the certificate user to authenticate with the FortiGate unit.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable user.		
	<i>disable</i>	Disable user.		
type	Type of certificate authentication method.	option	-	single-certificate
	Option	Description		
	<i>single-certificate</i>	Single certificate.		
	<i>trusted-issuer</i>	Trusted CA issuer.		
common-name	Certificate common name.	string	Maximum length: 64	
issuer	CA certificate used for client certificate verification.	string	Maximum length: 79	

config user domain-controller

Configure domain controller entries.

```
config user domain-controller
    Description: Configure domain controller entries.
    edit <name>
        set ad-mode [none|ds|...]
        set hostname {string}
        set username {string}
        set password {password}
        set ip-address {ipv4-address}
        set ip6 {ipv6-address}
        set port {integer}
        set source-ip-address {ipv4-address}
        set source-ip6 {ipv6-address}
        set source-port {integer}
        set interface-select-method [auto|specify]
        set interface {string}
    config extra-server
        Description: Extra servers.
        edit <id>
            set ip-address {ipv4-address}
            set port {integer}
            set source-ip-address {ipv4-address}
            set source-port {integer}
        next
    end
    set domain-name {string}
    set domain-name-src [server|client]
```

```

    set replication-port {integer}
    set ldap-server <name1>, <name2>, ...
    set change-detection [enable|disable]
    set change-detection-period {integer}
    set dns-srv-lookup [enable|disable]
    set adlds-dn {string}
    set adlds-ip-address {ipv4-address}
    set adlds-ip6 {ipv6-address}
    set adlds-port {integer}
next
end

```

config user domain-controller

Parameter	Description	Type	Size	Default								
name	Domain controller entry name.	string	Maximum length: 35									
ad-mode	Set Active Directory mode.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>The server is not configured as an Active Directory Domain Server (AD DS).</td></tr><tr><td><i>ds</i></td><td>The server is configured as an Active Directory Domain Server (AD DS).</td></tr><tr><td><i>lds</i></td><td>The server is an Active Directory Lightweight Domain Server (AD LDS).</td></tr></table>				Option	Description	<i>none</i>	The server is not configured as an Active Directory Domain Server (AD DS).	<i>ds</i>	The server is configured as an Active Directory Domain Server (AD DS).	<i>lds</i>	The server is an Active Directory Lightweight Domain Server (AD LDS).
	Option	Description										
	<i>none</i>	The server is not configured as an Active Directory Domain Server (AD DS).										
	<i>ds</i>	The server is configured as an Active Directory Domain Server (AD DS).										
<i>lds</i>	The server is an Active Directory Lightweight Domain Server (AD LDS).											
hostname	Hostname of the server to connect to.	string	Maximum length: 255									
username	User name to sign in with. Must have proper permissions for service.	string	Maximum length: 64									
password	Password for specified username.	password	Not Specified									
ip-address	Domain controller IPv4 address.	ipv4-address	Not Specified	0.0.0.0								
ip6	Domain controller IPv6 address.	ipv6-address	Not Specified	::								
port	Port to be used for communication with the domain controller.	integer	Minimum value: 0 Maximum value: 65535	445								
source-ip-address	FortiProxy IPv4 address to be used for communication with the domain controller.	ipv4-address	Not Specified	0.0.0.0								
source-ip6	FortiProxy IPv6 address to be used for communication with the domain controller.	ipv6-address	Not Specified	::								

Parameter	Description	Type	Size	Default						
source-port	Source port to be used for communication with the domain controller.	integer	Minimum value: 0 Maximum value: 65535	0						
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.			
Option	Description									
<i>auto</i>	Set outgoing interface automatically.									
<i>specify</i>	Set outgoing interface manually.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							
domain-name	Domain DNS name.	string	Maximum length: 255							
domain-name-src	Select where to extract domain name.	option	-	client						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>server</i></td><td>Extract domain name from server's (Domain Controller) data.</td></tr><tr><td><i>client</i></td><td>Extract domain name from client's data.</td></tr></table>	Option	Description	<i>server</i>	Extract domain name from server's (Domain Controller) data.	<i>client</i>	Extract domain name from client's data.			
Option	Description									
<i>server</i>	Extract domain name from server's (Domain Controller) data.									
<i>client</i>	Extract domain name from client's data.									
replication-port	Port to be used for communication with the domain controller for replication service. Port number 0 indicates automatic discovery.	integer	Minimum value: 0 Maximum value: 65535	0						
ldap-server <name>	LDAP server name(s). LDAP server name.	string	Maximum length: 79							
change-detection	Enable/disable detection of a configuration change in the Active Directory server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable detection of a configuration change in the Active Directory server.</td></tr><tr><td><i>disable</i></td><td>Disable detection of a configuration change in the Active Directory server.</td></tr></table>	Option	Description	<i>enable</i>	Enable detection of a configuration change in the Active Directory server.	<i>disable</i>	Disable detection of a configuration change in the Active Directory server.			
Option	Description									
<i>enable</i>	Enable detection of a configuration change in the Active Directory server.									
<i>disable</i>	Disable detection of a configuration change in the Active Directory server.									

Parameter	Description	Type	Size	Default
change-detection-period	Minutes to detect a configuration change in the Active Directory server.	integer	Minimum value: 5 Maximum value: 10080	60
dns-srv-lookup	Enable/disable DNS service lookup.	option	-	disable
	Option	Description		
	enable	Enable DNS service lookup.		
	disable	Disable DNS service lookup.		
adlds-dn	AD LDS distinguished name.	string	Maximum length: 255	
adlds-ip-address	AD LDS IPv4 address.	ipv4-address	Not Specified	0.0.0.0
adlds-ip6	AD LDS IPv6 address.	ipv6-address	Not Specified	::
adlds-port	Port number of AD LDS service.	integer	Minimum value: 0 Maximum value: 65535	389

config extra-server

Parameter	Description	Type	Size	Default
id	Server ID.	integer	Minimum value: 1 Maximum value: 100	0
ip-address	Domain controller IP address.	ipv4-address	Not Specified	0.0.0.0
port	Port to be used for communication with the domain controller.	integer	Minimum value: 0 Maximum value: 65535	445
source-ip-address	FortiProxy IPv4 address to be used for communication with the domain controller.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
source-port	Source port to be used for communication with the domain controller.	integer	Minimum value: 0 Maximum value: 65535	0

config user exchange

Configure MS Exchange server entries.

```
config user exchange
    Description: Configure MS Exchange server entries.
    edit <name>
        set server-name {string}
        set domain-name {string}
        set username {string}
        set password {password}
        set ip {ipv4-address-any}
        set connect-protocol [rpc-over-tcp|rpc-over-http|...]
        set auth-type [spnego|ntlm|...]
        set auth-level [connect|call|...]
        set http-auth-type [basic|ntlm]
        set ssl-min-proto-version [default|SSLv3|...]
        set auto-discover-kdc [enable|disable]
        set kdc-ip <ipv41>, <ipv42>, ...
    next
end
```

config user exchange

Parameter	Description	Type	Size	Default
name	MS Exchange server entry name.	string	Maximum length: 35	
server-name	MS Exchange server hostname.	string	Maximum length: 63	
domain-name	MS Exchange server fully qualified domain name.	string	Maximum length: 79	
username	User name used to sign in to the server. Must have proper permissions for service.	string	Maximum length: 64	
password	Password for the specified username.	password	Not Specified	

Parameter	Description	Type	Size	Default
ip	Server IPv4 address.	ipv4-address-any	Not Specified	0.0.0.0
connect-protocol	Connection protocol used to connect to MS Exchange service.	option	-	rpc-over-https
	Option		Description	
	rpc-over-tcp	Connect using RPC-over-TCP. Use for MS Exchange 2010 and earlier versions. Supported in MS Exchange 2013.		
	rpc-over-http	Connect using RPC-over-HTTP. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.		
	rpc-over-https	Connect using RPC-over-HTTPS. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.		
auth-type	Authentication security type used for the RPC protocol layer.	option	-	kerberos
	Option		Description	
	spnego	Negotiate authentication.		
	ntlm	NTLM authentication.		
	kerberos	Kerberos authentication.		
auth-level	Authentication security level used for the RPC protocol layer.	option	-	privacy
	Option		Description	
	connect	RPC authentication level 'connect'.		
	call	RPC authentication level 'call'.		
	packet	RPC authentication level 'packet'.		
	integrity	RPC authentication level 'integrity'.		
	privacy	RPC authentication level 'privacy'.		
http-auth-type	Authentication security type used for the HTTP transport.	option	-	ntlm
	Option		Description	
	basic	Basic HTTP authentication.		
	ntlm	NTLM HTTP authentication.		

Parameter	Description	Type	Size	Default
ssl-min-protocol-version	Minimum SSL/TLS protocol version for HTTPS transport.	option	-	default
	Option	Description		
	<i>default</i>	Follow system global setting.		
	<i>SSLv3</i>	SSLv3.		
	<i>TLSv1</i>	TLSv1.		
	<i>TLSv1-1</i>	TLSv1.1.		
	<i>TLSv1-2</i>	TLSv1.2.		
auto-discover-kdc	Enable/disable automatic discovery of KDC IP addresses.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable automatic discovery of KDC IP addresses.		
	<i>disable</i>	Disable automatic discovery of KDC IP addresses.		
kdc-ip <ipv4>	KDC IPv4 addresses for Kerberos authentication. KDC IPv4 addresses for Kerberos authentication.	string	Maximum length: 79	

config user external-identity-provider

Configure external identity provider.

```

config user external-identity-provider
    Description: Configure external identity provider.
    edit <name>
        set type {option}
        set version [v1.0|beta]
        set url {string}
        set user-attr-name {string}
        set group-attr-name {string}
        set port {integer}
        set source-ip {string}
        set interface-select-method [auto|specify]
        set interface {string}
        set server-identity-check [disable|enable]
        set timeout {integer}
    next
end

```

config user external-identity-provider

Parameter	Description	Type	Size	Default						
name	External identity provider name.	string	Maximum length: 35							
type	External identity provider type.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ms-graph</i></td><td>Microsoft Graph server.</td></tr></table>	Option	Description	<i>ms-graph</i>	Microsoft Graph server.					
Option	Description									
<i>ms-graph</i>	Microsoft Graph server.									
version	External identity API version.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>v1.0</i></td><td>MS Graph REST API v1.0.</td></tr><tr><td><i>beta</i></td><td>MS Graph REST API beta (debug build only).</td></tr></table>	Option	Description	<i>v1.0</i>	MS Graph REST API v1.0.	<i>beta</i>	MS Graph REST API beta (debug build only).			
Option	Description									
<i>v1.0</i>	MS Graph REST API v1.0.									
<i>beta</i>	MS Graph REST API beta (debug build only).									
url	External identity provider URL (e.g. "https://example.com:8080/api/v1").	string	Maximum length: 127							
user-attr-name	User attribute name in authentication query.	string	Maximum length: 63	userPrincipalName						
group-attr-name	Group attribute name in authentication query.	string	Maximum length: 63	id						
port	External identity provider service port number.	integer	Minimum value: 0 Maximum value: 65535	0						
source-ip	Use this IPv4/v6 address to connect to the external identity provider.	string	Maximum length: 63							
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.			
Option	Description									
<i>auto</i>	Set outgoing interface automatically.									
<i>specify</i>	Set outgoing interface manually.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							
server-identity-check	Enable/disable server's identity check against its certificate and subject alternative name(s).	option	-	enable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Do not check server's identity against its certificate and subject alternative name(s).		
	<i>enable</i>	Check server's identity against its certificate and subject alternative name(s).		
timeout	Connection timeout value in seconds.	integer	Minimum value: 1 Maximum value: 60	5

config user fortitoken

Configure FortiToken.

```
config user fortitoken
  Description: Configure FortiToken.
  edit <serial-number>
    set status [active|lock]
    set comments {var-string}
    set license {string}
    set activation-code {string}
    set activation-expire {integer}
    set reg-id {string}
    set os-ver {string}
  next
end
```

config user fortitoken

Parameter	Description	Type	Size	Default
serial-number	Serial number.	string	Maximum length: 16	
status	Status.	option	-	active
	Option	Description		
	<i>active</i>	Activate FortiToken.		
	<i>lock</i>	Lock FortiToken.		
comments	Comment.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default
license	Mobile token license.	string	Maximum length: 31	
activation-code	Mobile token user activation-code.	string	Maximum length: 32	
activation-expire	Mobile token user activation-code expire time.	integer	Minimum value: 0 Maximum value: 4294967295	0
reg-id	Device Reg ID.	string	Maximum length: 256	
os-ver	Device Mobile Version.	string	Maximum length: 15	

config user fsso-polling

Configure FSSO active directory servers for polling mode.

```

config user fsso-polling
    Description: Configure FSSO active directory servers for polling mode.
    edit <id>
        set status [enable|disable]
        set server {string}
        set default-domain {string}
        set port {integer}
        set user {string}
        set password {password}
        set ldap-server {string}
        set logon-history {integer}
        set polling-frequency {integer}
        config adgrp
            Description: LDAP Group Info.
            edit <name>
                next
            end
        set smbvl [enable|disable]
        set smb-ntlmv1-auth [enable|disable]
    next
end

```

config user fsso-polling

Parameter	Description	Type	Size	Default
id	Active Directory server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Enable/disable polling for the status of this Active Directory server.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
server	Host name or IP address of the Active Directory server.	string	Maximum length: 63	
default-domain	Default domain managed by this Active Directory server.	string	Maximum length: 35	
port	Port to communicate with this Active Directory server.	integer	Minimum value: 0 Maximum value: 65535	0
user	User name required to log into this Active Directory server.	string	Maximum length: 35	
password	Password required to log into this Active Directory server.	password	Not Specified	
ldap-server	LDAP server name used in LDAP connection strings.	string	Maximum length: 35	
logon-history	Number of hours of logon history to keep, 0 means keep all history.	integer	Minimum value: 0 Maximum value: 48	8
polling-frequency	Polling frequency (every 1 to 30 seconds).	integer	Minimum value: 1 Maximum value: 30	10
smbv1	Enable/disable support of SMBv1 for Samba.	option	-	disable
	Option	Description		
	enable	Enable support of SMBv1 for Samba.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable support of SMBv1 for Samba.		
smb-ntlmv1-auth	Enable/disable support of NTLMv1 for Samba authentication.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable support of NTLMv1 for Samba authentication.		
	<i>disable</i>	Disable support of NTLMv1 for Samba authentication.		

config adgrp

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 511	

config user fsso

Configure Fortinet Single Sign On (FSSO) agents.

```
config user fsso
  Description: Configure Fortinet Single Sign On (FSSO) agents.
  edit <name>
    set type [default|fortinac]
    set server {string}
    set port {integer}
    set password {password}
    set server2 {string}
    set port2 {integer}
    set password2 {password}
    set server3 {string}
    set port3 {integer}
    set password3 {password}
    set server4 {string}
    set port4 {integer}
    set password4 {password}
    set server5 {string}
    set port5 {integer}
    set password5 {password}
    set logon-timeout {integer}
    set ldap-server {string}
    set group-poll-interval {integer}
    set ldap-poll [enable|disable]
    set ldap-poll-interval {integer}
```

```

        set ldap-poll-filter {string}
        set user-info-server {string}
        set ssl [enable|disable]
        set sni {string}
        set ssl-server-host-ip-check [enable|disable]
        set ssl-trusted-cert {string}
        set source-ip {ipv4-address}
        set source-ip6 {ipv6-address}
        set interface-select-method [auto|specify]
        set interface {string}
    next
end

```

config user fssso

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
type	Server type.	option	-	default
	Option	Description		
	default	All other unspecified types of servers.		
	fortinac	FortiNAC server.		
server	Domain name or IP address of the first FSSO collector agent.	string	Maximum length: 63	
port	Port of the first FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
password	Password of the first FSSO collector agent.	password	Not Specified	
server2	Domain name or IP address of the second FSSO collector agent.	string	Maximum length: 63	
port2	Port of the second FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
password2	Password of the second FSSO collector agent.	password	Not Specified	
server3	Domain name or IP address of the third FSSO collector agent.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
port3	Port of the third FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
password3	Password of the third FSSO collector agent.	password	Not Specified	
server4	Domain name or IP address of the fourth FSSO collector agent.	string	Maximum length: 63	
port4	Port of the fourth FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
password4	Password of the fourth FSSO collector agent.	password	Not Specified	
server5	Domain name or IP address of the fifth FSSO collector agent.	string	Maximum length: 63	
port5	Port of the fifth FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
password5	Password of the fifth FSSO collector agent.	password	Not Specified	
logon-timeout	Interval in minutes to keep logons after FSSO server down.	integer	Minimum value: 1 Maximum value: 2880	5
ldap-server	LDAP server to get group information.	string	Maximum length: 35	
group-poll-interval	Interval in minutes within to fetch groups from FSSO server, or unset to disable.	integer	Minimum value: 1 Maximum value: 2880	0
ldap-poll	Enable/disable automatic fetching of groups from LDAP server.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable automatic fetching of groups from LDAP server.		
	<i>disable</i>	Disable automatic fetching of groups from LDAP server.		
ldap-poll-interval	Interval in minutes within to fetch groups from LDAP server.	integer	Minimum value: 1 Maximum value: 2880	180
ldap-poll-filter	Filter used to fetch groups.	string	Maximum length: 2047	(objectCategory=group)
user-info-server	LDAP server to get user information.	string	Maximum length: 35	
ssl	Enable/disable use of SSL.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable use of SSL.		
	<i>disable</i>	Disable use of SSL.		
sni	Server Name Indication.	string	Maximum length: 255	
ssl-server-host-ip-check	Enable/disable server host/IP verification.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable server host/IP verification.		
	<i>disable</i>	Disable server host/IP verification.		
ssl-trusted-cert	Trusted server certificate or CA certificate.	string	Maximum length: 79	
source-ip	Source IP for communications to FSSO agent.	ipv4-address	Not Specified	0.0.0.0
source-ip6	IPv6 source for communications to FSSO agent.	ipv6-address	Not Specified	::
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		

Parameter	Description	Type	Size	Default
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

config user group

Configure user groups.

```
config user group
  Description: Configure user groups.
  edit <name>
    set id {integer}
    set group-type [firewall|fsso-service|...]
    set authtimeout {integer}
    set auth-concurrent-override [enable|disable]
    set auth-concurrent-value {integer}
    set http-digest-realm {string}
    set sso-attribute-value {string}
    set logic-type [or|and]
    set member <name1>, <name2>, ...
  config match
    Description: Group matches.
    edit <id>
      set server-name {string}
      set group-name {string}
    next
  end
  set user-id [email|auto-generate|...]
  set password [auto-generate|specify|...]
  set user-name [disable|enable]
  set sponsor [optional|mandatory|...]
  set company [optional|mandatory|...]
  set email [disable|enable]
  set mobile-phone [disable|enable]
  set sms-server [fortiguard|custom]
  set sms-custom-server {string}
  set expire-type [immediately|first-successful-login]
  set expire {integer}
  set max-accounts {integer}
  set multiple-guest-add [disable|enable]
  config guest
    Description: Guest User.
    edit <id>
      set user-id {string}
      set name {string}
      set password {password}
      set mobile-phone {string}
      set sponsor {string}
      set company {string}
      set email {string}
      set expiration {user}
      set comment {var-string}
```



```

        next
    end
    next
end

```

config user group

Parameter	Description	Type	Size	Default										
name	Group name.	string	Maximum length: 35											
id	Group ID.	integer	Minimum value: 0 Maximum value: 4294967295	0										
group-type	Set the group to be for firewall authentication, FSSO, RSSO, or guest users.	option	-	firewall										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>firewall</td><td>Firewall.</td></tr><tr><td>fsso-service</td><td>Fortinet Single Sign-On Service.</td></tr><tr><td>rsso</td><td>RADIUS based Single Sign-On Service.</td></tr><tr><td>guest</td><td>Guest.</td></tr></table>				Option	Description	firewall	Firewall.	fsso-service	Fortinet Single Sign-On Service.	rsso	RADIUS based Single Sign-On Service.	guest	Guest.
	Option	Description												
	firewall	Firewall.												
	fsso-service	Fortinet Single Sign-On Service.												
	rsso	RADIUS based Single Sign-On Service.												
guest	Guest.													
authtimeout	Authentication timeout in minutes for this user group. 0 to use the global user setting auth-timeout.	integer	Minimum value: 0 Maximum value: 43200	0										
auth-concurrent-override	Enable/disable overriding the global number of concurrent authentication sessions for this user group.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable auth-concurrent-override.</td></tr><tr><td>disable</td><td>Disable auth-concurrent-override.</td></tr></table>				Option	Description	enable	Enable auth-concurrent-override.	disable	Disable auth-concurrent-override.				
	Option	Description												
	enable	Enable auth-concurrent-override.												
disable	Disable auth-concurrent-override.													
auth-concurrent-value	Maximum number of concurrent authenticated connections per user.	integer	Minimum value: 0 Maximum value: 100	0										
http-digest-realm	Realm attribute for MD5-digest authentication.	string	Maximum length: 35											

Parameter	Description	Type	Size	Default								
sso-attribute-value	Name of the RADIUS user group that this local user group represents.	string	Maximum length: 511									
logic-type	Set the logic between members or matching entries.	option	-	or								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>or</td><td>Logic OR between members or match entries.</td></tr><tr><td>and</td><td>Logic AND between members or match entries.</td></tr></table>	Option	Description	or	Logic OR between members or match entries.	and	Logic AND between members or match entries.					
Option	Description											
or	Logic OR between members or match entries.											
and	Logic AND between members or match entries.											
member <name>	Names of users, peers, LDAP servers, RADIUS servers or external idp servers to add to the user group. Group member name.	string	Maximum length: 511									
user-id	Guest user ID type.	option	-	email								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>email</td><td>Email address.</td></tr><tr><td>auto-generate</td><td>Automatically generate.</td></tr><tr><td>specify</td><td>Specify.</td></tr></table>	Option	Description	email	Email address.	auto-generate	Automatically generate.	specify	Specify.			
Option	Description											
email	Email address.											
auto-generate	Automatically generate.											
specify	Specify.											
password	Guest user password type.	option	-	auto-generate								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto-generate</td><td>Automatically generate.</td></tr><tr><td>specify</td><td>Specify.</td></tr><tr><td>disable</td><td>Disable.</td></tr></table>	Option	Description	auto-generate	Automatically generate.	specify	Specify.	disable	Disable.			
Option	Description											
auto-generate	Automatically generate.											
specify	Specify.											
disable	Disable.											
user-name	Enable/disable the guest user name entry.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable setting.</td></tr><tr><td>enable</td><td>Enable setting.</td></tr></table>	Option	Description	disable	Disable setting.	enable	Enable setting.					
Option	Description											
disable	Disable setting.											
enable	Enable setting.											
sponsor	Set the action for the sponsor guest user field.	option	-	optional								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>optional</td><td>Optional.</td></tr><tr><td>mandatory</td><td>Mandatory.</td></tr><tr><td>disabled</td><td>Disabled.</td></tr></table>	Option	Description	optional	Optional.	mandatory	Mandatory.	disabled	Disabled.			
Option	Description											
optional	Optional.											
mandatory	Mandatory.											
disabled	Disabled.											

Parameter	Description	Type	Size	Default								
company	Set the action for the company guest user field.	option	-	optional								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>optional</i></td><td>Optional.</td></tr><tr><td><i>mandatory</i></td><td>Mandatory.</td></tr><tr><td><i>disabled</i></td><td>Disabled.</td></tr></table>	Option	Description	<i>optional</i>	Optional.	<i>mandatory</i>	Mandatory.	<i>disabled</i>	Disabled.			
Option	Description											
<i>optional</i>	Optional.											
<i>mandatory</i>	Mandatory.											
<i>disabled</i>	Disabled.											
email	Enable/disable the guest user email address field.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr></table>	Option	Description	<i>disable</i>	Disable setting.	<i>enable</i>	Enable setting.					
Option	Description											
<i>disable</i>	Disable setting.											
<i>enable</i>	Enable setting.											
mobile-phone	Enable/disable the guest user mobile phone number field.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr></table>	Option	Description	<i>disable</i>	Disable setting.	<i>enable</i>	Enable setting.					
Option	Description											
<i>disable</i>	Disable setting.											
<i>enable</i>	Enable setting.											
sms-server	Send SMS through FortiGuard or other external server.	option	-	fortiguard								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortiguard</i></td><td>Send SMS by FortiGuard.</td></tr><tr><td><i>custom</i></td><td>Send SMS by custom server.</td></tr></table>	Option	Description	<i>fortiguard</i>	Send SMS by FortiGuard.	<i>custom</i>	Send SMS by custom server.					
Option	Description											
<i>fortiguard</i>	Send SMS by FortiGuard.											
<i>custom</i>	Send SMS by custom server.											
sms-custom-server	SMS server.	string	Maximum length: 35									
expire-type	Determine when the expiration countdown begins.	option	-	immediately								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>immediately</i></td><td>Immediately.</td></tr><tr><td><i>first-successful-login</i></td><td>First successful login.</td></tr></table>	Option	Description	<i>immediately</i>	Immediately.	<i>first-successful-login</i>	First successful login.					
Option	Description											
<i>immediately</i>	Immediately.											
<i>first-successful-login</i>	First successful login.											
expire	Time in seconds before guest user accounts expire.	integer	Minimum value: 1 Maximum value: 31536000	14400								

Parameter	Description	Type	Size	Default
max-accounts	Maximum number of guest accounts that can be created for this group (0 means unlimited).	integer	Minimum value: 0 Maximum value: 1024	0
multiple-guest-add	Enable/disable addition of multiple guests.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable setting.		
	<i>enable</i>	Enable setting.		

config match

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
server-name	Name of remote auth server.	string	Maximum length: 35	
group-name	Name of matching user or group on remote authentication server.	string	Maximum length: 511	

config guest

Parameter	Description	Type	Size	Default
id	Guest ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
user-id	Guest ID.	string	Maximum length: 64	
name	Guest name.	string	Maximum length: 64	
password	Guest password.	password	Not Specified	

Parameter	Description	Type	Size	Default
mobile-phone	Mobile phone.	string	Maximum length: 35	
sponsor	Set the action for the sponsor guest user field.	string	Maximum length: 35	
company	Set the action for the company guest user field.	string	Maximum length: 35	
email	Email.	string	Maximum length: 64	
expiration	Expire time.	user	Not Specified	
comment	Comment.	var-string	Maximum length: 255	

config user krb-keytab

Configure Kerberos keytab entries.

```
config user krb-keytab
    Description: Configure Kerberos keytab entries.
    edit <name>
        set pac-data [enable|disable]
        set principal {string}
        set ldap-server <name1>, <name2>, ...
        set keytab {string}
    next
end
```

config user krb-keytab

Parameter	Description	Type	Size	Default
name	Kerberos keytab entry name.	string	Maximum length: 35	
pac-data	Enable/disable parsing PAC data in the ticket.	option	-	enable
	Option	Description		
	enable	Enable parsing PAC data in the ticket.		
	disable	Disable parsing PAC data in the ticket.		
principal	Kerberos service principal. For example, HTTP/myfgt.example.com@example.com.	string	Maximum length: 511	

Parameter	Description	Type	Size	Default
ldap-server <name>	LDAP server name(s). LDAP server name.	string	Maximum length: 79	
keytab	Base64 coded keytab file containing a pre-shared key.	string	Maximum length: 8191	

config user ldap

Configure LDAP server entries.

```
config user ldap
  Description: Configure LDAP server entries.
  edit <name>
    set server {string}
    set secondary-server {string}
    set tertiary-server {string}
    set server-identity-check [enable|disable]
    set source-ip {string}
    set source-port {integer}
    set cnid {string}
    set dn {string}
    set type [simple|anonymous|...]
    set two-factor [disable|fortitoken-cloud]
    set two-factor-authentication [fortitoken|email|...]
    set two-factor-notification [email|sms]
    set two-factor-filter {string}
    set username {string}
    set password {password}
    set group-member-check [user-attr|group-object|...]
    set group-search-base {string}
    set group-object-filter {string}
    set group-filter {string}
    set secure [disable|starttls|...]
    set ssl-max-proto-version [SSLv3|TLSv1|...]
    set ssl-min-proto-version [default|SSLv3|...]
    set ca-cert {string}
    set port {integer}
    set password-expiry-warning [enable|disable]
    set password-renewal [enable|disable]
    set member-attr {string}
    set account-key-processing [same|strip]
    set account-key-upn-san [othername|rfc822name|...]
    set account-key-filter {string}
    set search-type {option1}, {option2}, ...
    set max-connections {integer}
    set client-cert-auth [enable|disable]
    set client-cert {string}
    set obtain-user-info [enable|disable]
    set user-info-exchange-server {string}
    set interface-select-method [auto|specify]
    set interface {string}
```

```

        set antiphish [enable|disable]
        set password-attr {string}
    next
end

```

config user ldap

Parameter	Description	Type	Size	Default
name	LDAP server entry name.	string	Maximum length: 35	
server	LDAP server CN domain name or IP.	string	Maximum length: 63	
secondary-server	Secondary LDAP server CN domain name or IP.	string	Maximum length: 63	
tertiary-server	Tertiary LDAP server CN domain name or IP.	string	Maximum length: 63	
server-identity-check	Enable/disable LDAP server identity check (verify server domain name/IP address against the server certificate).	option	-	enable
	Option	Description		
	enable	Enable server identity check.		
	disable	Disable server identity check.		
source-ip	FortiProxy IP address to be used for communication with the LDAP server.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default								
source-port	Source port to be used for communication with the LDAP server.	integer	Minimum value: 0 Maximum value: 65535	0								
cnid	Common name identifier for the LDAP server. The common name identifier for most LDAP servers is "cn".	string	Maximum length: 20	cn								
dn	Distinguished name used to look up entries on the LDAP server.	string	Maximum length: 511									
type	Authentication type for LDAP searches.	option	-	simple								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>simple</i></td><td>Simple password authentication without search.</td></tr><tr><td><i>anonymous</i></td><td>Bind using anonymous user search.</td></tr><tr><td><i>regular</i></td><td>Bind using username/password and then search.</td></tr></table>				Option	Description	<i>simple</i>	Simple password authentication without search.	<i>anonymous</i>	Bind using anonymous user search.	<i>regular</i>	Bind using username/password and then search.
Option	Description											
<i>simple</i>	Simple password authentication without search.											
<i>anonymous</i>	Bind using anonymous user search.											
<i>regular</i>	Bind using username/password and then search.											
two-factor	Enable/disable two-factor authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>disable two-factor authentication.</td></tr><tr><td><i>fortitoken-cloud</i></td><td>FortiToken Cloud Service.</td></tr></table>				Option	Description	<i>disable</i>	disable two-factor authentication.	<i>fortitoken-cloud</i>	FortiToken Cloud Service.		
Option	Description											
<i>disable</i>	disable two-factor authentication.											
<i>fortitoken-cloud</i>	FortiToken Cloud Service.											
two-factor-authentication	Authentication method by FortiToken Cloud.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortitoken</i></td><td>FortiToken authentication.</td></tr></table>				Option	Description	<i>fortitoken</i>	FortiToken authentication.				
Option	Description											
<i>fortitoken</i>	FortiToken authentication.											

Parameter	Description	Type	Size	Default
	Option	Description		
	email	Email one time password.		
	sms	SMS one time password.		
two-factor-notification	Notification method for user activation by FortiToken Cloud.	option	-	
	Option	Description		
	email	Email notification for activation code.		
	sms	SMS notification for activation code.		
two-factor-filter	Filter used to synchronize users to FortiToken Cloud.	string	Maximum length: 2047	
username	Username (full DN) for initial binding.	string	Maximum length: 511	
password	Password for initial binding.	password	Not Specified	
group-member-check	Group member checking methods.	option	-	user-attr
	Option	Description		
	user-attr	User attribute checking.		
	group-object	Group object checking.		
	posix-group-object	POSIX group object checking.		
group-search-base	Search base used for group searching.	string	Maximum length: 511	
group-object-filter	Filter used for group searching.	string	Maximum length: 2047	(&(objectcategory=group)(member=*))

Parameter	Description	Type	Size	Default														
group-filter	Filter used for group matching.	string	Maximum length: 2047															
secure	Port to be used for authentication.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>No SSL.</td></tr><tr><td><i>starttls</i></td><td>Use StartTLS.</td></tr><tr><td><i>ldaps</i></td><td>Use LDAPS.</td></tr></table>	Option	Description	<i>disable</i>	No SSL.	<i>starttls</i>	Use StartTLS.	<i>ldaps</i>	Use LDAPS.									
Option	Description																	
<i>disable</i>	No SSL.																	
<i>starttls</i>	Use StartTLS.																	
<i>ldaps</i>	Use LDAPS.																	
ssl-max-protocol-version	Maximum supported protocol version for SSL/TLS connections.	option	-	TLSv1-3														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr><tr><td><i>TLSv1-3</i></td><td>TLSv1.3.</td></tr></table>	Option	Description	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.	<i>TLSv1-3</i>	TLSv1.3.					
Option	Description																	
<i>SSLv3</i>	SSLv3.																	
<i>TLSv1</i>	TLSv1.																	
<i>TLSv1-1</i>	TLSv1.1.																	
<i>TLSv1-2</i>	TLSv1.2.																	
<i>TLSv1-3</i>	TLSv1.3.																	
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr><tr><td><i>TLSv1-3</i></td><td>TLSv1.3.</td></tr></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.	<i>TLSv1-3</i>	TLSv1.3.			
Option	Description																	
<i>default</i>	Follow system global setting.																	
<i>SSLv3</i>	SSLv3.																	
<i>TLSv1</i>	TLSv1.																	
<i>TLSv1-1</i>	TLSv1.1.																	
<i>TLSv1-2</i>	TLSv1.2.																	
<i>TLSv1-3</i>	TLSv1.3.																	

Parameter	Description	Type	Size	Default
ca-cert	CA certificate name.	string	Maximum length: 79	
port	Port to be used for communication with the LDAP server.	integer	Minimum value: 1 Maximum value: 65535	389
password-expiry-warning	Enable/disable password expiry warnings.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable password expiry warnings.	
		<i>disable</i>	Disable password expiry warnings.	
password-renewal	Enable/disable online password renewal.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable online password renewal.	
		<i>disable</i>	Disable online password renewal.	
member-attr	Name of attribute from which to get group membership.	string	Maximum length: 63	memberOf
account-key-processing	Account key processing operation, either keep or strip domain string of UPN in the token.	option	-	same
		Option	Description	
		<i>same</i>	Same as UPN.	
		<i>strip</i>	Strip domain string from UPN.	

Parameter	Description	Type	Size	Default
account-key-upn-san	Define SAN in certificate for user principle name matching.	option	-	othername
	Option	Description		
	<i>othername</i>	Other name in SAN.		
	<i>rfc822name</i>	RFC822 Email address in SAN.		
	<i>dnsname</i>	DNS name in SAN.		
account-key-filter	Account key filter, using the UPN as the search filter.	string	Maximum length: 2047	(&(userPrincipalName=%s)(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))
search-type	Search type.	option	-	recursive
	Option	Description		
	<i>recursive</i>	Recursively retrieve the user-group chain information of a user in a particular Microsoft AD domain.		
max-connections	Maximum LDAP server connections.	integer	Minimum value: 16 Maximum value: 5000	64
client-cert-auth	Enable/disable using client certificate for TLS authentication.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable using client certificate for TLS authentication.		
	<i>disable</i>	Disable using client certificate for TLS authentication.		
client-cert	Client certificate name.	string	Maximum length: 79	
obtain-user-info	Enable/disable obtaining of user information.	option	-	enable

Parameter	Description	Type	Size	Default
	Option		Description	
	enable	Enable obtaining of user information.		
	disable	Disable obtaining of user information.		
user-info-exchange-server	MS Exchange server from which to fetch user information.	string	Maximum length: 35	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option		Description	
	auto	Set outgoing interface automatically.		
	specify	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
antiphish	Enable/disable AntiPhishing credential backend.	option	-	disable
	Option		Description	
	enable	Enable AntiPhishing credential backend.		
	disable	Disable AntiPhishing credential backend.		
password-attr	Name of attribute to get password hash.	string	Maximum length: 35	userPassword

config user local

Configure local users.

```
config user local
  Description: Configure local users.
  edit <name>
    set id {integer}
    set status [enable|disable]
```

```

set type [password|radius|...]
set passwd {password}
set ldap-server {string}
set radius-server {string}
set tacacs+-server {string}
set two-factor [disable|fortitoken|...]
set two-factor-authentication [fortitoken|email|...]
set two-factor-notification [email|sms]
set fortitoken {string}
set email-to {string}
set sms-server [fortiguard|custom]
set sms-custom-server {string}
set sms-phone {string}
set passwd-policy {string}
set passwd-time {user}
set authtimeout {integer}
set workstation {string}
set auth-concurrent-override [enable|disable]
set auth-concurrent-value {integer}
set ppk-secret {password-3}
set ppk-identity {string}
set username-sensitivity [disable|enable]
next
end

```

config user local

Parameter	Description	Type	Size	Default						
name	Local user name.	string	Maximum length: 64							
id	User ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
status	Enable/disable allowing the local user to authenticate with the FortiProxy unit.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable user.</td></tr><tr><td><i>disable</i></td><td>Disable user.</td></tr></table>				Option	Description	<i>enable</i>	Enable user.	<i>disable</i>	Disable user.
Option	Description									
<i>enable</i>	Enable user.									
<i>disable</i>	Disable user.									
type	Authentication method.	option	-	password						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>password</i></td><td>Password authentication.</td></tr><tr><td><i>radius</i></td><td>RADIUS server authentication.</td></tr></table>				Option	Description	<i>password</i>	Password authentication.	<i>radius</i>	RADIUS server authentication.
Option	Description									
<i>password</i>	Password authentication.									
<i>radius</i>	RADIUS server authentication.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>tacacs+</i>	TACACS+ server authentication.		
	<i>ldap</i>	LDAP server authentication.		
passwd	User's password.	password	Not Specified	
ldap-server	Name of LDAP server with which the user must authenticate.	string	Maximum length: 35	
radius-server	Name of RADIUS server with which the user must authenticate.	string	Maximum length: 35	
tacacs+-server	Name of TACACS+ server with which the user must authenticate.	string	Maximum length: 35	
two-factor	Enable/disable two-factor authentication.	option	-	disable
	Option	Description		
	<i>disable</i>	disable		
	<i>fortitoken</i>	FortiToken		
	<i>fortitoken-cloud</i>	FortiToken Cloud Service.		
	<i>email</i>	Email authentication code.		
	<i>sms</i>	SMS authentication code.		
two-factor-authentication	Authentication method by FortiToken Cloud.	option	-	
	Option	Description		
	<i>fortitoken</i>	FortiToken authentication.		
	<i>email</i>	Email one time password.		
	<i>sms</i>	SMS one time password.		
two-factor-notification	Notification method for user activation by FortiToken Cloud.	option	-	
	Option	Description		
	<i>email</i>	Email notification for activation code.		
	<i>sms</i>	SMS notification for activation code.		
fortitoken	Two-factor recipient's FortiToken serial number.	string	Maximum length: 16	

Parameter	Description	Type	Size	Default						
email-to	Two-factor recipient's email address.	string	Maximum length: 63							
sms-server	Send SMS through FortiGuard or other external server.	option	-	fortiguard						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>fortiguard</td><td>Send SMS by FortiGuard.</td></tr><tr><td>custom</td><td>Send SMS by custom server.</td></tr></table>				Option	Description	fortiguard	Send SMS by FortiGuard.	custom	Send SMS by custom server.
Option	Description									
fortiguard	Send SMS by FortiGuard.									
custom	Send SMS by custom server.									
sms-custom-server	Two-factor recipient's SMS server.	string	Maximum length: 35							
sms-phone	Two-factor recipient's mobile phone number.	string	Maximum length: 15							
passwd-policy	Password policy to apply to this user, as defined in config user password-policy.	string	Maximum length: 35							
passwd-time	Time of the last password update.	user	Not Specified							
authtimeout	Time in minutes before the authentication timeout for a user is reached.	integer	Minimum value: 0 Maximum value: 1440	0						
workstation	Name of the remote user workstation, if you want to limit the user to authenticate only from a particular workstation.	string	Maximum length: 35							
auth-concurrent-override	Enable/disable overriding the policy-auth-concurrent under config system global.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable auth-concurrent-override.</td></tr><tr><td>disable</td><td>Disable auth-concurrent-override.</td></tr></table>				Option	Description	enable	Enable auth-concurrent-override.	disable	Disable auth-concurrent-override.
Option	Description									
enable	Enable auth-concurrent-override.									
disable	Disable auth-concurrent-override.									
auth-concurrent-value	Maximum number of concurrent logins permitted from the same user.	integer	Minimum value: 0 Maximum value: 100	0						
ppk-secret	IKEv2 Postquantum Preshared Key (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified							
ppk-identity	IKEv2 Postquantum Preshared Key Identity.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default
username-sensitivity	Enable/disable case and accent sensitivity when performing username matching (accents are stripped and case is ignored when disabled).	option	-	enable
	Option	Description		
	<i>disable</i>	Ignore case and accents. Username at prompt not required to match case or accents.		
	<i>enable</i>	Do not ignore case and accents. Username at prompt must be an exact match.		

config user password-policy

Configure user password policy.

```
config user password-policy
  Description: Configure user password policy.
  edit <name>
    set expire-days {integer}
    set warn-days {integer}
    set expired-password-renewal [enable|disable]
  next
end
```

config user password-policy

Parameter	Description	Type	Size	Default
name	Password policy name.	string	Maximum length: 35	
expire-days	Time in days before the user's password expires.	integer	Minimum value: 0 Maximum value: 999	180
warn-days	Time in days before a password expiration warning message is displayed to the user upon login.	integer	Minimum value: 0 Maximum value: 30	15
expired-password-renewal	Enable/disable renewal of a password that already is expired.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable renewal of a password that already is expired.		
	<i>disable</i>	Disable renewal of a password that already is expired.		

config user peer

Configure peer users.

```
config user peer
  Description: Configure peer users.
  edit <name>
    set mandatory-ca-verify [enable|disable]
    set ca {string}
    set subject {string}
    set cn {string}
    set cn-type [string|email|...]
    set ldap-server {string}
    set ldap-username {string}
    set ldap-password {password}
    set ldap-mode [password|principal-name]
    set ocap-override-server {string}
    set two-factor [enable|disable]
    set passwd {password}
  next
end
```

config user peer

Parameter	Description	Type	Size	Default
name	Peer name.	string	Maximum length: 35	
mandatory-ca-verify	Determine what happens to the peer if the CA certificate is not installed. Disable to automatically consider the peer certificate as valid.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ca	Name of the CA certificate.	string	Maximum length: 127	

Parameter	Description	Type	Size	Default
subject	Peer certificate name constraints.	string	Maximum length: 255	
cn	Peer certificate common name.	string	Maximum length: 255	
cn-type	Peer certificate common name type.	option	-	string
	OptionDescription			
	string	Normal string.		
	email	Email address.		
	FQDN	Fully Qualified Domain Name.		
	ipv4	IPv4 address.		
	ipv6	IPv6 address.		
ldap-server	Name of an LDAP server defined under the user ldap command. Performs client access rights check.	string	Maximum length: 35	
ldap-username	Username for LDAP server bind.	string	Maximum length: 35	
ldap-password	Password for LDAP server bind.	password	Not Specified	
ldap-mode	Mode for LDAP peer authentication.	option	-	password
	OptionDescription			
	password	Username/password.		
	principal-name	Principal name.		
ocsp-override-server	Online Certificate Status Protocol (OCSP) server for certificate retrieval.	string	Maximum length: 35	
two-factor	Enable/disable two-factor authentication, applying certificate and password-based authentication.	option	-	disable
	OptionDescription			
	enable	Enable 2-factor authentication.		
	disable	Disable 2-factor authentication.		
passwd	Peer's password used for two-factor authentication.	password	Not Specified	

config user peergrp

Configure peer groups.

```
config user peergrp
  Description: Configure peer groups.
  edit <name>
    set member <name1>, <name2>, ...
  next
end
```

config user peergrp

Parameter	Description	Type	Size	Default
name	Peer group name.	string	Maximum length: 35	
member <name>	Peer group members. Peer group member name.	string	Maximum length: 35	

config user pop3

POP3 server entry configuration.

```
config user pop3
  Description: POP3 server entry configuration.
  edit <name>
    set server {string}
    set port {integer}
    set secure [none|starttls|...]
    set ssl-min-proto-version [default|SSLv3|...]
  next
end
```

config user pop3

Parameter	Description	Type	Size	Default
name	POP3 server entry name.	string	Maximum length: 35	
server	Server domain name or IP address.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
port	POP3 service port number.	integer	Minimum value: 0 Maximum value: 65535	0
secure	SSL connection.	option	-	starttls
	Option		Description	
	<i>none</i>	None.		
	<i>starttls</i>	Use StartTLS.		
	<i>pop3s</i>	Use POP3 over SSL.		
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default
	Option		Description	
	<i>default</i>	Follow system global setting.		
	<i>SSLv3</i>	SSLv3.		
	<i>TLSv1</i>	TLSv1.		
	<i>TLSv1-1</i>	TLSv1.1.		
	<i>TLSv1-2</i>	TLSv1.2.		

config user radius

Configure RADIUS server entries.

```
config user radius
    Description: Configure RADIUS server entries.
    edit <name>
        set server {string}
        set secret {password}
        set secondary-server {string}
        set secondary-secret {password}
        set tertiary-server {string}
        set tertiary-secret {password}
        set timeout {integer}
        set all-usergroup [disable|enable]
        set use-management-vdom [enable|disable]
        set nas-ip {ipv4-address}
        set nas-id-type [legacy|custom|...]
        set nas-id {string}
        set acct-interim-interval {integer}
        set radius-coa [enable|disable]
```

```
set radius-port {integer}
set h3c-compatibility [enable|disable]
set auth-type [auto|ms_chap_v2|...]
set source-ip {string}
set username-case-sensitive [enable|disable]
set group-override-attr-type [filter-Id|class]
set class <name1>, <name2>, ...
set password-renewal [enable|disable]
set require-message-authenticator [enable|disable]
set password-encoding [auto|ISO-8859-1]
set mac-username-delimiter [hyphen|single-hyphen|...]
set mac-password-delimiter [hyphen|single-hyphen|...]
set mac-case [uppercase|lowercase]
set acct-all-servers [enable|disable]
set switch-controller-acct-fast-framedip-detect {integer}
set interface-select-method [auto|specify]
set interface {string}
set switch-controller-service-type {option1}, {option2}, ...
set rso [enable|disable]
set rso-radius-server-port {integer}
set rso-radius-response [enable|disable]
set rso-validate-request-secret [enable|disable]
set rso-secret {password}
set rso-endpoint-attribute [User-Name|NAS-IP-Address|...]
set rso-endpoint-block-attribute [User-Name|NAS-IP-Address|...]
set sso-attribute [User-Name|NAS-IP-Address|...]
set sso-attribute-key {string}
set sso-attribute-value-override [enable|disable]
set rso-context-timeout {integer}
set rso-log-period {integer}
set rso-log-flags {option1}, {option2}, ...
set rso-flush-ip-session [enable|disable]
set rso-ep-one-ip-only [enable|disable]
set delimiter [plus|comma]
config accounting-server
    Description: Additional accounting servers.
    edit <id>
        set status [enable|disable]
        set server {string}
        set secret {password}
        set port {integer}
        set source-ip {string}
        set interface-select-method [auto|specify]
        set interface {string}
    next
end
next
end
```

config user radius

Parameter	Description	Type	Size	Default						
name	RADIUS server entry name.	string	Maximum length: 35							
server	Primary RADIUS server CN domain name or IP address.	string	Maximum length: 63							
secret	Pre-shared secret key used to access the primary RADIUS server.	password	Not Specified							
secondary-server	Secondary RADIUS CN domain name or IP address.	string	Maximum length: 63							
secondary-secret	Secret key to access the secondary server.	password	Not Specified							
tertiary-server	Tertiary RADIUS CN domain name or IP address.	string	Maximum length: 63							
tertiary-secret	Secret key to access the tertiary server.	password	Not Specified							
timeout	Time in seconds between re-sending authentication requests.	integer	Minimum value: 1 Maximum value: 300	5						
all-usergroup	Enable/disable automatically including this RADIUS server in all user groups.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not automatically include this server in a user group.</td></tr><tr><td><i>enable</i></td><td>Include this RADIUS server in every user group.</td></tr></table>				Option	Description	<i>disable</i>	Do not automatically include this server in a user group.	<i>enable</i>	Include this RADIUS server in every user group.
Option	Description									
<i>disable</i>	Do not automatically include this server in a user group.									
<i>enable</i>	Include this RADIUS server in every user group.									
use-management-vdom	Enable/disable using management VDOM to send requests.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Send requests using the management VDOM.</td></tr><tr><td><i>disable</i></td><td>Send requests using the current VDOM.</td></tr></table>				Option	Description	<i>enable</i>	Send requests using the management VDOM.	<i>disable</i>	Send requests using the current VDOM.
Option	Description									
<i>enable</i>	Send requests using the management VDOM.									
<i>disable</i>	Send requests using the current VDOM.									
nas-ip	IP address used to communicate with the RADIUS server and used as NAS-IP-Address and Called-Station-ID attributes.	ipv4-address	Not Specified	0.0.0.0						
nas-id-type	NAS identifier type configuration.	option	-	legacy						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>legacy</i>	NAS-ID value is the value previously used by each daemon.		
	<i>custom</i>	NAS-ID value is customized.		
	<i>hostname</i>	NAS-ID value is hostname or HA group name if applicable.		
nas-id	Custom NAS identifier.	string	Maximum length: 255	
acct-interim-interval	Time in seconds between each accounting interim update message.	integer	Minimum value: 60 Maximum value: 86400	0
radius-coa	Enable to allow a mechanism to change the attributes of an authentication, authorization, and accounting session after it is authenticated.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable RADIUS CoA.		
	<i>disable</i>	Disable RADIUS CoA.		
radius-port	RADIUS service port number.	integer	Minimum value: 0 Maximum value: 65535	0
h3c-compatibility	Enable/disable compatibility with the H3C, a mechanism that performs security checking for authentication.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable H3C compatibility.		
	<i>disable</i>	Disable H3C compatibility.		
auth-type	Authentication methods/protocols permitted for this RADIUS server.	option	-	auto
	Option	Description		
	<i>auto</i>	Use PAP, MSCHAP_v2, and CHAP (in that order).		
	<i>ms_chap_v2</i>	Microsoft Challenge Handshake Authentication Protocol version 2.		
	<i>ms_chap</i>	Microsoft Challenge Handshake Authentication Protocol.		

Parameter	Description	Type	Size	Default
	Option Description			
	<i>chap</i>	Challenge Handshake Authentication Protocol.		
	<i>pap</i>	Password Authentication Protocol.		
source-ip	Source IP address for communications to the RADIUS server.	string	Maximum length: 63	
username-case-sensitive	Enable/disable case sensitive user names.	option	-	disable
	Option Description			
	<i>enable</i>	Enable username case-sensitive.		
	<i>disable</i>	Disable username case-sensitive.		
group-override-attr-type	RADIUS attribute type to override user group information.	option	-	
	Option Description			
	<i>filter-id</i>	Filter-Id		
	<i>class</i>	Class		
class <name>	Class attribute name(s). Class name.	string	Maximum length: 79	
password-renewal	Enable/disable password renewal.	option	-	enable
	Option Description			
	<i>enable</i>	Enable password renewal.		
	<i>disable</i>	Disable password renewal.		
require-message-authenticator	Require message authenticator in authentication response.	option	-	enable
	Option Description			
	<i>enable</i>	Make the validation of message authenticator mandatory in authentication response.		
	<i>disable</i>	Make the validation of message authenticator optional in authentication response.		

Parameter	Description	Type	Size	Default										
password-encoding	Password encoding.	option	-	auto										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Use original password encoding.</td></tr><tr><td><i>ISO-8859-1</i></td><td>Use ISO-8859-1 password encoding.</td></tr></table>	Option	Description	<i>auto</i>	Use original password encoding.	<i>ISO-8859-1</i>	Use ISO-8859-1 password encoding.							
Option	Description													
<i>auto</i>	Use original password encoding.													
<i>ISO-8859-1</i>	Use ISO-8859-1 password encoding.													
mac-username-delimiter	MAC authentication username delimiter.	option	-	hyphen										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hyphen</i></td><td>Use hyphen as delimiter for MAC authentication username.</td></tr><tr><td><i>single-hyphen</i></td><td>Use single hyphen as delimiter for MAC authentication username.</td></tr><tr><td><i>colon</i></td><td>Use colon as delimiter for MAC authentication username.</td></tr><tr><td><i>none</i></td><td>No delimiter for MAC authentication username.</td></tr></table>	Option	Description	<i>hyphen</i>	Use hyphen as delimiter for MAC authentication username.	<i>single-hyphen</i>	Use single hyphen as delimiter for MAC authentication username.	<i>colon</i>	Use colon as delimiter for MAC authentication username.	<i>none</i>	No delimiter for MAC authentication username.			
Option	Description													
<i>hyphen</i>	Use hyphen as delimiter for MAC authentication username.													
<i>single-hyphen</i>	Use single hyphen as delimiter for MAC authentication username.													
<i>colon</i>	Use colon as delimiter for MAC authentication username.													
<i>none</i>	No delimiter for MAC authentication username.													
mac-password-delimiter	MAC authentication password delimiter.	option	-	hyphen										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hyphen</i></td><td>Use hyphen as delimiter for MAC authentication password.</td></tr><tr><td><i>single-hyphen</i></td><td>Use single hyphen as delimiter for MAC authentication password.</td></tr><tr><td><i>colon</i></td><td>Use colon as delimiter for MAC authentication password.</td></tr><tr><td><i>none</i></td><td>No delimiter for MAC authentication password.</td></tr></table>	Option	Description	<i>hyphen</i>	Use hyphen as delimiter for MAC authentication password.	<i>single-hyphen</i>	Use single hyphen as delimiter for MAC authentication password.	<i>colon</i>	Use colon as delimiter for MAC authentication password.	<i>none</i>	No delimiter for MAC authentication password.			
Option	Description													
<i>hyphen</i>	Use hyphen as delimiter for MAC authentication password.													
<i>single-hyphen</i>	Use single hyphen as delimiter for MAC authentication password.													
<i>colon</i>	Use colon as delimiter for MAC authentication password.													
<i>none</i>	No delimiter for MAC authentication password.													
mac-case	MAC authentication case.	option	-	lowercase										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>uppercase</i></td><td>Use uppercase MAC.</td></tr><tr><td><i>lowercase</i></td><td>Use lowercase MAC.</td></tr></table>	Option	Description	<i>uppercase</i>	Use uppercase MAC.	<i>lowercase</i>	Use lowercase MAC.							
Option	Description													
<i>uppercase</i>	Use uppercase MAC.													
<i>lowercase</i>	Use lowercase MAC.													
acct-all-servers	Enable/disable sending of accounting messages to all configured servers.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Send accounting messages to all configured servers.</td></tr><tr><td><i>disable</i></td><td>Send accounting message only to servers that are confirmed to be reachable.</td></tr></table>	Option	Description	<i>enable</i>	Send accounting messages to all configured servers.	<i>disable</i>	Send accounting message only to servers that are confirmed to be reachable.							
Option	Description													
<i>enable</i>	Send accounting messages to all configured servers.													
<i>disable</i>	Send accounting message only to servers that are confirmed to be reachable.													

Parameter	Description	Type	Size	Default																								
switch-controller-acct-fast-framedip-detect	Switch controller accounting message Framed-IP detection from DHCP snooping.	integer	Minimum value: 2 Maximum value: 600	2																								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	auto	Set outgoing interface automatically.	specify	Set outgoing interface manually.																		
	Option	Description																										
	auto	Set outgoing interface automatically.																										
specify	Set outgoing interface manually.																											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15																									
switch-controller-service-type	RADIUS service type.	option	-																									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>login</td><td>User should be connected to a host.</td></tr><tr><td>framed</td><td>User use Framed Protocol.</td></tr><tr><td>callback-login</td><td>User disconnected and called back.</td></tr><tr><td>callback-framed</td><td>User disconnected and called back, then a Framed Protocol.</td></tr><tr><td>outbound</td><td>User granted access to outgoing devices.</td></tr><tr><td>administrative</td><td>User granted access to the administrative unsigned interface.</td></tr><tr><td>nas-prompt</td><td>User provided a command prompt on the NAS.</td></tr><tr><td>authenticate-only</td><td>Authentication requested, and no auth info needs to be returned.</td></tr><tr><td>callback-nas-prompt</td><td>User disconnected and called back, then provided a command prompt.</td></tr><tr><td>call-check</td><td>Used by the NAS in an Access-Request packet, Access-Accept to answer the call.</td></tr><tr><td>callback-administrative</td><td>User disconnected and called back, granted access to the admin unsigned interface.</td></tr></table>				Option	Description	login	User should be connected to a host.	framed	User use Framed Protocol.	callback-login	User disconnected and called back.	callback-framed	User disconnected and called back, then a Framed Protocol.	outbound	User granted access to outgoing devices.	administrative	User granted access to the administrative unsigned interface.	nas-prompt	User provided a command prompt on the NAS.	authenticate-only	Authentication requested, and no auth info needs to be returned.	callback-nas-prompt	User disconnected and called back, then provided a command prompt.	call-check	Used by the NAS in an Access-Request packet, Access-Accept to answer the call.	callback-administrative	User disconnected and called back, granted access to the admin unsigned interface.
	Option	Description																										
	login	User should be connected to a host.																										
	framed	User use Framed Protocol.																										
	callback-login	User disconnected and called back.																										
	callback-framed	User disconnected and called back, then a Framed Protocol.																										
	outbound	User granted access to outgoing devices.																										
	administrative	User granted access to the administrative unsigned interface.																										
	nas-prompt	User provided a command prompt on the NAS.																										
	authenticate-only	Authentication requested, and no auth info needs to be returned.																										
	callback-nas-prompt	User disconnected and called back, then provided a command prompt.																										
call-check	Used by the NAS in an Access-Request packet, Access-Accept to answer the call.																											
callback-administrative	User disconnected and called back, granted access to the admin unsigned interface.																											
rsso	Enable/disable RADIUS based single sign on feature.	option	-	disable																								

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable RADIUS based single sign on feature.		
	<i>disable</i>	Disable RADIUS based single sign on feature.		
rsso-radius-server-port	UDP port to listen on for RADIUS Start and Stop records.	integer	Minimum value: 0 Maximum value: 65535	1813
rsso-radius-response	Enable/disable sending RADIUS response packets after receiving Start and Stop records.	option	-	disable
	Option Description			
	<i>enable</i>	Enable sending RADIUS response packets.		
	<i>disable</i>	Disable sending RADIUS response packets.		
rsso-validate-request-secret	Enable/disable validating the RADIUS request shared secret in the Start or End record.	option	-	disable
	Option Description			
	<i>enable</i>	Enable validating RADIUS request shared secret.		
	<i>disable</i>	Disable validating RADIUS request shared secret.		
rsso-secret	RADIUS secret used by the RADIUS accounting server.	password	Not Specified	
rsso-endpoint-attribute	RADIUS attributes used to extract the user endpoint identifier from the RADIUS Start record.	option	-	Calling-Station-Id
	Option Description			
	<i>User-Name</i>	Use this attribute.		
	<i>NAS-IP-Address</i>	Use this attribute.		
	<i>Framed-IP-Address</i>	Use this attribute.		
	<i>Framed-IP-Netmask</i>	Use this attribute.		
	<i>Filter-Id</i>	Use this attribute.		
	<i>Login-IP-Host</i>	Use this attribute.		
	<i>Reply-Message</i>	Use this attribute.		

Parameter	Description	Type	Size	Default																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>Callback-Number</td><td>Use this attribute.</td></tr><tr><td>Callback-Id</td><td>Use this attribute.</td></tr><tr><td>Framed-Route</td><td>Use this attribute.</td></tr><tr><td>Framed-IPX-Network</td><td>Use this attribute.</td></tr><tr><td>Class</td><td>Use this attribute.</td></tr><tr><td>Called-Station-Id</td><td>Use this attribute.</td></tr><tr><td>Calling-Station-Id</td><td>Use this attribute.</td></tr><tr><td>NAS-Identifier</td><td>Use this attribute.</td></tr><tr><td>Proxy-State</td><td>Use this attribute.</td></tr><tr><td>Login-LAT-Service</td><td>Use this attribute.</td></tr><tr><td>Login-LAT-Node</td><td>Use this attribute.</td></tr><tr><td>Login-LAT-Group</td><td>Use this attribute.</td></tr><tr><td>Framed-AppleTalk-Zone</td><td>Use this attribute.</td></tr><tr><td>Acct-Session-Id</td><td>Use this attribute.</td></tr><tr><td>Acct-Multi-Session-Id</td><td>Use this attribute.</td></tr></table>	Option	Description	Callback-Number	Use this attribute.	Callback-Id	Use this attribute.	Framed-Route	Use this attribute.	Framed-IPX-Network	Use this attribute.	Class	Use this attribute.	Called-Station-Id	Use this attribute.	Calling-Station-Id	Use this attribute.	NAS-Identifier	Use this attribute.	Proxy-State	Use this attribute.	Login-LAT-Service	Use this attribute.	Login-LAT-Node	Use this attribute.	Login-LAT-Group	Use this attribute.	Framed-AppleTalk-Zone	Use this attribute.	Acct-Session-Id	Use this attribute.	Acct-Multi-Session-Id	Use this attribute.			
	Option	Description																																		
	Callback-Number	Use this attribute.																																		
	Callback-Id	Use this attribute.																																		
	Framed-Route	Use this attribute.																																		
	Framed-IPX-Network	Use this attribute.																																		
	Class	Use this attribute.																																		
	Called-Station-Id	Use this attribute.																																		
	Calling-Station-Id	Use this attribute.																																		
	NAS-Identifier	Use this attribute.																																		
	Proxy-State	Use this attribute.																																		
	Login-LAT-Service	Use this attribute.																																		
	Login-LAT-Node	Use this attribute.																																		
	Login-LAT-Group	Use this attribute.																																		
	Framed-AppleTalk-Zone	Use this attribute.																																		
Acct-Session-Id	Use this attribute.																																			
Acct-Multi-Session-Id	Use this attribute.																																			
rsso-endpoint-block-attribute	RADIUS attributes used to block a user.	option	-																																	
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>User-Name</td><td>Use this attribute.</td></tr><tr><td>NAS-IP-Address</td><td>Use this attribute.</td></tr><tr><td>Framed-IP-Address</td><td>Use this attribute.</td></tr><tr><td>Framed-IP-Netmask</td><td>Use this attribute.</td></tr><tr><td>Filter-Id</td><td>Use this attribute.</td></tr></table>	Option	Description	User-Name	Use this attribute.	NAS-IP-Address	Use this attribute.	Framed-IP-Address	Use this attribute.	Framed-IP-Netmask	Use this attribute.	Filter-Id	Use this attribute.																							
	Option	Description																																		
	User-Name	Use this attribute.																																		
	NAS-IP-Address	Use this attribute.																																		
	Framed-IP-Address	Use this attribute.																																		
	Framed-IP-Netmask	Use this attribute.																																		
Filter-Id	Use this attribute.																																			

Parameter	Description	Type	Size	Default																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>Login-IP-Host</td><td>Use this attribute.</td></tr><tr><td>Reply-Message</td><td>Use this attribute.</td></tr><tr><td>Callback-Number</td><td>Use this attribute.</td></tr><tr><td>Callback-Id</td><td>Use this attribute.</td></tr><tr><td>Framed-Route</td><td>Use this attribute.</td></tr><tr><td>Framed-IPX-Network</td><td>Use this attribute.</td></tr><tr><td>Class</td><td>Use this attribute.</td></tr><tr><td>Called-Station-Id</td><td>Use this attribute.</td></tr><tr><td>Calling-Station-Id</td><td>Use this attribute.</td></tr><tr><td>NAS-Identifier</td><td>Use this attribute.</td></tr><tr><td>Proxy-State</td><td>Use this attribute.</td></tr><tr><td>Login-LAT-Service</td><td>Use this attribute.</td></tr><tr><td>Login-LAT-Node</td><td>Use this attribute.</td></tr><tr><td>Login-LAT-Group</td><td>Use this attribute.</td></tr><tr><td>Framed-AppleTalk-Zone</td><td>Use this attribute.</td></tr><tr><td>Acct-Session-Id</td><td>Use this attribute.</td></tr><tr><td>Acct-Multi-Session-Id</td><td>Use this attribute.</td></tr></table>	Option	Description	Login-IP-Host	Use this attribute.	Reply-Message	Use this attribute.	Callback-Number	Use this attribute.	Callback-Id	Use this attribute.	Framed-Route	Use this attribute.	Framed-IPX-Network	Use this attribute.	Class	Use this attribute.	Called-Station-Id	Use this attribute.	Calling-Station-Id	Use this attribute.	NAS-Identifier	Use this attribute.	Proxy-State	Use this attribute.	Login-LAT-Service	Use this attribute.	Login-LAT-Node	Use this attribute.	Login-LAT-Group	Use this attribute.	Framed-AppleTalk-Zone	Use this attribute.	Acct-Session-Id	Use this attribute.	Acct-Multi-Session-Id	Use this attribute.			
	Option	Description																																						
	Login-IP-Host	Use this attribute.																																						
	Reply-Message	Use this attribute.																																						
	Callback-Number	Use this attribute.																																						
	Callback-Id	Use this attribute.																																						
	Framed-Route	Use this attribute.																																						
	Framed-IPX-Network	Use this attribute.																																						
	Class	Use this attribute.																																						
	Called-Station-Id	Use this attribute.																																						
	Calling-Station-Id	Use this attribute.																																						
	NAS-Identifier	Use this attribute.																																						
	Proxy-State	Use this attribute.																																						
	Login-LAT-Service	Use this attribute.																																						
	Login-LAT-Node	Use this attribute.																																						
	Login-LAT-Group	Use this attribute.																																						
	Framed-AppleTalk-Zone	Use this attribute.																																						
	Acct-Session-Id	Use this attribute.																																						
Acct-Multi-Session-Id	Use this attribute.																																							
sso-attribute	RADIUS attribute that contains the profile group name to be extracted from the RADIUS Start record.	option	-	Class																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>User-Name</td><td>Use this attribute.</td></tr><tr><td>NAS-IP-Address</td><td>Use this attribute.</td></tr><tr><td>Framed-IP-Address</td><td>Use this attribute.</td></tr></table>	Option	Description	User-Name	Use this attribute.	NAS-IP-Address	Use this attribute.	Framed-IP-Address	Use this attribute.																															
	Option	Description																																						
	User-Name	Use this attribute.																																						
	NAS-IP-Address	Use this attribute.																																						
Framed-IP-Address	Use this attribute.																																							

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>Framed-IP-Netmask</i>	Use this attribute.		
	<i>Filter-Id</i>	Use this attribute.		
	<i>Login-IP-Host</i>	Use this attribute.		
	<i>Reply-Message</i>	Use this attribute.		
	<i>Callback-Number</i>	Use this attribute.		
	<i>Callback-Id</i>	Use this attribute.		
	<i>Framed-Route</i>	Use this attribute.		
	<i>Framed-IPX-Network</i>	Use this attribute.		
	<i>Class</i>	Use this attribute.		
	<i>Called-Station-Id</i>	Use this attribute.		
	<i>Calling-Station-Id</i>	Use this attribute.		
	<i>NAS-Identifier</i>	Use this attribute.		
	<i>Proxy-State</i>	Use this attribute.		
	<i>Login-LAT-Service</i>	Use this attribute.		
	<i>Login-LAT-Node</i>	Use this attribute.		
	<i>Login-LAT-Group</i>	Use this attribute.		
	<i>Framed-AppleTalk-Zone</i>	Use this attribute.		
	<i>Acct-Session-Id</i>	Use this attribute.		
	<i>Acct-Multi-Session-Id</i>	Use this attribute.		
sso-attribute-key	Key prefix for SSO group value in the SSO attribute.	string	Maximum length: 35	
sso-attribute-value-override	Enable/disable override old attribute value with new value for the same endpoint.	option	-	enable

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable override old attribute value with new value for the same endpoint.</td></tr><tr><td><i>disable</i></td><td>Disable override old attribute value with new value for the same endpoint.</td></tr></table>	Option	Description	<i>enable</i>	Enable override old attribute value with new value for the same endpoint.	<i>disable</i>	Disable override old attribute value with new value for the same endpoint.													
	Option	Description																		
	<i>enable</i>	Enable override old attribute value with new value for the same endpoint.																		
<i>disable</i>	Disable override old attribute value with new value for the same endpoint.																			
rsso-context-timeout	Time in seconds before the logged out user is removed from the "user context list" of logged on users.	integer	Minimum value: 0 Maximum value: 4294967295	28800																
rsso-log-period	Time interval in seconds that group event log messages will be generated for dynamic profile events.	integer	Minimum value: 0 Maximum value: 4294967295	0																
rsso-log-flags	Events to log.	option	-	protocol-error profile-missing accounting-stop-missed accounting-event endpoint-block radiusd-other																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>protocol-error</i></td><td>Enable this log type.</td></tr><tr><td><i>profile-missing</i></td><td>Enable this log type.</td></tr><tr><td><i>accounting-stop-missed</i></td><td>Enable this log type.</td></tr><tr><td><i>accounting-event</i></td><td>Enable this log type.</td></tr><tr><td><i>endpoint-block</i></td><td>Enable this log type.</td></tr><tr><td><i>radiusd-other</i></td><td>Enable this log type.</td></tr><tr><td><i>none</i></td><td>Disable all logging.</td></tr></table>	Option	Description	<i>protocol-error</i>	Enable this log type.	<i>profile-missing</i>	Enable this log type.	<i>accounting-stop-missed</i>	Enable this log type.	<i>accounting-event</i>	Enable this log type.	<i>endpoint-block</i>	Enable this log type.	<i>radiusd-other</i>	Enable this log type.	<i>none</i>	Disable all logging.			
	Option	Description																		
	<i>protocol-error</i>	Enable this log type.																		
	<i>profile-missing</i>	Enable this log type.																		
	<i>accounting-stop-missed</i>	Enable this log type.																		
	<i>accounting-event</i>	Enable this log type.																		
	<i>endpoint-block</i>	Enable this log type.																		
<i>radiusd-other</i>	Enable this log type.																			
<i>none</i>	Disable all logging.																			
rsso-flush-ip-session	Enable/disable flushing user IP sessions on RADIUS accounting Stop messages.	option	-	disable																

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable flush user IP sessions on RADIUS accounting stop.		
	<i>disable</i>	Disable flush user IP sessions on RADIUS accounting stop.		
rsso-ep-one-ip-only	Enable/disable the replacement of old IP addresses with new ones for the same endpoint on RADIUS accounting Start messages.	option	-	disable
	Option Description			
	<i>enable</i>	Enable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.		
	<i>disable</i>	Disable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.		
delimiter	Configure delimiter to be used for separating profile group names in the SSO attribute.	option	-	plus
	Option Description			
	<i>plus</i>	Plus character "+".		
	<i>comma</i>	Comma character ",".		

config accounting-server

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Status.	option	-	disable
	Option Description			
	<i>enable</i>	Log to remote syslog server.		
	<i>disable</i>	Do not log to remote syslog server.		
server	Server CN domain name or IP address.	string	Maximum length: 63	
secret	Secret key.	password	Not Specified	

Parameter	Description	Type	Size	Default						
port	RADIUS accounting port number.	integer	Minimum value: 0 Maximum value: 65535	0						
source-ip	Source IP address for communications to the RADIUS server.	string	Maximum length: 63							
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>specify</i>	Set outgoing interface manually.
	Option	Description								
	<i>auto</i>	Set outgoing interface automatically.								
<i>specify</i>	Set outgoing interface manually.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							

config user saml

SAML server entry configuration.

```

config user saml
  Description: SAML server entry configuration.
  edit <name>
    set cert {string}
    set entity-id {string}
    set single-sign-on-url {string}
    set single-logout-url {string}
    set idp-entity-id {string}
    set idp-single-sign-on-url {string}
    set idp-single-logout-url {string}
    set idp-cert {string}
    set user-name {string}
    set group-name {string}
    set digest-method [sha1|sha256]
    set limit-relaystate [enable|disable]
    set clock-tolerance {integer}
    set adfs-claim [enable|disable]
    set user-claim-type [email|given-name|...]
    set group-claim-type [email|given-name|...]
  next
end

```

config user saml

Parameter	Description	Type	Size	Default						
name	SAML server entry name.	string	Maximum length: 35							
cert	Certificate to sign SAML messages.	string	Maximum length: 35							
entity-id	SP entity ID.	string	Maximum length: 255							
single-sign-on-url	SP single sign-on URL.	string	Maximum length: 255							
single-logout-url	SP single logout URL.	string	Maximum length: 255							
idp-entity-id	IDP entity ID.	string	Maximum length: 255							
idp-single-sign-on-url	IDP single sign-on URL.	string	Maximum length: 255							
idp-single-logout-url	IDP single logout url.	string	Maximum length: 255							
idp-cert	IDP Certificate name.	string	Maximum length: 35							
user-name	User name in assertion statement.	string	Maximum length: 255							
group-name	Group name in assertion statement.	string	Maximum length: 255							
digest-method	Digest method algorithm.	option	-	sha1						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sha1</td><td>Digest Method Algorithm is SHA1.</td></tr><tr><td>sha256</td><td>Digest Method Algorithm is SHA256.</td></tr></table>				Option	Description	sha1	Digest Method Algorithm is SHA1.	sha256	Digest Method Algorithm is SHA256.
Option	Description									
sha1	Digest Method Algorithm is SHA1.									
sha256	Digest Method Algorithm is SHA256.									
limit-relaystate	Enable/disable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).</td></tr><tr><td>disable</td><td>Disable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).</td></tr></table>				Option	Description	enable	Enable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).	disable	Disable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).
Option	Description									
enable	Enable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).									
disable	Disable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).									

Parameter	Description	Type	Size	Default
clock-tolerance	Clock skew tolerance in seconds.	integer	Minimum value: 0 Maximum value: 300	15
adfs-claim	Enable/disable ADFS Claim for user/group attribute in assertion statement.	option	-	disable
	Option		Description	
	<i>enable</i>		Enable ADFS Claim for user/group attribute in assertion statement.	
	<i>disable</i>		Disable ADFS Claim for user/group attribute in assertion statement.	
user-claim-type	User name claim in assertion statement.	option	-	upn
	Option		Description	
	<i>email</i>		E-mail address of the user.	
	<i>given-name</i>		Given name of the user.	
	<i>name</i>		Unique name of the user.	
	<i>upn</i>		User principal name (UPN) of the user.	
	<i>common-name</i>		Common name of the user.	
	<i>email-adfs-1x</i>		E-mail address of the user when interoperating with AD FS 1.1 or ADFS 1.0.	
	<i>group</i>		Group that the user is a member of.	
	<i>upn-adfs-1x</i>		User principal name (UPN) of the user.	
	<i>role</i>		Role that the user has.	
	<i>sur-name</i>		Surname of the user	
	<i>ppid</i>		Private identifier of the user.	
	<i>name-identifier</i>		SAML name identifier of the user.	
	<i>authentication-method</i>		Method used to authenticate the user.	
	<i>deny-only-group-sid</i>		Deny-only group SID of the user.	
	<i>deny-only-primary-sid</i>		Deny-only primary SID of the user.	
	<i>deny-only-primary-group-sid</i>		Deny-only primary group SID of the user.	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>group-sid</i>	Group SID of the user.		
	<i>primary-group-sid</i>	Primary group SID of the user.		
	<i>primary-sid</i>	Primary SID of the user.		
	<i>windows-account-name</i>	Domain account name of the user in the form of <domain>\<user>.		
group-claim-type	Group claim in assertion statement.	option	-	group
	Option	Description		
	<i>email</i>	E-mail address of the user.		
	<i>given-name</i>	Given name of the user.		
	<i>name</i>	Unique name of the user.		
	<i>upn</i>	User principal name (UPN) of the user.		
	<i>common-name</i>	Common name of the user.		
	<i>email-adfs-1x</i>	E-mail address of the user when interoperating with AD FS 1.1 or ADFS 1.0.		
	<i>group</i>	Group that the user is a member of.		
	<i>upn-adfs-1x</i>	User principal name (UPN) of the user.		
	<i>role</i>	Role that the user has.		
	<i>sur-name</i>	Surname of the user		
	<i>ppid</i>	Private identifier of the user.		
	<i>name-identifier</i>	SAML name identifier of the user.		
	<i>authentication-method</i>	Method used to authenticate the user.		
	<i>deny-only-group-sid</i>	Deny-only group SID of the user.		
	<i>deny-only-primary-sid</i>	Deny-only primary SID of the user.		
	<i>deny-only-primary-group-sid</i>	Deny-only primary group SID of the user.		
<i>group-sid</i>	Group SID of the user.			

Parameter	Description	Type	Size	Default
Option	Description			
<i>primary-group-sid</i>	Primary group SID of the user.			
<i>primary-sid</i>	Primary SID of the user.			
<i>windows-account-name</i>	Domain account name of the user in the form of <domain>\<user>.			

config user security-exempt-list

Configure security exemption list.

```

config user security-exempt-list
    Description: Configure security exemption list.
    edit <name>
        set description {string}
        config rule
            Description: Configure rules for exempting users from captive portal
authentication.
            edit <id>
                set srcaddr <name1>, <name2>, ...
                set dstaddr <name1>, <name2>, ...
                set service <name1>, <name2>, ...
            next
        end
    next
end

```

config user security-exempt-list

Parameter	Description	Type	Size	Default
name	Name of the exempt list.	string	Maximum length: 35	
description	Description.	string	Maximum length: 127	

config rule

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
srcaddr <name>	Source addresses or address groups. Address or group name.	string	Maximum length: 79	
dstaddr <name>	Destination addresses or address groups. Address or group name.	string	Maximum length: 79	
service <name>	Destination services. Service name.	string	Maximum length: 79	

config user setting

Configure user authentication setting.

```
config user setting
    Description: Configure user authentication setting.
    set auth-type {option1}, {option2}, ...
    set auth-cert {string}
    set auth-ca-cert {string}
    set auth-secure-http [enable|disable]
    set auth-http-basic [enable|disable]
    set auth-ssl-allow-renegotiation [enable|disable]
    set auth-src-mac [enable|disable]
    set auth-on-demand [always|implicitly]
    set auth-portal-timeout {integer}
    set radius-ses-timeout-act [hard-timeout|ignore-timeout]
    set auth-blackout-time {integer}
    set auth-invalid-max {integer}
    set auth-lockout-threshold {integer}
    set auth-lockout-duration {integer}
    set per-policy-disclaimer [enable|disable]
    config auth-ports
        Description: Set up non-standard ports for authentication with HTTP, HTTPS, FTP, and
        TELNET.
        edit <id>
            set type [http|https|...]
            set port {integer}
        next
    end
    set auth-ssl-min-proto-version [default|SSLv3|...]
    set auth-ssl-max-proto-version [sslv3|tlsv1|...]
    set auth-ssl-sigalgs [no-rsa-pss|all]
end
```

config user setting

Parameter	Description	Type	Size	Default										
auth-type	Supported firewall policy authentication protocols/methods.	option	-	http https ftp telnet										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>Allow HTTP authentication.</td></tr><tr><td><i>https</i></td><td>Allow HTTPS authentication.</td></tr><tr><td><i>ftp</i></td><td>Allow FTP authentication.</td></tr><tr><td><i>telnet</i></td><td>Allow TELNET authentication.</td></tr></table>	Option	Description	<i>http</i>	Allow HTTP authentication.	<i>https</i>	Allow HTTPS authentication.	<i>ftp</i>	Allow FTP authentication.	<i>telnet</i>	Allow TELNET authentication.			
Option	Description													
<i>http</i>	Allow HTTP authentication.													
<i>https</i>	Allow HTTPS authentication.													
<i>ftp</i>	Allow FTP authentication.													
<i>telnet</i>	Allow TELNET authentication.													
auth-cert	HTTPS server certificate for policy authentication.	string	Maximum length: 35											
auth-ca-cert	HTTPS CA certificate for policy authentication.	string	Maximum length: 35											
auth-secure-http	Enable/disable redirecting HTTP user authentication to more secure HTTPS.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
auth-http-basic	Enable/disable use of HTTP basic authentication for identity-based firewall policies.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
auth-ssl-allow-renegotiation	Allow/forbid SSL re-negotiation for HTTPS authentication.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow SSL re-negotiation.</td></tr><tr><td><i>disable</i></td><td>Forbid SSL re-negotiation.</td></tr></table>	Option	Description	<i>enable</i>	Allow SSL re-negotiation.	<i>disable</i>	Forbid SSL re-negotiation.							
Option	Description													
<i>enable</i>	Allow SSL re-negotiation.													
<i>disable</i>	Forbid SSL re-negotiation.													
auth-src-mac	Enable/disable source MAC for user identity.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable source MAC for user identity.</td></tr></table>	Option	Description	<i>enable</i>	Enable source MAC for user identity.									
Option	Description													
<i>enable</i>	Enable source MAC for user identity.													

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable source MAC for user identity.</td></tr></table>	Option	Description	<i>disable</i>	Disable source MAC for user identity.					
	Option	Description								
<i>disable</i>	Disable source MAC for user identity.									
auth-on-demand	Always/implicitly trigger firewall authentication on demand.	option	-	implicitly						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>always</i></td><td>Always trigger firewall authentication on demand.</td></tr><tr><td><i>implicitly</i></td><td>Implicitly trigger firewall authentication on demand.</td></tr></table>	Option	Description	<i>always</i>	Always trigger firewall authentication on demand.	<i>implicitly</i>	Implicitly trigger firewall authentication on demand.			
	Option	Description								
	<i>always</i>	Always trigger firewall authentication on demand.								
<i>implicitly</i>	Implicitly trigger firewall authentication on demand.									
auth-portal-timeout	Time in minutes before captive portal user have to re-authenticate.	integer	Minimum value: 1 Maximum value: 30	3						
radius-ses-timeout-act	Set the RADIUS session timeout to a hard timeout or to ignore RADIUS server session timeouts.	option	-	hard-timeout						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hard-timeout</i></td><td>Use session timeout from RADIUS as hard-timeout.</td></tr><tr><td><i>ignore-timeout</i></td><td>Ignore session timeout from RADIUS.</td></tr></table>	Option	Description	<i>hard-timeout</i>	Use session timeout from RADIUS as hard-timeout.	<i>ignore-timeout</i>	Ignore session timeout from RADIUS.			
	Option	Description								
	<i>hard-timeout</i>	Use session timeout from RADIUS as hard-timeout.								
<i>ignore-timeout</i>	Ignore session timeout from RADIUS.									
auth-blackout-time	Time in seconds an IP address is denied access after failing to authenticate five times within one minute.	integer	Minimum value: 0 Maximum value: 3600	0						
auth-invalid-max	Maximum number of failed authentication attempts before the user is blocked.	integer	Minimum value: 1 Maximum value: 100	5						
auth-lockout-threshold	Maximum number of failed login attempts before login lockout is triggered.	integer	Minimum value: 1 Maximum value: 10	3						
auth-lockout-duration	Lockout period in seconds after too many login failures.	integer	Minimum value: 0 Maximum value: 4294967295	0						
per-policy-disclaimer	Enable/disable per policy disclaimer.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable per policy disclaimer.		
	<i>disable</i>	Disable per policy disclaimer.		
auth-ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default
	Option	Description		
	<i>default</i>	Follow system global setting.		
	<i>SSLv3</i>	SSLv3.		
	<i>TLSv1</i>	TLSv1.		
	<i>TLSv1-1</i>	TLSv1.1.		
	<i>TLSv1-2</i>	TLSv1.2.		
auth-ssl-max-proto-version	Maximum supported protocol version for SSL/TLS connections.	option	-	
	Option	Description		
	<i>ssl/v3</i>	SSLv3.		
	<i>tlsv1</i>	TLSv1.		
	<i>tlsv1-1</i>	TLSv1.1.		
	<i>tlsv1-2</i>	TLSv1.2.		
	<i>tlsv1-3</i>	TLSv1.3.		
auth-ssl-sigalgs	Set signature algorithms related to HTTPS authentication.	option	-	all
	Option	Description		
	<i>no-rsa-pss</i>	Disable RSA-PSS signature algorithms for HTTPS authentication.		
	<i>all</i>	Enable all supported signature algorithms for HTTPS authentication.		

config auth-ports

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
type	Service type.	option	-	http
	Option		Description	
	<i>http</i>		HTTP service.	
	<i>https</i>		HTTPS service.	
	<i>ftp</i>		FTP service.	
	<i>telnet</i>		TELNET service.	
port	Non-standard port for firewall user authentication.	integer	Minimum value: 1 Maximum value: 65535	1024

config user tacacs+

Configure TACACS+ server entries.

```
config user tacacs+
  Description: Configure TACACS+ server entries.
  edit <name>
    set server {string}
    set secondary-server {string}
    set tertiary-server {string}
    set port {integer}
    set key {password}
    set secondary-key {password}
    set tertiary-key {password}
    set authen-type [mschap|chap|...]
    set authorization [enable|disable]
    set source-ip {string}
    set interface-select-method [auto|specify]
    set interface {string}
  next
end
```

config user tacacs+

Parameter	Description	Type	Size	Default												
name	TACACS+ server entry name.	string	Maximum length: 35													
server	Primary TACACS+ server CN domain name or IP address.	string	Maximum length: 63													
secondary-server	Secondary TACACS+ server CN domain name or IP address.	string	Maximum length: 63													
tertiary-server	Tertiary TACACS+ server CN domain name or IP address.	string	Maximum length: 63													
port	Port number of the TACACS+ server.	integer	Minimum value: 1 Maximum value: 65535	49												
key	Key to access the primary server.	password	Not Specified													
secondary-key	Key to access the secondary server.	password	Not Specified													
tertiary-key	Key to access the tertiary server.	password	Not Specified													
authen-type	Allowed authentication protocols/methods.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mschap</i></td><td>MSCHAP.</td></tr><tr><td><i>chap</i></td><td>CHAP.</td></tr><tr><td><i>pap</i></td><td>PAP.</td></tr><tr><td><i>ascii</i></td><td>ASCII.</td></tr><tr><td><i>auto</i></td><td>Use PAP, MSCHAP, and CHAP (in that order).</td></tr></table>	Option	Description	<i>mschap</i>	MSCHAP.	<i>chap</i>	CHAP.	<i>pap</i>	PAP.	<i>ascii</i>	ASCII.	<i>auto</i>	Use PAP, MSCHAP, and CHAP (in that order).			
Option	Description															
<i>mschap</i>	MSCHAP.															
<i>chap</i>	CHAP.															
<i>pap</i>	PAP.															
<i>ascii</i>	ASCII.															
<i>auto</i>	Use PAP, MSCHAP, and CHAP (in that order).															
authorization	Enable/disable TACACS+ authorization.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ authorization.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ authorization.</td></tr></table>	Option	Description	<i>enable</i>	Enable TACACS+ authorization.	<i>disable</i>	Disable TACACS+ authorization.									
Option	Description															
<i>enable</i>	Enable TACACS+ authorization.															
<i>disable</i>	Disable TACACS+ authorization.															
source-ip	Source IP address for communications to TACACS+ server.	string	Maximum length: 63													

Parameter	Description	Type	Size	Default
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

videofilter

This section includes syntax for the following commands:

- [config videofilter profile on page 1070](#)
- [config videofilter youtube-channel-filter on page 1072](#)
- [config videofilter youtube-key on page 1074](#)

config videofilter profile

Configure VideoFilter profile.

```
config videofilter profile
  Description: Configure VideoFilter profile.
  edit <name>
    set comment {var-string}
    set default-action [allow|monitor|...]
    set log [enable|disable]
    set youtube-channel-filter {integer}
    config fortiguard-category
      Description: Configure FortiGuard categories.
      config filters
        Description: Configure VideoFilter FortiGuard category.
        edit <id>
          set action [allow|monitor|...]
          set category-id {integer}
          set log [enable|disable]
        next
      end
    end
    set youtube [enable|disable]
    set vimeo [enable|disable]
    set dailymotion [enable|disable]
    set replacemsg-group {string}
  next
end
```

config videofilter profile

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default								
default-action	Video filter default action.	option	-	monitor								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow videos to be accessed.</td></tr><tr><td><i>monitor</i></td><td>Monitor videos.</td></tr><tr><td><i>block</i></td><td>Block videos.</td></tr></table>	Option	Description	<i>allow</i>	Allow videos to be accessed.	<i>monitor</i>	Monitor videos.	<i>block</i>	Block videos.			
Option	Description											
<i>allow</i>	Allow videos to be accessed.											
<i>monitor</i>	Monitor videos.											
<i>block</i>	Block videos.											
log	Enable/disable logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging.</td></tr><tr><td><i>disable</i></td><td>Disable logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging.	<i>disable</i>	Disable logging.					
Option	Description											
<i>enable</i>	Enable logging.											
<i>disable</i>	Disable logging.											
youtube-channel-filter	Set YouTube channel filter.	integer	Minimum value: 0 Maximum value: 4294967295	0								
youtube	Enable/disable YouTube video source.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable YouTube source.</td></tr><tr><td><i>disable</i></td><td>Disable YouTube source.</td></tr></table>	Option	Description	<i>enable</i>	Enable YouTube source.	<i>disable</i>	Disable YouTube source.					
Option	Description											
<i>enable</i>	Enable YouTube source.											
<i>disable</i>	Disable YouTube source.											
vimeo	Enable/disable Vimeo video source.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Vimeo source.</td></tr><tr><td><i>disable</i></td><td>Disable Vimeo source.</td></tr></table>	Option	Description	<i>enable</i>	Enable Vimeo source.	<i>disable</i>	Disable Vimeo source.					
Option	Description											
<i>enable</i>	Enable Vimeo source.											
<i>disable</i>	Disable Vimeo source.											
dailymotion	Enable/disable Dailymotion video source.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Dailymotion source.</td></tr><tr><td><i>disable</i></td><td>Disable Dailymotion source.</td></tr></table>	Option	Description	<i>enable</i>	Enable Dailymotion source.	<i>disable</i>	Disable Dailymotion source.					
Option	Description											
<i>enable</i>	Enable Dailymotion source.											
<i>disable</i>	Disable Dailymotion source.											
replacemsg-group	Replacement message group.	string	Maximum length: 35									

config filters

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
action	VideoFilter action.	option	-	monitor
	OptionDescription			
	allow	Allow videos to be accessed.		
	monitor	Monitor videos.		
	block	Block videos.		
category-id	Category ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
log	Enable/disable logging.	option	-	enable
	OptionDescription			
	enable	Enable logging.		
	disable	Disable logging.		

config videofilter youtube-channel-filter

Configure YouTube channel filter.

```

config videofilter youtube-channel-filter
  Description: Configure YouTube channel filter.
  edit <id>
    set name {string}
    set comment {var-string}
    config entries
      Description: YouTube filter entries.
      edit <id>
        set comment {var-string}
        set action [allow|monitor|...]
        set channel-id {string}
      next
    end
  set log [enable|disable]

```



```

    next
end

```

config videofilter youtube-channel-filter

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
log	Enable/disable logging.	option	-	enable
	Option	Description		
	enable	Enable logging.		
	disable	Disable logging.		

config entries

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
comment	Comment.	var-string	Maximum length: 255	
action	YouTube channel filter action.	option	-	monitor
	Option	Description		
	allow	Allow videos to be accessed.		
	monitor	Monitor videos.		
	block	Block videos.		
channel-id	Channel ID.	string	Maximum length: 255	

config videofilter youtube-key

Configure YouTube API keys.

```
config videofilter youtube-key
    Description: Configure YouTube API keys.
    edit <id>
        set key {string}
    next
end
```

config videofilter youtube-key

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
key	Key.	string	Maximum length: 47	

vpn

This section includes syntax for the following commands:

- [config vpn certificate ca on page 1075](#)
- [config vpn certificate crl on page 1077](#)
- [config vpn certificate local on page 1078](#)
- [config vpn certificate ocsf-server on page 1082](#)
- [config vpn certificate remote on page 1083](#)
- [config vpn certificate setting on page 1084](#)
- [config vpn ipsec phase1-interface on page 1089](#)
- [config vpn ipsec phase2-interface on page 1104](#)

config vpn certificate ca

CA certificate.

```
config vpn certificate ca
  Description: CA certificate.
  edit <name>
    set ca {user}
    set range [global|vdom]
    set source [factory|user|...]
    set ssl-inspection-trusted [enable|disable]
    set scep-url {string}
    set auto-update-days {integer}
    set auto-update-days-warning {integer}
    set source-ip {ipv4-address}
    set ca-identifier {string}
    set obsolete [disable|enable]
  next
end
```

config vpn certificate ca

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 79	
ca	CA certificate as a PEM file.	user	Not Specified	
range	Either global or VDOM IP address range for the CA certificate.	option	-	vdom

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>global</i>	Global range.		
	<i>vdom</i>	VDOM IP address range.		
source	CA certificate source type.	option	-	user
	Option	Description		
	<i>factory</i>	Factory installed certificate.		
	<i>user</i>	User generated certificate.		
	<i>bundle</i>	Bundle file certificate.		
ssl-inspection-trusted	Enable/disable this CA as a trusted CA for SSL inspection.	option	-	enable
	Option	Description		
	<i>enable</i>	Trusted CA for SSL inspection.		
	<i>disable</i>	Untrusted CA for SSL inspection.		
scep-url	URL of the SCEP server.	string	Maximum length: 255	
auto-update-days	Number of days to wait before requesting an updated CA certificate.	integer	Minimum value: 0 Maximum value: 4294967295	0
auto-update-days-warning	Number of days before an expiry-warning message is generated.	integer	Minimum value: 0 Maximum value: 4294967295	0
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0
ca-identifier	CA identifier of the SCEP server.	string	Maximum length: 255	
obsolete	Enable/disable this CA as obsoleted.	option	-	disable
	Option	Description		
	<i>disable</i>	Alive.		
	<i>enable</i>	Obsolete.		

config vpn certificate crl

Certificate Revocation List as a PEM file.

```
config vpn certificate crl
    Description: Certificate Revocation List as a PEM file.
    edit <name>
        set crl {user}
        set range [global|vdom]
        set source [factory|user|...]
        set update-vdom {string}
        set ldap-server {string}
        set ldap-username {string}
        set ldap-password {password}
        set http-url {string}
        set scep-url {string}
        set scep-cert {string}
        set update-interval {integer}
        set source-ip {ipv4-address}
    next
end
```

config vpn certificate crl

Parameter	Description	Type	Size	Default								
name	Name.	string	Maximum length: 35									
crl	Certificate Revocation List as a PEM file.	user	Not Specified									
range	Either global or VDOM IP address range for the certificate.	option	-	vdom								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Global range.</td></tr><tr><td><i>vdom</i></td><td>VDOM IP address range.</td></tr></table>	Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.					
Option	Description											
<i>global</i>	Global range.											
<i>vdom</i>	VDOM IP address range.											
source	Certificate source type.	option	-	user								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>factory</i></td><td>Factory installed certificate.</td></tr><tr><td><i>user</i></td><td>User generated certificate.</td></tr><tr><td><i>bundle</i></td><td>Bundle file certificate.</td></tr></table>	Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.			
Option	Description											
<i>factory</i>	Factory installed certificate.											
<i>user</i>	User generated certificate.											
<i>bundle</i>	Bundle file certificate.											
update-vdom	VDOM for CRL update.	string	Maximum length: 31	root								

Parameter	Description	Type	Size	Default
ldap-server	LDAP server name for CRL auto-update.	string	Maximum length: 35	
ldap-username	LDAP server user name.	string	Maximum length: 63	
ldap-password	LDAP server user password.	password	Not Specified	
http-url	HTTP server URL for CRL auto-update.	string	Maximum length: 255	
scep-url	SCEP server URL for CRL auto-update.	string	Maximum length: 255	
scep-cert	Local certificate for SCEP communication for CRL auto-update.	string	Maximum length: 35	Fortinet_CA_SSL
update-interval	Time in seconds before the FortiProxy checks for an updated CRL. Set to 0 to update only when it expires.	integer	Minimum value: 0 Maximum value: 4294967295	0
source-ip	Source IP address for communications to a HTTP or SCEP CA server.	ipv4-address	Not Specified	0.0.0.0

config vpn certificate local

Local keys and certificates.

```

config vpn certificate local
    Description: Local keys and certificates.
    edit <name>
        set type [normal|hsm]
        set password {password}
        set hsm-vendor [safenet|primus]
        set hsm-slot {string}
        set hsm-keytype [rsa|ec]
        set comments {string}
        set private-key {user}
        set certificate {user}
        set csr {user}
        set state {user}
        set scep-url {string}
        set range [global|vdom]
        set source [factory|user|...]
        set auto-regenerate-days {integer}
        set auto-regenerate-days-warning {integer}
        set scep-password {password}
        set ca-identifier {string}
    
```

```

set name-encoding [printable|utf8]
set source-ip {ipv4-address}
set ike-localid {string}
set ike-localid-type [asn1dn|fqdn]
set enroll-protocol [none|scep|...]
set private-key-retain [enable|disable]
set cmp-server {string}
set cmp-path {string}
set cmp-server-cert {string}
set cmp-regeneration-method [keyupate|renewal]
set acme-ca-url {string}
set acme-domain {string}
set acme-email {string}
set acme-rsa-key-size {integer}
set acme-renew-window {integer}
next
end

```

config vpn certificate local

Parameter	Description	Type	Size	Default						
name	Name.	string	Maximum length: 35							
type	Type.	option	-	normal						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>normal</i></td><td>Normal</td></tr><tr><td><i>hsm</i></td><td>HSM</td></tr></table>				Option	Description	<i>normal</i>	Normal	<i>hsm</i>	HSM
	Option	Description								
	<i>normal</i>	Normal								
<i>hsm</i>	HSM									
password	Password as a PEM file.	password	Not Specified							
hsm-vendor	HSM vendor.	option	-	safenet						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>safenet</i></td><td>Safenet HSM.</td></tr><tr><td><i>primus</i></td><td>Securosys Primus HSM.</td></tr></table>				Option	Description	<i>safenet</i>	Safenet HSM.	<i>primus</i>	Securosys Primus HSM.
	Option	Description								
	<i>safenet</i>	Safenet HSM.								
<i>primus</i>	Securosys Primus HSM.									
hsm-slot	HSM slot to use with this certificate.	string	Maximum length: 35							
hsm-keytype	HSM certificate key type.	option	-	rsa						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rsa</i></td><td>RSA key type.</td></tr><tr><td><i>ec</i></td><td>EC key type.</td></tr></table>				Option	Description	<i>rsa</i>	RSA key type.	<i>ec</i>	EC key type.
	Option	Description								
	<i>rsa</i>	RSA key type.								
<i>ec</i>	EC key type.									

Parameter	Description	Type	Size	Default								
comments	Comment.	string	Maximum length: 511									
private-key	PEM format key encrypted with a password.	user	Not Specified									
certificate	PEM format certificate.	user	Not Specified									
csr	Certificate Signing Request.	user	Not Specified									
state	Certificate Signing Request State.	user	Not Specified									
scep-url	SCEP server URL.	string	Maximum length: 255									
range	Either a global or VDOM IP address range for the certificate.	option	-	vdom								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>global</td><td>Global range.</td></tr><tr><td>vdom</td><td>VDOM IP address range.</td></tr></table>				Option	Description	global	Global range.	vdom	VDOM IP address range.		
Option	Description											
global	Global range.											
vdom	VDOM IP address range.											
source	Certificate source type.	option	-	user								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>factory</td><td>Factory installed certificate.</td></tr><tr><td>user</td><td>User generated certificate.</td></tr><tr><td>bundle</td><td>Bundle file certificate.</td></tr></table>				Option	Description	factory	Factory installed certificate.	user	User generated certificate.	bundle	Bundle file certificate.
Option	Description											
factory	Factory installed certificate.											
user	User generated certificate.											
bundle	Bundle file certificate.											
auto-regenerate-days	Number of days to wait before expiry of an updated local certificate is requested (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0								
auto-regenerate-days-warning	Number of days to wait before an expiry warning message is generated (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0								
scep-password	SCEP server challenge password for auto-regeneration.	password	Not Specified									

Parameter	Description	Type	Size	Default
ca-identifier	CA identifier of the CA server for signing via SCEP.	string	Maximum length: 255	
name-encoding	Name encoding method for auto-regeneration.	option	-	printable
	Option		Description	
	printable	Printable encoding (default).		
	utf8	UTF-8 encoding.		
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0
ike-localid	Local ID the FortiProxy uses for authentication as a VPN client.	string	Maximum length: 63	
ike-localid-type	IKE local ID type.	option	-	asn1dn
	Option		Description	
	asn1dn	ASN.1 distinguished name.		
	fqdn	Fully qualified domain name.		
enroll-protocol	Certificate enrollment protocol.	option	-	none
	Option		Description	
	none	None (default).		
	scep	Simple Certificate Enrollment Protocol.		
	cmpv2	Certificate Management Protocol Version 2.		
	acme2	Automated Certificate Management Environment Version 2.		
private-key-retain	Enable/disable retention of private key during SCEP renewal.	option	-	disable
	Option		Description	
	enable	Keep the existing private key during SCEP renewal.		
	disable	Generate a new private key during SCEP renewal.		

Parameter	Description	Type	Size	Default						
cmp-server	Address and port for CMP server (format = address:port).	string	Maximum length: 63							
cmp-path	Path location inside CMP server.	string	Maximum length: 255							
cmp-server-cert	CMP server certificate.	string	Maximum length: 79							
cmp-regeneration-method	CMP auto-regeneration method.	option	-	keyupate						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>keyupate</i></td><td>Key Update.</td></tr><tr><td><i>renewal</i></td><td>Renewal.</td></tr></table>				Option	Description	<i>keyupate</i>	Key Update.	<i>renewal</i>	Renewal.
Option	Description									
<i>keyupate</i>	Key Update.									
<i>renewal</i>	Renewal.									
acme-ca-url	The URL for the ACME CA server.	string	Maximum length: 255	https://acme-v02.api.letsencrypt.org/directory						
acme-domain	A valid domain that resolves to this FortiProxy unit.	string	Maximum length: 255							
acme-email	Contact email address that is required by some CAs like LetsEncrypt.	string	Maximum length: 255							
acme-rsa-key-size	Length of the RSA private key of the generated cert (Minimum 2048 bits).	integer	Minimum value: 2048 Maximum value: 4096	2048						
acme-renew-window	Beginning of the renewal window.	integer	Minimum value: 1 Maximum value: 60	30						

config vpn certificate ocsf-server

OCSP server configuration.

```
config vpn certificate ocsf-server
  Description: OCSP server configuration.
  edit <name>
    set url {string}
    set cert {string}
    set secondary-url {string}
    set secondary-cert {string}
```

```

        set unavail-action [revoke|ignore]
        set source-ip {string}
    next
end

```

config vpn certificate ocsf-server

Parameter	Description	Type	Size	Default						
name	OCSP server entry name.	string	Maximum length: 35							
url	OCSP server URL.	string	Maximum length: 127							
cert	OCSP server certificate.	string	Maximum length: 127							
secondary-url	Secondary OCSP server URL.	string	Maximum length: 127							
secondary-cert	Secondary OCSP server certificate.	string	Maximum length: 127							
unavail-action	Action when server is unavailable (revoke the certificate or ignore the result of the check).	option	-	revoke						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>revoke</i></td><td>Revoke certificate if server is unavailable.</td></tr><tr><td><i>ignore</i></td><td>Ignore OCSP check if server is unavailable.</td></tr></table>				Option	Description	<i>revoke</i>	Revoke certificate if server is unavailable.	<i>ignore</i>	Ignore OCSP check if server is unavailable.
	Option	Description								
	<i>revoke</i>	Revoke certificate if server is unavailable.								
<i>ignore</i>	Ignore OCSP check if server is unavailable.									
source-ip	Source IP address for dynamic AIA and OCSP queries.	string	Maximum length: 63							

config vpn certificate remote

Remote certificate as a PEM file.

```

config vpn certificate remote
    Description: Remote certificate as a PEM file.
    edit <name>
        set remote {user}
        set range [global|vdom]
        set source [factory|user|...]
    next
end

```

config vpn certificate remote

Parameter	Description	Type	Size	Default								
name	Name.	string	Maximum length: 35									
remote	Remote certificate.	user	Not Specified									
range	Either the global or VDOM IP address range for the remote certificate.	option	-	vdom								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Global range.</td></tr><tr><td><i>vdom</i></td><td>VDOM IP address range.</td></tr></table>				Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.		
Option	Description											
<i>global</i>	Global range.											
<i>vdom</i>	VDOM IP address range.											
source	Remote certificate source type.	option	-	user								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>factory</i></td><td>Factory installed certificate.</td></tr><tr><td><i>user</i></td><td>User generated certificate.</td></tr><tr><td><i>bundle</i></td><td>Bundle file certificate.</td></tr></table>				Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.
Option	Description											
<i>factory</i>	Factory installed certificate.											
<i>user</i>	User generated certificate.											
<i>bundle</i>	Bundle file certificate.											

config vpn certificate setting

VPN certificate setting.

```

config vpn certificate setting
  Description: VPN certificate setting.
  set ocsdp-status [enable|disable]
  set ocsdp-option [certificate|server]
  set proxy {string}
  set proxy-port {integer}
  set proxy-username {string}
  set proxy-password {password}
  set source-ip {string}
  set ocsdp-default-server {string}
  set interface-select-method [auto|specify]
  set interface {string}
  set check-ca-cert [enable|disable]
  set check-ca-chain [enable|disable]
  set subject-match [substring|value]
  set subject-set [subset|superset]
  set cn-match [substring|value]
  set cn-allow-multi [disable|enable]
  config crl-verification
    Description: CRL verification options.
```

```

        set expiry [ignore|revoke]
        set leaf-crl-absence [ignore|revoke]
        set chain-crl-absence [ignore|revoke]
    end
    set strict-ocsp-check [enable|disable]
    set ssl-min-proto-version [default|SSLv3|...]
    set cmp-save-extra-certs [enable|disable]
    set cmp-key-usage-checking [enable|disable]
    set cert-expire-warning {integer}
    set certname-rsa1024 {string}
    set certname-rsa2048 {string}
    set certname-rsa4096 {string}
    set certname-dsa1024 {string}
    set certname-dsa2048 {string}
    set certname-ecdsa256 {string}
    set certname-ecdsa384 {string}
    set certname-ecdsa521 {string}
    set certname-ed25519 {string}
    set certname-ed448 {string}
end

```

config vpn certificate setting

Parameter	Description	Type	Size	Default
ocsp-status	Enable/disable receiving certificates using the OCSP.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ocsp-option	Specify whether the OCSP URL is from certificate or configured OCSP server.	option	-	server
	Option	Description		
	<i>certificate</i>	Use URL from certificate.		
	<i>server</i>	Use URL from configured OCSP server.		
proxy	Proxy server FQDN or IP for OCSP/CA queries during certificate verification.	string	Maximum length: 127	
proxy-port	Proxy server port.	integer	Minimum value: 1 Maximum value: 65535	8080
proxy-username	Proxy server user name.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default						
proxy-password	Proxy server password.	password	Not Specified							
source-ip	Source IP address for dynamic AIA and OCSP queries.	string	Maximum length: 63							
ocsp-default-server	Default OCSP server.	string	Maximum length: 35							
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	auto	Set outgoing interface automatically.	specify	Set outgoing interface manually.
Option	Description									
auto	Set outgoing interface automatically.									
specify	Set outgoing interface manually.									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15							
check-ca-cert	Enable/disable verification of the user certificate and pass authentication if any CA in the chain is trusted.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable verification of the user certificate.</td></tr><tr><td>disable</td><td>Disable verification of the user certificate.</td></tr></table>				Option	Description	enable	Enable verification of the user certificate.	disable	Disable verification of the user certificate.
Option	Description									
enable	Enable verification of the user certificate.									
disable	Disable verification of the user certificate.									
check-ca-chain	Enable/disable verification of the entire certificate chain and pass authentication only if the chain is complete and all of the CAs in the chain are trusted.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable verification of the entire certificate chain.</td></tr><tr><td>disable</td><td>Disable verification of the entire certificate chain.</td></tr></table>				Option	Description	enable	Enable verification of the entire certificate chain.	disable	Disable verification of the entire certificate chain.
Option	Description									
enable	Enable verification of the entire certificate chain.									
disable	Disable verification of the entire certificate chain.									
subject-match	When searching for a matching certificate, control how to do RDN value matching with certificate subject name.	option	-	substring						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>substring</td><td>Find a match if the name being searched for is a part or the same as a certificate subject RDN.</td></tr><tr><td>value</td><td>Find a match if the name being searched for is same as a certificate subject RDN.</td></tr></table>				Option	Description	substring	Find a match if the name being searched for is a part or the same as a certificate subject RDN.	value	Find a match if the name being searched for is same as a certificate subject RDN.
Option	Description									
substring	Find a match if the name being searched for is a part or the same as a certificate subject RDN.									
value	Find a match if the name being searched for is same as a certificate subject RDN.									

Parameter	Description	Type	Size	Default												
subject-set	When searching for a matching certificate, control how to do RDN set matching with certificate subject name.	option	-	subset												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>subset</i></td><td>Find a match if the name being searched for is a subset of a certificate subject.</td></tr><tr><td><i>superset</i></td><td>Find a match if the name being searched for is a superset of a certificate subject.</td></tr></table>	Option	Description	<i>subset</i>	Find a match if the name being searched for is a subset of a certificate subject.	<i>superset</i>	Find a match if the name being searched for is a superset of a certificate subject.									
Option	Description															
<i>subset</i>	Find a match if the name being searched for is a subset of a certificate subject.															
<i>superset</i>	Find a match if the name being searched for is a superset of a certificate subject.															
cn-match	When searching for a matching certificate, control how to do CN value matching with certificate subject name.	option	-	substring												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>substring</i></td><td>Find a match if the name being searched for is a part or the same as a certificate CN.</td></tr><tr><td><i>value</i></td><td>Find a match if the name being searched for is same as a certificate CN.</td></tr></table>	Option	Description	<i>substring</i>	Find a match if the name being searched for is a part or the same as a certificate CN.	<i>value</i>	Find a match if the name being searched for is same as a certificate CN.									
Option	Description															
<i>substring</i>	Find a match if the name being searched for is a part or the same as a certificate CN.															
<i>value</i>	Find a match if the name being searched for is same as a certificate CN.															
cn-allow-multi	When searching for a matching certificate, allow multiple CN fields in certificate subject name.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Does not allow multiple CN entries in certificate matching.</td></tr><tr><td><i>enable</i></td><td>Allow multiple CN entries in certificate matching.</td></tr></table>	Option	Description	<i>disable</i>	Does not allow multiple CN entries in certificate matching.	<i>enable</i>	Allow multiple CN entries in certificate matching.									
Option	Description															
<i>disable</i>	Does not allow multiple CN entries in certificate matching.															
<i>enable</i>	Allow multiple CN entries in certificate matching.															
strict-ocsp-check	Enable/disable strict mode OCSP checking.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable strict mode OCSP checking.</td></tr><tr><td><i>disable</i></td><td>Disable strict mode OCSP checking.</td></tr></table>	Option	Description	<i>enable</i>	Enable strict mode OCSP checking.	<i>disable</i>	Disable strict mode OCSP checking.									
Option	Description															
<i>enable</i>	Enable strict mode OCSP checking.															
<i>disable</i>	Disable strict mode OCSP checking.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															

Parameter	Description	Type	Size	Default						
cmp-save-extra-certs	Enable/disable saving extra certificates in CMP mode.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable saving extra certificates in CMP mode.</td></tr><tr><td><i>disable</i></td><td>Disable saving extra certificates in CMP mode.</td></tr></table>				Option	Description	<i>enable</i>	Enable saving extra certificates in CMP mode.	<i>disable</i>	Disable saving extra certificates in CMP mode.
Option	Description									
<i>enable</i>	Enable saving extra certificates in CMP mode.									
<i>disable</i>	Disable saving extra certificates in CMP mode.									
cmp-key-usage-checking	Enable/disable server certificate key usage checking in CMP mode.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable server certificate key usage checking in CMP mode.</td></tr><tr><td><i>disable</i></td><td>Disable server certificate key usage checking in CMP mode.</td></tr></table>				Option	Description	<i>enable</i>	Enable server certificate key usage checking in CMP mode.	<i>disable</i>	Disable server certificate key usage checking in CMP mode.
Option	Description									
<i>enable</i>	Enable server certificate key usage checking in CMP mode.									
<i>disable</i>	Disable server certificate key usage checking in CMP mode.									
cert-expire-warning	Number of days before a certificate expires to send a warning. Set to 0 to disable sending of the warning.	integer	Minimum value: 0 Maximum value: 100	14						
certname-rsa1024	1024 bit RSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_RSA1024						
certname-rsa2048	2048 bit RSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_RSA2048						
certname-rsa4096	4096 bit RSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_RSA4096						
certname-dsa1024	1024 bit DSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_DSA1024						
certname-dsa2048	2048 bit DSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_DSA2048						
certname-ecdsa256	256 bit ECDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ECDSA256						
certname-ecdsa384	384 bit ECDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ECDSA384						

Parameter	Description	Type	Size	Default
certname-ecdsa521	521 bit ECDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ECDSA521
certname-ed25519	253 bit EdDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ED25519
certname-ed448	456 bit EdDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ED448

config curl-verification

Parameter	Description	Type	Size	Default						
expiry	CRL verification option when CRL is expired.	option	-	ignore						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ignore</td><td>Certificate status will be verified even if CRL is expired.</td></tr><tr><td>revoke</td><td>Certificate will be revoked if CRL is expired.</td></tr></table>	Option	Description	ignore	Certificate status will be verified even if CRL is expired.	revoke	Certificate will be revoked if CRL is expired.			
Option	Description									
ignore	Certificate status will be verified even if CRL is expired.									
revoke	Certificate will be revoked if CRL is expired.									
leaf-crl-absence	CRL verification option when leaf CRL is absent.	option	-	ignore						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ignore</td><td>CRL verification against leaf certificate is ignored if CRL is absent.</td></tr><tr><td>revoke</td><td>Certificate will be revoked if CRL of leaf certificate is absent.</td></tr></table>	Option	Description	ignore	CRL verification against leaf certificate is ignored if CRL is absent.	revoke	Certificate will be revoked if CRL of leaf certificate is absent.			
Option	Description									
ignore	CRL verification against leaf certificate is ignored if CRL is absent.									
revoke	Certificate will be revoked if CRL of leaf certificate is absent.									
chain-crl-absence	CRL verification option when CRL of any certificate in chain is absent.	option	-	ignore						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ignore</td><td>CRL verification is ignored if CRL of any certificate in chain is absent.</td></tr><tr><td>revoke</td><td>Certificate will be revoked if CRL of any certificate in chain is absent.</td></tr></table>	Option	Description	ignore	CRL verification is ignored if CRL of any certificate in chain is absent.	revoke	Certificate will be revoked if CRL of any certificate in chain is absent.			
Option	Description									
ignore	CRL verification is ignored if CRL of any certificate in chain is absent.									
revoke	Certificate will be revoked if CRL of any certificate in chain is absent.									

config vpn ipsec phase1-interface

Configure VPN remote gateway.

```
config vpn ipsec phase1-interface
    Description: Configure VPN remote gateway.
    edit <name>
        set interface {string}
```

```
set ike-version [1|2]
set local-gw {ipv4-address}
set remote-gw {ipv4-address}
set keylife {integer}
set certificate <name1>, <name2>, ...
set authmethod [psk|signature]
set mode [aggressive|main]
set peertype {option}
set peerid {string}
set peer {string}
set packet-redistribution [enable|disable]
set proposal {option1}, {option2}, ...
set psksecret {password-3}
set keepalive {integer}
set distance {integer}
set priority {integer}
set localid {string}
set localid-type [auto|fqdn|...]
set negotiate-timeout {integer}
set fragmentation [enable|disable]
set comments {var-string}
set send-cert-chain [enable|disable]
set dhgrp {option1}, {option2}, ...
set eap [enable|disable]
set eap-identity [use-id-payload|send-request]
set eap-exclude-peergrp {string}
set acct-verify [enable|disable]
set ppk [disable|allow|...]
set ppk-secret {password-3}
set ppk-identity {string}
set wizard-type [custom|dialup-forticlient|...]
set xauthtype [disable|client|...]
set reauth [disable|enable]
set authusr {string}
set authpasswd {password}
set group-authentication [enable|disable]
set group-authentication-secret {password-3}
set authusrgrp {string}
set idle-timeout [enable|disable]
set idle-timeoutinterval {integer}
set fgsp-sync [enable|disable]
set inbound-dscp-copy [enable|disable]
set auto-discovery-sender [enable|disable]
set auto-discovery-receiver [enable|disable]
set auto-discovery-forwarder [enable|disable]
set auto-discovery-psk [enable|disable]
set auto-discovery-shortcuts [independent|dependent]
set auto-discovery-crossover [allow|block]
set auto-discovery-offer-interval {integer}
set fragmentation-mtu {integer}
set childless-ike [enable|disable]
set azure-ad-autoconnect [enable|disable]
set rekey [enable|disable]
set digital-signature-auth [enable|disable]
set signature-hash-alg {option1}, {option2}, ...
set rsa-signature-format [pkcs1|pss]
```

```

set rsa-signature-hash-override [enable|disable]
set enforce-unique-id [disable|keep-new|...]
set cert-id-validation [enable|disable]
set network-overlay [disable|enable]
set network-id {integer}
set dev-id-notification [disable|enable]
set dev-id {string}
set loopback-asymroute [enable|disable]
set link-cost {integer}
set exchange-fgt-device-id [enable|disable]
set ems-sn-check [enable|disable]
set remote-gw-match [any|ipmask|...]
set remote-gw-subnet {ipv4-classnet-any}
set remote-gw-start-ip {ipv4-address-any}
set remote-gw-end-ip {ipv4-address-any}
set remote-gw-country {string}
set remote-gw6-match [any|ipprefix|...]
set remote-gw6-subnet {ipv6-network}
set remote-gw6-start-ip {ipv6-address}
set remote-gw6-end-ip {ipv6-address}
set remote-gw6-country {string}
set cert-trust-store [local|ems]
next
end

```

config vpn ipsec phase1-interface

Parameter	Description	Type	Size	Default						
name	IPsec remote gateway name.	string	Maximum length: 15							
interface	Local physical, aggregate, or VLAN outgoing interface.	string	Maximum length: 35							
ike-version	IKE protocol version.	option	-	1						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Use IKEv1 protocol.</td></tr><tr><td>2</td><td>Use IKEv2 protocol.</td></tr></table>				Option	Description	1	Use IKEv1 protocol.	2	Use IKEv2 protocol.
	Option	Description								
	1	Use IKEv1 protocol.								
2	Use IKEv2 protocol.									
local-gw	IPv4 address of the local gateway's external interface.	ipv4-address	Not Specified	0.0.0.0						
remote-gw	IPv4 address of the remote gateway's external interface.	ipv4-address	Not Specified	0.0.0.0						
keylife	Time to wait in seconds before phase 1 encryption key expires.	integer	Minimum value: 120 Maximum value: 172800	86400						

Parameter	Description	Type	Size	Default										
certificate <name>	The names of up to 4 signed personal certificates. Certificate name.	string	Maximum length: 79											
authmethod	Authentication method.	option	-	psk										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>psk</i></td><td>PSK authentication method.</td></tr><tr><td><i>signature</i></td><td>Signature authentication method.</td></tr></table>	Option	Description	<i>psk</i>	PSK authentication method.	<i>signature</i>	Signature authentication method.							
Option	Description													
<i>psk</i>	PSK authentication method.													
<i>signature</i>	Signature authentication method.													
mode	The ID protection mode used to establish a secure channel.	option	-	main										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>aggressive</i></td><td>Aggressive mode.</td></tr><tr><td><i>main</i></td><td>Main mode.</td></tr></table>	Option	Description	<i>aggressive</i>	Aggressive mode.	<i>main</i>	Main mode.							
Option	Description													
<i>aggressive</i>	Aggressive mode.													
<i>main</i>	Main mode.													
peertype	Accept this peer type.	option	-											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Accept any peer ID.</td></tr></table>	Option	Description	<i>any</i>	Accept any peer ID.									
Option	Description													
<i>any</i>	Accept any peer ID.													
peerid	Accept this peer identity.	string	Maximum length: 255											
peer	Accept this peer certificate.	string	Maximum length: 35											
packet-redistribution	Enable/disable packet distribution (RPS) on the IPsec interface.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable packet redistribution.</td></tr><tr><td><i>disable</i></td><td>Disable packet redistribution.</td></tr></table>	Option	Description	<i>enable</i>	Enable packet redistribution.	<i>disable</i>	Disable packet redistribution.							
Option	Description													
<i>enable</i>	Enable packet redistribution.													
<i>disable</i>	Disable packet redistribution.													
proposal	Phase1 proposal.	option	-											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>des-md5</i></td><td>des-md5</td></tr><tr><td><i>des-sha1</i></td><td>des-sha1</td></tr><tr><td><i>des-sha256</i></td><td>des-sha256</td></tr><tr><td><i>des-sha384</i></td><td>des-sha384</td></tr></table>	Option	Description	<i>des-md5</i>	des-md5	<i>des-sha1</i>	des-sha1	<i>des-sha256</i>	des-sha256	<i>des-sha384</i>	des-sha384			
Option	Description													
<i>des-md5</i>	des-md5													
<i>des-sha1</i>	des-sha1													
<i>des-sha256</i>	des-sha256													
<i>des-sha384</i>	des-sha384													

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>des-sha512</i>	des-sha512		
	<i>3des-md5</i>	3des-md5		
	<i>3des-sha1</i>	3des-sha1		
	<i>3des-sha256</i>	3des-sha256		
	<i>3des-sha384</i>	3des-sha384		
	<i>3des-sha512</i>	3des-sha512		
	<i>aes128-md5</i>	aes128-md5		
	<i>aes128-sha1</i>	aes128-sha1		
	<i>aes128-sha256</i>	aes128-sha256		
	<i>aes128-sha384</i>	aes128-sha384		
	<i>aes128-sha512</i>	aes128-sha512		
	<i>aes128gcm-prfsha1</i>	aes128gcm-prfsha1		
	<i>aes128gcm-prfsha256</i>	aes128gcm-prfsha256		
	<i>aes128gcm-prfsha384</i>	aes128gcm-prfsha384		
	<i>aes128gcm-prfsha512</i>	aes128gcm-prfsha512		
	<i>aes192-md5</i>	aes192-md5		
	<i>aes192-sha1</i>	aes192-sha1		
	<i>aes192-sha256</i>	aes192-sha256		
	<i>aes192-sha384</i>	aes192-sha384		
	<i>aes192-sha512</i>	aes192-sha512		
	<i>aes256-md5</i>	aes256-md5		
	<i>aes256-sha1</i>	aes256-sha1		
	<i>aes256-sha256</i>	aes256-sha256		
	<i>aes256-sha384</i>	aes256-sha384		
	<i>aes256-sha512</i>	aes256-sha512		
	<i>aes256gcm-prfsha1</i>	aes256gcm-prfsha1		
	<i>aes256gcm-prfsha256</i>	aes256gcm-prfsha256		
	<i>aes256gcm-prfsha384</i>	aes256gcm-prfsha384		
	<i>aes256gcm-prfsha512</i>	aes256gcm-prfsha512		

Parameter	Description	Type	Size	Default																																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>chacha20poly1305-prfsha1</i></td><td>chacha20poly1305-prfsha1</td></tr><tr><td><i>chacha20poly1305-prfsha256</i></td><td>chacha20poly1305-prfsha256</td></tr><tr><td><i>chacha20poly1305-prfsha384</i></td><td>chacha20poly1305-prfsha384</td></tr><tr><td><i>chacha20poly1305-prfsha512</i></td><td>chacha20poly1305-prfsha512</td></tr><tr><td><i>aria128-md5</i></td><td>aria128-md5</td></tr><tr><td><i>aria128-sha1</i></td><td>aria128-sha1</td></tr><tr><td><i>aria128-sha256</i></td><td>aria128-sha256</td></tr><tr><td><i>aria128-sha384</i></td><td>aria128-sha384</td></tr><tr><td><i>aria128-sha512</i></td><td>aria128-sha512</td></tr><tr><td><i>aria192-md5</i></td><td>aria192-md5</td></tr><tr><td><i>aria192-sha1</i></td><td>aria192-sha1</td></tr><tr><td><i>aria192-sha256</i></td><td>aria192-sha256</td></tr><tr><td><i>aria192-sha384</i></td><td>aria192-sha384</td></tr><tr><td><i>aria192-sha512</i></td><td>aria192-sha512</td></tr><tr><td><i>aria256-md5</i></td><td>aria256-md5</td></tr><tr><td><i>aria256-sha1</i></td><td>aria256-sha1</td></tr><tr><td><i>aria256-sha256</i></td><td>aria256-sha256</td></tr><tr><td><i>aria256-sha384</i></td><td>aria256-sha384</td></tr><tr><td><i>aria256-sha512</i></td><td>aria256-sha512</td></tr><tr><td><i>seed-md5</i></td><td>seed-md5</td></tr><tr><td><i>seed-sha1</i></td><td>seed-sha1</td></tr><tr><td><i>seed-sha256</i></td><td>seed-sha256</td></tr><tr><td><i>seed-sha384</i></td><td>seed-sha384</td></tr><tr><td><i>seed-sha512</i></td><td>seed-sha512</td></tr></table>	Option	Description	<i>chacha20poly1305-prfsha1</i>	chacha20poly1305-prfsha1	<i>chacha20poly1305-prfsha256</i>	chacha20poly1305-prfsha256	<i>chacha20poly1305-prfsha384</i>	chacha20poly1305-prfsha384	<i>chacha20poly1305-prfsha512</i>	chacha20poly1305-prfsha512	<i>aria128-md5</i>	aria128-md5	<i>aria128-sha1</i>	aria128-sha1	<i>aria128-sha256</i>	aria128-sha256	<i>aria128-sha384</i>	aria128-sha384	<i>aria128-sha512</i>	aria128-sha512	<i>aria192-md5</i>	aria192-md5	<i>aria192-sha1</i>	aria192-sha1	<i>aria192-sha256</i>	aria192-sha256	<i>aria192-sha384</i>	aria192-sha384	<i>aria192-sha512</i>	aria192-sha512	<i>aria256-md5</i>	aria256-md5	<i>aria256-sha1</i>	aria256-sha1	<i>aria256-sha256</i>	aria256-sha256	<i>aria256-sha384</i>	aria256-sha384	<i>aria256-sha512</i>	aria256-sha512	<i>seed-md5</i>	seed-md5	<i>seed-sha1</i>	seed-sha1	<i>seed-sha256</i>	seed-sha256	<i>seed-sha384</i>	seed-sha384	<i>seed-sha512</i>	seed-sha512				
	Option	Description																																																					
	<i>chacha20poly1305-prfsha1</i>	chacha20poly1305-prfsha1																																																					
	<i>chacha20poly1305-prfsha256</i>	chacha20poly1305-prfsha256																																																					
	<i>chacha20poly1305-prfsha384</i>	chacha20poly1305-prfsha384																																																					
	<i>chacha20poly1305-prfsha512</i>	chacha20poly1305-prfsha512																																																					
	<i>aria128-md5</i>	aria128-md5																																																					
	<i>aria128-sha1</i>	aria128-sha1																																																					
	<i>aria128-sha256</i>	aria128-sha256																																																					
	<i>aria128-sha384</i>	aria128-sha384																																																					
	<i>aria128-sha512</i>	aria128-sha512																																																					
	<i>aria192-md5</i>	aria192-md5																																																					
	<i>aria192-sha1</i>	aria192-sha1																																																					
	<i>aria192-sha256</i>	aria192-sha256																																																					
	<i>aria192-sha384</i>	aria192-sha384																																																					
	<i>aria192-sha512</i>	aria192-sha512																																																					
	<i>aria256-md5</i>	aria256-md5																																																					
	<i>aria256-sha1</i>	aria256-sha1																																																					
	<i>aria256-sha256</i>	aria256-sha256																																																					
	<i>aria256-sha384</i>	aria256-sha384																																																					
	<i>aria256-sha512</i>	aria256-sha512																																																					
	<i>seed-md5</i>	seed-md5																																																					
	<i>seed-sha1</i>	seed-sha1																																																					
	<i>seed-sha256</i>	seed-sha256																																																					
<i>seed-sha384</i>	seed-sha384																																																						
<i>seed-sha512</i>	seed-sha512																																																						
psksecret	Pre-shared secret for PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified																																																				
keepalive	NAT-T keep alive interval.	integer	Minimum value: 10 Maximum value: 900	10																																																			

Parameter	Description	Type	Size	Default														
distance	Distance for routes added by IKE.	integer	Minimum value: 1 Maximum value: 255	15														
priority	Priority for routes added by IKE.	integer	Minimum value: 1 Maximum value: 65535	1														
localid	Local ID.	string	Maximum length: 63															
localid-type	Local ID type.	option	-	auto														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Select ID type automatically.</td></tr><tr><td><i>fqdn</i></td><td>Use fully qualified domain name.</td></tr><tr><td><i>user-fqdn</i></td><td>Use user fully qualified domain name.</td></tr><tr><td><i>keyid</i></td><td>Use key-id string.</td></tr><tr><td><i>address</i></td><td>Use local IP address.</td></tr><tr><td><i>asn1dn</i></td><td>Use ASN.1 distinguished name.</td></tr></table>	Option	Description	<i>auto</i>	Select ID type automatically.	<i>fqdn</i>	Use fully qualified domain name.	<i>user-fqdn</i>	Use user fully qualified domain name.	<i>keyid</i>	Use key-id string.	<i>address</i>	Use local IP address.	<i>asn1dn</i>	Use ASN.1 distinguished name.			
Option	Description																	
<i>auto</i>	Select ID type automatically.																	
<i>fqdn</i>	Use fully qualified domain name.																	
<i>user-fqdn</i>	Use user fully qualified domain name.																	
<i>keyid</i>	Use key-id string.																	
<i>address</i>	Use local IP address.																	
<i>asn1dn</i>	Use ASN.1 distinguished name.																	
negotiate-timeout	IKE SA negotiation timeout in seconds.	integer	Minimum value: 1 Maximum value: 300	30														
fragmentation	Enable/disable fragment IKE message on re-transmission.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable intra-IKE fragmentation support on re-transmission.</td></tr><tr><td><i>disable</i></td><td>Disable intra-IKE fragmentation support.</td></tr></table>	Option	Description	<i>enable</i>	Enable intra-IKE fragmentation support on re-transmission.	<i>disable</i>	Disable intra-IKE fragmentation support.											
Option	Description																	
<i>enable</i>	Enable intra-IKE fragmentation support on re-transmission.																	
<i>disable</i>	Disable intra-IKE fragmentation support.																	
comments	Comment.	var-string	Maximum length: 255															
send-cert-chain	Enable/disable sending certificate chain.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending certificate chain.</td></tr><tr><td><i>disable</i></td><td>Disable sending certificate chain.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending certificate chain.	<i>disable</i>	Disable sending certificate chain.											
Option	Description																	
<i>enable</i>	Enable sending certificate chain.																	
<i>disable</i>	Disable sending certificate chain.																	
dhgrp	DH group.	option	-	14														

Parameter	Description	Type	Size	Default																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>DH Group 1.</td></tr><tr><td>2</td><td>DH Group 2.</td></tr><tr><td>5</td><td>DH Group 5.</td></tr><tr><td>14</td><td>DH Group 14.</td></tr><tr><td>15</td><td>DH Group 15.</td></tr><tr><td>16</td><td>DH Group 16.</td></tr><tr><td>17</td><td>DH Group 17.</td></tr><tr><td>18</td><td>DH Group 18.</td></tr><tr><td>19</td><td>DH Group 19.</td></tr><tr><td>20</td><td>DH Group 20.</td></tr><tr><td>21</td><td>DH Group 21.</td></tr><tr><td>27</td><td>DH Group 27.</td></tr><tr><td>28</td><td>DH Group 28.</td></tr><tr><td>29</td><td>DH Group 29.</td></tr><tr><td>30</td><td>DH Group 30.</td></tr><tr><td>31</td><td>DH Group 31.</td></tr><tr><td>32</td><td>DH Group 32.</td></tr></table>	Option	Description	1	DH Group 1.	2	DH Group 2.	5	DH Group 5.	14	DH Group 14.	15	DH Group 15.	16	DH Group 16.	17	DH Group 17.	18	DH Group 18.	19	DH Group 19.	20	DH Group 20.	21	DH Group 21.	27	DH Group 27.	28	DH Group 28.	29	DH Group 29.	30	DH Group 30.	31	DH Group 31.	32	DH Group 32.			
	Option	Description																																						
	1	DH Group 1.																																						
	2	DH Group 2.																																						
	5	DH Group 5.																																						
	14	DH Group 14.																																						
	15	DH Group 15.																																						
	16	DH Group 16.																																						
	17	DH Group 17.																																						
	18	DH Group 18.																																						
	19	DH Group 19.																																						
	20	DH Group 20.																																						
	21	DH Group 21.																																						
	27	DH Group 27.																																						
	28	DH Group 28.																																						
	29	DH Group 29.																																						
	30	DH Group 30.																																						
	31	DH Group 31.																																						
	32	DH Group 32.																																						
eap	Enable/disable IKEv2 EAP authentication.	option	-	disable																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IKEv2 EAP authentication.</td></tr><tr><td>disable</td><td>Disable IKEv2 EAP authentication.</td></tr></table>	Option	Description	enable	Enable IKEv2 EAP authentication.	disable	Disable IKEv2 EAP authentication.																																	
	Option	Description																																						
	enable	Enable IKEv2 EAP authentication.																																						
disable	Disable IKEv2 EAP authentication.																																							
eap-identity	IKEv2 EAP peer identity type.	option	-	use-id-payload																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>use-id-payload</td><td>Use IKEv2 IDi payload to resolve peer identity.</td></tr><tr><td>send-request</td><td>Use EAP identity request to resolve peer identity.</td></tr></table>	Option	Description	use-id-payload	Use IKEv2 IDi payload to resolve peer identity.	send-request	Use EAP identity request to resolve peer identity.																																	
	Option	Description																																						
	use-id-payload	Use IKEv2 IDi payload to resolve peer identity.																																						
send-request	Use EAP identity request to resolve peer identity.																																							
eap-exclude-peergrp	Peer group excluded from EAP authentication.	string	Maximum length: 35																																					
acct-verify	Enable/disable verification of RADIUS accounting record.	option	-	disable																																				

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable verification of RADIUS accounting record.</td></tr><tr><td><i>disable</i></td><td>Disable verification of RADIUS accounting record.</td></tr></table>	Option	Description	<i>enable</i>	Enable verification of RADIUS accounting record.	<i>disable</i>	Disable verification of RADIUS accounting record.																									
	Option	Description																														
	<i>enable</i>	Enable verification of RADIUS accounting record.																														
<i>disable</i>	Disable verification of RADIUS accounting record.																															
ppk	Enable/disable IKEv2 Postquantum Preshared Key (PPK).	option	-	disable																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use of IKEv2 Postquantum Preshared Key (PPK).</td></tr><tr><td><i>allow</i></td><td>Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).</td></tr><tr><td><i>require</i></td><td>Require use of IKEv2 Postquantum Preshared Key (PPK).</td></tr></table>	Option	Description	<i>disable</i>	Disable use of IKEv2 Postquantum Preshared Key (PPK).	<i>allow</i>	Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).	<i>require</i>	Require use of IKEv2 Postquantum Preshared Key (PPK).																							
	Option	Description																														
	<i>disable</i>	Disable use of IKEv2 Postquantum Preshared Key (PPK).																														
	<i>allow</i>	Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).																														
<i>require</i>	Require use of IKEv2 Postquantum Preshared Key (PPK).																															
ppk-secret	IKEv2 Postquantum Preshared Key (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified																													
ppk-identity	IKEv2 Postquantum Preshared Key Identity.	string	Maximum length: 35																													
wizard-type	GUI VPN Wizard Type.	option	-	custom																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>custom</i></td><td>Custom VPN configuration.</td></tr><tr><td><i>dialup-forticlient</i></td><td>Dial Up - FortiClient Windows, Mac and Android.</td></tr><tr><td><i>dialup-ios</i></td><td>Dial Up - iPhone / iPad Native IPsec Client.</td></tr><tr><td><i>dialup-android</i></td><td>Dial Up - Android Native IPsec Client.</td></tr><tr><td><i>dialup-windows</i></td><td>Dial Up - Windows Native IPsec Client.</td></tr><tr><td><i>dialup-cisco</i></td><td>Dial Up - Cisco IPsec Client.</td></tr><tr><td><i>static-fortiproxy</i></td><td>Site to Site - FortiProxy.</td></tr><tr><td><i>dialup-fortiproxy</i></td><td>Dial Up - FortiProxy.</td></tr><tr><td><i>static-cisco</i></td><td>Site to Site - Cisco.</td></tr><tr><td><i>dialup-cisco-fw</i></td><td>Dialup Up - Cisco Firewall.</td></tr><tr><td><i>simplified-static-fortiproxy</i></td><td>Site to Site - FortiProxy (SD-WAN).</td></tr><tr><td><i>hub-fortiproxy-auto-discovery</i></td><td>Hub role in a Hub-and-Spoke auto-discovery VPN.</td></tr><tr><td><i>spoke-fortiproxy-auto-discovery</i></td><td>Spoke role in a Hub-and-Spoke auto-discovery VPN.</td></tr></table>	Option	Description	<i>custom</i>	Custom VPN configuration.	<i>dialup-forticlient</i>	Dial Up - FortiClient Windows, Mac and Android.	<i>dialup-ios</i>	Dial Up - iPhone / iPad Native IPsec Client.	<i>dialup-android</i>	Dial Up - Android Native IPsec Client.	<i>dialup-windows</i>	Dial Up - Windows Native IPsec Client.	<i>dialup-cisco</i>	Dial Up - Cisco IPsec Client.	<i>static-fortiproxy</i>	Site to Site - FortiProxy.	<i>dialup-fortiproxy</i>	Dial Up - FortiProxy.	<i>static-cisco</i>	Site to Site - Cisco.	<i>dialup-cisco-fw</i>	Dialup Up - Cisco Firewall.	<i>simplified-static-fortiproxy</i>	Site to Site - FortiProxy (SD-WAN).	<i>hub-fortiproxy-auto-discovery</i>	Hub role in a Hub-and-Spoke auto-discovery VPN.	<i>spoke-fortiproxy-auto-discovery</i>	Spoke role in a Hub-and-Spoke auto-discovery VPN.			
	Option	Description																														
	<i>custom</i>	Custom VPN configuration.																														
	<i>dialup-forticlient</i>	Dial Up - FortiClient Windows, Mac and Android.																														
	<i>dialup-ios</i>	Dial Up - iPhone / iPad Native IPsec Client.																														
	<i>dialup-android</i>	Dial Up - Android Native IPsec Client.																														
	<i>dialup-windows</i>	Dial Up - Windows Native IPsec Client.																														
	<i>dialup-cisco</i>	Dial Up - Cisco IPsec Client.																														
	<i>static-fortiproxy</i>	Site to Site - FortiProxy.																														
	<i>dialup-fortiproxy</i>	Dial Up - FortiProxy.																														
	<i>static-cisco</i>	Site to Site - Cisco.																														
	<i>dialup-cisco-fw</i>	Dialup Up - Cisco Firewall.																														
	<i>simplified-static-fortiproxy</i>	Site to Site - FortiProxy (SD-WAN).																														
	<i>hub-fortiproxy-auto-discovery</i>	Hub role in a Hub-and-Spoke auto-discovery VPN.																														
<i>spoke-fortiproxy-auto-discovery</i>	Spoke role in a Hub-and-Spoke auto-discovery VPN.																															

Parameter	Description	Type	Size	Default
xauthtype	XAuth type.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>client</i>	Enable as client.		
	<i>pap</i>	Enable as server PAP.		
	<i>chap</i>	Enable as server CHAP.		
	<i>auto</i>	Enable as server auto.		
reauth	Enable/disable re-authentication upon IKE SA lifetime expiration.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable IKE SA re-authentication.		
	<i>enable</i>	Enable IKE SA re-authentication.		
authusr	XAuth user name.	string	Maximum length: 64	
authpasswd	XAuth password (max 35 characters).	password	Not Specified	
group-authentication	Enable/disable IKEv2 IDi group authentication.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IKEv2 IDi group authentication.		
	<i>disable</i>	Disable IKEv2 IDi group authentication.		
group-authentication-secret	Password for IKEv2 ID group authentication. ASCII string or hexadecimal indicated by a leading 0x.	password-3	Not Specified	
authusrgrp	Authentication user group.	string	Maximum length: 35	
idle-timeout	Enable/disable IPsec tunnel idle timeout.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable IPsec tunnel idle timeout.		
	<i>disable</i>	Disable IPsec tunnel idle timeout.		

Parameter	Description	Type	Size	Default						
idle-timeoutinterval	IPsec tunnel idle timeout in minutes.	integer	Minimum value: 5 Maximum value: 43200	15						
fgsp-sync	Enable/disable IPsec syncing of tunnels for FGSP IPsec.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IPsec syncing of tunnels to other cluster members.</td></tr><tr><td>disable</td><td>Disable IPsec syncing of tunnels to other cluster members.</td></tr></table>	Option	Description	enable	Enable IPsec syncing of tunnels to other cluster members.	disable	Disable IPsec syncing of tunnels to other cluster members.			
Option	Description									
enable	Enable IPsec syncing of tunnels to other cluster members.									
disable	Disable IPsec syncing of tunnels to other cluster members.									
inbound-dscp-copy	Enable/disable copy the dscp in the ESP header to the inner IP Header.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable copy the dscp in the ESP header to the inner IP Header.</td></tr><tr><td>disable</td><td>Disable copy the dscp in the ESP header to the inner IP Header.</td></tr></table>	Option	Description	enable	Enable copy the dscp in the ESP header to the inner IP Header.	disable	Disable copy the dscp in the ESP header to the inner IP Header.			
Option	Description									
enable	Enable copy the dscp in the ESP header to the inner IP Header.									
disable	Disable copy the dscp in the ESP header to the inner IP Header.									
auto-discovery-sender	Enable/disable sending auto-discovery short-cut messages.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sending auto-discovery short-cut messages.</td></tr><tr><td>disable</td><td>Disable sending auto-discovery short-cut messages.</td></tr></table>	Option	Description	enable	Enable sending auto-discovery short-cut messages.	disable	Disable sending auto-discovery short-cut messages.			
Option	Description									
enable	Enable sending auto-discovery short-cut messages.									
disable	Disable sending auto-discovery short-cut messages.									
auto-discovery-receiver	Enable/disable accepting auto-discovery short-cut messages.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable receiving auto-discovery short-cut messages.</td></tr><tr><td>disable</td><td>Disable receiving auto-discovery short-cut messages.</td></tr></table>	Option	Description	enable	Enable receiving auto-discovery short-cut messages.	disable	Disable receiving auto-discovery short-cut messages.			
Option	Description									
enable	Enable receiving auto-discovery short-cut messages.									
disable	Disable receiving auto-discovery short-cut messages.									
auto-discovery-forwarder	Enable/disable forwarding auto-discovery short-cut messages.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable forwarding auto-discovery short-cut messages.</td></tr><tr><td>disable</td><td>Disable forwarding auto-discovery short-cut messages.</td></tr></table>	Option	Description	enable	Enable forwarding auto-discovery short-cut messages.	disable	Disable forwarding auto-discovery short-cut messages.			
Option	Description									
enable	Enable forwarding auto-discovery short-cut messages.									
disable	Disable forwarding auto-discovery short-cut messages.									
auto-discovery-psk	Enable/disable use of pre-shared secrets for authentication of auto-discovery tunnels.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of pre-shared-secret authentication for auto-discovery tunnels.</td></tr><tr><td><i>disable</i></td><td>Disable use of authentication defined by 'authmethod' for auto-discovery tunnels.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of pre-shared-secret authentication for auto-discovery tunnels.	<i>disable</i>	Disable use of authentication defined by 'authmethod' for auto-discovery tunnels.			
	Option	Description								
	<i>enable</i>	Enable use of pre-shared-secret authentication for auto-discovery tunnels.								
<i>disable</i>	Disable use of authentication defined by 'authmethod' for auto-discovery tunnels.									
auto-discovery-shortcuts	Control deletion of child short-cut tunnels when the parent tunnel goes down.	option	-	independent						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>independent</i></td><td>Short-cut tunnels remain up if the parent tunnel goes down.</td></tr><tr><td><i>dependent</i></td><td>Short-cut tunnels are brought down if the parent tunnel goes down.</td></tr></table>	Option	Description	<i>independent</i>	Short-cut tunnels remain up if the parent tunnel goes down.	<i>dependent</i>	Short-cut tunnels are brought down if the parent tunnel goes down.			
	Option	Description								
	<i>independent</i>	Short-cut tunnels remain up if the parent tunnel goes down.								
<i>dependent</i>	Short-cut tunnels are brought down if the parent tunnel goes down.									
auto-discovery-crossover	Allow/block set-up of short-cut tunnels between different network IDs.	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow set-up of short-cut tunnels between different network IDs.</td></tr><tr><td><i>block</i></td><td>Block set-up of short-cut tunnels between different network IDs.</td></tr></table>	Option	Description	<i>allow</i>	Allow set-up of short-cut tunnels between different network IDs.	<i>block</i>	Block set-up of short-cut tunnels between different network IDs.			
	Option	Description								
	<i>allow</i>	Allow set-up of short-cut tunnels between different network IDs.								
<i>block</i>	Block set-up of short-cut tunnels between different network IDs.									
auto-discovery-offer-interval	Interval between shortcut offer messages in seconds.	integer	Minimum value: 1 Maximum value: 300	5						
fragmentation-mtu	IKE fragmentation MTU.	integer	Minimum value: 500 Maximum value: 16000	1200						
childless-ike	Enable/disable childless IKEv2 initiation (RFC 6023).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable childless IKEv2 initiation (RFC 6023).</td></tr><tr><td><i>disable</i></td><td>Disable childless IKEv2 initiation (RFC 6023).</td></tr></table>	Option	Description	<i>enable</i>	Enable childless IKEv2 initiation (RFC 6023).	<i>disable</i>	Disable childless IKEv2 initiation (RFC 6023).			
	Option	Description								
	<i>enable</i>	Enable childless IKEv2 initiation (RFC 6023).								
<i>disable</i>	Disable childless IKEv2 initiation (RFC 6023).									
azure-ad-autoconnect	Enable/disable Azure AD Auto-Connect for FortiClient.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Azure AD Auto-Connect for FortiClient.</td></tr><tr><td><i>disable</i></td><td>Disable Azure AD Auto-Connect for FortiClient.</td></tr></table>	Option	Description	<i>enable</i>	Enable Azure AD Auto-Connect for FortiClient.	<i>disable</i>	Disable Azure AD Auto-Connect for FortiClient.			
	Option	Description								
	<i>enable</i>	Enable Azure AD Auto-Connect for FortiClient.								
<i>disable</i>	Disable Azure AD Auto-Connect for FortiClient.									

Parameter	Description	Type	Size	Default										
rekey	Enable/disable phase1 rekey.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable phase1 rekey.</td></tr><tr><td><i>disable</i></td><td>Disable phase1 rekey.</td></tr></table>	Option	Description	<i>enable</i>	Enable phase1 rekey.	<i>disable</i>	Disable phase1 rekey.							
Option	Description													
<i>enable</i>	Enable phase1 rekey.													
<i>disable</i>	Disable phase1 rekey.													
digital-signature-auth	Enable/disable IKEv2 Digital Signature Authentication (RFC 7427).	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IKEv2 Digital Signature Authentication (RFC 7427).</td></tr><tr><td><i>disable</i></td><td>Disable IKEv2 Digital Signature Authentication (RFC 7427).</td></tr></table>	Option	Description	<i>enable</i>	Enable IKEv2 Digital Signature Authentication (RFC 7427).	<i>disable</i>	Disable IKEv2 Digital Signature Authentication (RFC 7427).							
Option	Description													
<i>enable</i>	Enable IKEv2 Digital Signature Authentication (RFC 7427).													
<i>disable</i>	Disable IKEv2 Digital Signature Authentication (RFC 7427).													
signature-hash-alg	Digital Signature Authentication hash algorithms.	option	-	sha2-512										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sha1</i></td><td>SHA1.</td></tr><tr><td><i>sha2-256</i></td><td>SHA2-256.</td></tr><tr><td><i>sha2-384</i></td><td>SHA2-384.</td></tr><tr><td><i>sha2-512</i></td><td>SHA2-512.</td></tr></table>	Option	Description	<i>sha1</i>	SHA1.	<i>sha2-256</i>	SHA2-256.	<i>sha2-384</i>	SHA2-384.	<i>sha2-512</i>	SHA2-512.			
Option	Description													
<i>sha1</i>	SHA1.													
<i>sha2-256</i>	SHA2-256.													
<i>sha2-384</i>	SHA2-384.													
<i>sha2-512</i>	SHA2-512.													
rsa-signature-format	Digital Signature Authentication RSA signature format.	option	-	pkcs1										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pkcs1</i></td><td>RSASSA PKCS#1 v1.5.</td></tr><tr><td><i>pss</i></td><td>RSASSA Probabilistic Signature Scheme (PSS).</td></tr></table>	Option	Description	<i>pkcs1</i>	RSASSA PKCS#1 v1.5.	<i>pss</i>	RSASSA Probabilistic Signature Scheme (PSS).							
Option	Description													
<i>pkcs1</i>	RSASSA PKCS#1 v1.5.													
<i>pss</i>	RSASSA Probabilistic Signature Scheme (PSS).													
rsa-signature-hash-override	Enable/disable IKEv2 RSA signature hash algorithm override.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IKEv2 RSA signature hash algorithm override.</td></tr><tr><td><i>disable</i></td><td>Disable IKEv2 RSA signature hash algorithm override.</td></tr></table>	Option	Description	<i>enable</i>	Enable IKEv2 RSA signature hash algorithm override.	<i>disable</i>	Disable IKEv2 RSA signature hash algorithm override.							
Option	Description													
<i>enable</i>	Enable IKEv2 RSA signature hash algorithm override.													
<i>disable</i>	Disable IKEv2 RSA signature hash algorithm override.													
enforce-unique-id	Enable/disable peer ID uniqueness check.	option	-	disable										

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable peer ID uniqueness enforcement.</td></tr><tr><td><i>keep-new</i></td><td>Enforce peer ID uniqueness, keep new connection if collision found.</td></tr><tr><td><i>keep-old</i></td><td>Enforce peer ID uniqueness, keep old connection if collision found.</td></tr></table>	Option	Description	<i>disable</i>	Disable peer ID uniqueness enforcement.	<i>keep-new</i>	Enforce peer ID uniqueness, keep new connection if collision found.	<i>keep-old</i>	Enforce peer ID uniqueness, keep old connection if collision found.			
	Option	Description										
	<i>disable</i>	Disable peer ID uniqueness enforcement.										
	<i>keep-new</i>	Enforce peer ID uniqueness, keep new connection if collision found.										
<i>keep-old</i>	Enforce peer ID uniqueness, keep old connection if collision found.											
cert-id-validation	Enable/disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.</td></tr><tr><td><i>disable</i></td><td>Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.</td></tr></table>	Option	Description	<i>enable</i>	Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.	<i>disable</i>	Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.					
	Option	Description										
	<i>enable</i>	Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.										
<i>disable</i>	Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.											
network-overlay	Enable/disable network overlays.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable network overlays.</td></tr><tr><td><i>enable</i></td><td>Enable network overlays.</td></tr></table>	Option	Description	<i>disable</i>	Disable network overlays.	<i>enable</i>	Enable network overlays.					
	Option	Description										
	<i>disable</i>	Disable network overlays.										
<i>enable</i>	Enable network overlays.											
network-id	VPN gateway network ID.	integer	Minimum value: 0 Maximum value: 255	0								
dev-id-notification	Enable/disable device ID notification.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable device ID notification.</td></tr><tr><td><i>enable</i></td><td>Enable device ID notification.</td></tr></table>	Option	Description	<i>disable</i>	Disable device ID notification.	<i>enable</i>	Enable device ID notification.					
	Option	Description										
	<i>disable</i>	Disable device ID notification.										
<i>enable</i>	Enable device ID notification.											
dev-id	Device ID carried by the device ID notification.	string	Maximum length: 63									
loopback-asmroute	Enable/disable asymmetric routing for IKE traffic on loopback interface.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow ingress/egress IKE traffic to be routed over different interfaces.</td></tr><tr><td><i>disable</i></td><td>Ingress/egress IKE traffic must be routed over the same interface.</td></tr></table>	Option	Description	<i>enable</i>	Allow ingress/egress IKE traffic to be routed over different interfaces.	<i>disable</i>	Ingress/egress IKE traffic must be routed over the same interface.					
	Option	Description										
	<i>enable</i>	Allow ingress/egress IKE traffic to be routed over different interfaces.										
<i>disable</i>	Ingress/egress IKE traffic must be routed over the same interface.											

Parameter	Description	Type	Size	Default										
link-cost	VPN tunnel underlay link cost.	integer	Minimum value: 0 Maximum value: 255	0										
exchange-fgt-device-id	Enable/disable device identifier exchange with peer FortiGate units for use of VPN monitor data by FortiManager.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable exchange of FortiProxy device identifier.</td></tr><tr><td><i>disable</i></td><td>Disable exchange of FortiProxy device identifier.</td></tr></table>	Option	Description	<i>enable</i>	Enable exchange of FortiProxy device identifier.	<i>disable</i>	Disable exchange of FortiProxy device identifier.							
Option	Description													
<i>enable</i>	Enable exchange of FortiProxy device identifier.													
<i>disable</i>	Disable exchange of FortiProxy device identifier.													
ems-sn-check	Enable/disable verification of EMS serial number.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable EMS serial number verification.</td></tr><tr><td><i>disable</i></td><td>Disable EMS serial number verification.</td></tr></table>	Option	Description	<i>enable</i>	Enable EMS serial number verification.	<i>disable</i>	Disable EMS serial number verification.							
Option	Description													
<i>enable</i>	Enable EMS serial number verification.													
<i>disable</i>	Disable EMS serial number verification.													
remote-gw-match	Set type of IPv4 remote gateway address matching.	option	-	any										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Match any IPv4 gateway address.</td></tr><tr><td><i>ipmask</i></td><td>Match IPv4 gateway address and mask.</td></tr><tr><td><i>iprange</i></td><td>Match IPv4 gateway address range.</td></tr><tr><td><i>geography</i></td><td>Match IPv4 gateway address from a specified country.</td></tr></table>	Option	Description	<i>any</i>	Match any IPv4 gateway address.	<i>ipmask</i>	Match IPv4 gateway address and mask.	<i>iprange</i>	Match IPv4 gateway address range.	<i>geography</i>	Match IPv4 gateway address from a specified country.			
Option	Description													
<i>any</i>	Match any IPv4 gateway address.													
<i>ipmask</i>	Match IPv4 gateway address and mask.													
<i>iprange</i>	Match IPv4 gateway address range.													
<i>geography</i>	Match IPv4 gateway address from a specified country.													
remote-gw-subnet	IPv4 address and subnet mask.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0										
remote-gw-start-ip	First IPv4 address in the range.	ipv4-address-any	Not Specified	0.0.0.0										
remote-gw-end-ip	Last IPv4 address in the range.	ipv4-address-any	Not Specified	0.0.0.0										
remote-gw-country	IPv4 addresses associated to a specific country.	string	Maximum length: 2											
remote-gw6-match	Set type of IPv6 remote gateway address matching.	option	-	any										

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Match any IPv6 gateway address.</td></tr><tr><td><i>ipprefix</i></td><td>Match IPv6 gateway address and prefix.</td></tr><tr><td><i>iprange</i></td><td>Match IPv6 gateway address range.</td></tr><tr><td><i>geography</i></td><td>Match IPv6 gateway address from a specified country.</td></tr></table>	Option	Description	<i>any</i>	Match any IPv6 gateway address.	<i>ipprefix</i>	Match IPv6 gateway address and prefix.	<i>iprange</i>	Match IPv6 gateway address range.	<i>geography</i>	Match IPv6 gateway address from a specified country.			
	Option	Description												
	<i>any</i>	Match any IPv6 gateway address.												
	<i>ipprefix</i>	Match IPv6 gateway address and prefix.												
	<i>iprange</i>	Match IPv6 gateway address range.												
<i>geography</i>	Match IPv6 gateway address from a specified country.													
remote-gw6-subnet	IPv6 address and prefix.	ipv6-network	Not Specified	::/0										
remote-gw6-start-ip	First IPv6 address in the range.	ipv6-address	Not Specified	::										
remote-gw6-end-ip	Last IPv6 address in the range.	ipv6-address	Not Specified	::										
remote-gw6-country	IPv6 addresses associated to a specific country.	string	Maximum length: 2											
cert-trust-store	CA certificate trust store.	option	-	local										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>local</i></td><td>Use local CA certificate.</td></tr><tr><td><i>ems</i></td><td>Use EMS CA certificate.</td></tr></table>	Option	Description	<i>local</i>	Use local CA certificate.	<i>ems</i>	Use EMS CA certificate.							
	Option	Description												
	<i>local</i>	Use local CA certificate.												
<i>ems</i>	Use EMS CA certificate.													

config vpn ipsec phase2-interface

Configure VPN autokey tunnel.

```
config vpn ipsec phase2-interface
  Description: Configure VPN autokey tunnel.
  edit <name>
    set phase1name {string}
    set proposal {option1}, {option2}, ...
    set dhgrp {option1}, {option2}, ...
    set replay [enable|disable]
    set keepalive [enable|disable]
    set auto-negotiate [enable|disable]
    set add-route [phase1|enable|...]
    set inbound-dscp-copy [phase1|enable|...]
    set auto-discovery-sender [phase1|enable|...]
    set auto-discovery-forwarder [phase1|enable|...]
    set keylifeseconds {integer}
    set keylifekbs {integer}
    set keylife-type [seconds|kbs|...]
    set single-source [enable|disable]
    set route-overlap [use-old|use-new|...]
```



```

    set comments {var-string}
    set protocol {integer}
    set src-name {string}
    set src-name6 {string}
    set src-addr-type [subnet|range|...]
    set src-start-ip {ipv4-address-any}
    set src-start-ip6 {ipv6-address}
    set src-end-ip {ipv4-address-any}
    set src-end-ip6 {ipv6-address}
    set src-subnet {ipv4-classnet-any}
    set src-subnet6 {ipv6-prefix}
    set src-port {integer}
    set dst-name {string}
    set dst-name6 {string}
    set dst-addr-type [subnet|range|...]
    set dst-start-ip {ipv4-address-any}
    set dst-start-ip6 {ipv6-address}
    set dst-end-ip {ipv4-address-any}
    set dst-end-ip6 {ipv6-address}
    set dst-subnet {ipv4-classnet-any}
    set dst-subnet6 {ipv6-prefix}
    set dst-port {integer}
  next
end

```

config vpn ipsec phase2-interface

Parameter	Description	Type	Size	Default																		
name	IPsec tunnel name.	string	Maximum length: 35																			
phase1name	Phase 1 determines the options required for phase 2.	string	Maximum length: 15																			
proposal	Phase2 proposal.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>null-md5</i></td><td>null-md5</td></tr><tr><td><i>null-sha1</i></td><td>null-sha1</td></tr><tr><td><i>null-sha256</i></td><td>null-sha256</td></tr><tr><td><i>null-sha384</i></td><td>null-sha384</td></tr><tr><td><i>null-sha512</i></td><td>null-sha512</td></tr><tr><td><i>des-null</i></td><td>des-null</td></tr><tr><td><i>des-md5</i></td><td>des-md5</td></tr><tr><td><i>des-sha1</i></td><td>des-sha1</td></tr></table>				Option	Description	<i>null-md5</i>	null-md5	<i>null-sha1</i>	null-sha1	<i>null-sha256</i>	null-sha256	<i>null-sha384</i>	null-sha384	<i>null-sha512</i>	null-sha512	<i>des-null</i>	des-null	<i>des-md5</i>	des-md5	<i>des-sha1</i>	des-sha1
Option	Description																					
<i>null-md5</i>	null-md5																					
<i>null-sha1</i>	null-sha1																					
<i>null-sha256</i>	null-sha256																					
<i>null-sha384</i>	null-sha384																					
<i>null-sha512</i>	null-sha512																					
<i>des-null</i>	des-null																					
<i>des-md5</i>	des-md5																					
<i>des-sha1</i>	des-sha1																					

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>des-sha256</i>	des-sha256		
	<i>des-sha384</i>	des-sha384		
	<i>des-sha512</i>	des-sha512		
	<i>3des-null</i>	3des-null		
	<i>3des-md5</i>	3des-md5		
	<i>3des-sha1</i>	3des-sha1		
	<i>3des-sha256</i>	3des-sha256		
	<i>3des-sha384</i>	3des-sha384		
	<i>3des-sha512</i>	3des-sha512		
	<i>aes128-null</i>	aes128-null		
	<i>aes128-md5</i>	aes128-md5		
	<i>aes128-sha1</i>	aes128-sha1		
	<i>aes128-sha256</i>	aes128-sha256		
	<i>aes128-sha384</i>	aes128-sha384		
	<i>aes128-sha512</i>	aes128-sha512		
	<i>aes128gcm</i>	aes128gcm		
	<i>aes192-null</i>	aes192-null		
	<i>aes192-md5</i>	aes192-md5		
	<i>aes192-sha1</i>	aes192-sha1		
	<i>aes192-sha256</i>	aes192-sha256		
	<i>aes192-sha384</i>	aes192-sha384		
	<i>aes192-sha512</i>	aes192-sha512		
	<i>aes256-null</i>	aes256-null		
	<i>aes256-md5</i>	aes256-md5		
	<i>aes256-sha1</i>	aes256-sha1		
	<i>aes256-sha256</i>	aes256-sha256		
	<i>aes256-sha384</i>	aes256-sha384		
	<i>aes256-sha512</i>	aes256-sha512		
	<i>aes256gcm</i>	aes256gcm		

Parameter	Description	Type	Size	Default																																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>chacha20poly1305</i></td><td>chacha20poly1305</td></tr><tr><td><i>aria128-null</i></td><td>aria128-null</td></tr><tr><td><i>aria128-md5</i></td><td>aria128-md5</td></tr><tr><td><i>aria128-sha1</i></td><td>aria128-sha1</td></tr><tr><td><i>aria128-sha256</i></td><td>aria128-sha256</td></tr><tr><td><i>aria128-sha384</i></td><td>aria128-sha384</td></tr><tr><td><i>aria128-sha512</i></td><td>aria128-sha512</td></tr><tr><td><i>aria192-null</i></td><td>aria192-null</td></tr><tr><td><i>aria192-md5</i></td><td>aria192-md5</td></tr><tr><td><i>aria192-sha1</i></td><td>aria192-sha1</td></tr><tr><td><i>aria192-sha256</i></td><td>aria192-sha256</td></tr><tr><td><i>aria192-sha384</i></td><td>aria192-sha384</td></tr><tr><td><i>aria192-sha512</i></td><td>aria192-sha512</td></tr><tr><td><i>aria256-null</i></td><td>aria256-null</td></tr><tr><td><i>aria256-md5</i></td><td>aria256-md5</td></tr><tr><td><i>aria256-sha1</i></td><td>aria256-sha1</td></tr><tr><td><i>aria256-sha256</i></td><td>aria256-sha256</td></tr><tr><td><i>aria256-sha384</i></td><td>aria256-sha384</td></tr><tr><td><i>aria256-sha512</i></td><td>aria256-sha512</td></tr><tr><td><i>seed-null</i></td><td>seed-null</td></tr><tr><td><i>seed-md5</i></td><td>seed-md5</td></tr><tr><td><i>seed-sha1</i></td><td>seed-sha1</td></tr><tr><td><i>seed-sha256</i></td><td>seed-sha256</td></tr><tr><td><i>seed-sha384</i></td><td>seed-sha384</td></tr><tr><td><i>seed-sha512</i></td><td>seed-sha512</td></tr></table>	Option	Description	<i>chacha20poly1305</i>	chacha20poly1305	<i>aria128-null</i>	aria128-null	<i>aria128-md5</i>	aria128-md5	<i>aria128-sha1</i>	aria128-sha1	<i>aria128-sha256</i>	aria128-sha256	<i>aria128-sha384</i>	aria128-sha384	<i>aria128-sha512</i>	aria128-sha512	<i>aria192-null</i>	aria192-null	<i>aria192-md5</i>	aria192-md5	<i>aria192-sha1</i>	aria192-sha1	<i>aria192-sha256</i>	aria192-sha256	<i>aria192-sha384</i>	aria192-sha384	<i>aria192-sha512</i>	aria192-sha512	<i>aria256-null</i>	aria256-null	<i>aria256-md5</i>	aria256-md5	<i>aria256-sha1</i>	aria256-sha1	<i>aria256-sha256</i>	aria256-sha256	<i>aria256-sha384</i>	aria256-sha384	<i>aria256-sha512</i>	aria256-sha512	<i>seed-null</i>	seed-null	<i>seed-md5</i>	seed-md5	<i>seed-sha1</i>	seed-sha1	<i>seed-sha256</i>	seed-sha256	<i>seed-sha384</i>	seed-sha384	<i>seed-sha512</i>	seed-sha512			
	Option	Description																																																						
	<i>chacha20poly1305</i>	chacha20poly1305																																																						
	<i>aria128-null</i>	aria128-null																																																						
	<i>aria128-md5</i>	aria128-md5																																																						
	<i>aria128-sha1</i>	aria128-sha1																																																						
	<i>aria128-sha256</i>	aria128-sha256																																																						
	<i>aria128-sha384</i>	aria128-sha384																																																						
	<i>aria128-sha512</i>	aria128-sha512																																																						
	<i>aria192-null</i>	aria192-null																																																						
	<i>aria192-md5</i>	aria192-md5																																																						
	<i>aria192-sha1</i>	aria192-sha1																																																						
	<i>aria192-sha256</i>	aria192-sha256																																																						
	<i>aria192-sha384</i>	aria192-sha384																																																						
	<i>aria192-sha512</i>	aria192-sha512																																																						
	<i>aria256-null</i>	aria256-null																																																						
	<i>aria256-md5</i>	aria256-md5																																																						
	<i>aria256-sha1</i>	aria256-sha1																																																						
	<i>aria256-sha256</i>	aria256-sha256																																																						
	<i>aria256-sha384</i>	aria256-sha384																																																						
	<i>aria256-sha512</i>	aria256-sha512																																																						
	<i>seed-null</i>	seed-null																																																						
	<i>seed-md5</i>	seed-md5																																																						
	<i>seed-sha1</i>	seed-sha1																																																						
	<i>seed-sha256</i>	seed-sha256																																																						
	<i>seed-sha384</i>	seed-sha384																																																						
	<i>seed-sha512</i>	seed-sha512																																																						
dhgrp	Phase2 DH group.	option	-	14																																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>DH Group 1.</td></tr></table>	Option	Description	1	DH Group 1.																																																			
	Option	Description																																																						
1	DH Group 1.																																																							

Parameter	Description	Type	Size	Default																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>2</td><td>DH Group 2.</td></tr><tr><td>5</td><td>DH Group 5.</td></tr><tr><td>14</td><td>DH Group 14.</td></tr><tr><td>15</td><td>DH Group 15.</td></tr><tr><td>16</td><td>DH Group 16.</td></tr><tr><td>17</td><td>DH Group 17.</td></tr><tr><td>18</td><td>DH Group 18.</td></tr><tr><td>19</td><td>DH Group 19.</td></tr><tr><td>20</td><td>DH Group 20.</td></tr><tr><td>21</td><td>DH Group 21.</td></tr><tr><td>27</td><td>DH Group 27.</td></tr><tr><td>28</td><td>DH Group 28.</td></tr><tr><td>29</td><td>DH Group 29.</td></tr><tr><td>30</td><td>DH Group 30.</td></tr><tr><td>31</td><td>DH Group 31.</td></tr><tr><td>32</td><td>DH Group 32.</td></tr></table>	Option	Description	2	DH Group 2.	5	DH Group 5.	14	DH Group 14.	15	DH Group 15.	16	DH Group 16.	17	DH Group 17.	18	DH Group 18.	19	DH Group 19.	20	DH Group 20.	21	DH Group 21.	27	DH Group 27.	28	DH Group 28.	29	DH Group 29.	30	DH Group 30.	31	DH Group 31.	32	DH Group 32.			
	Option	Description																																				
	2	DH Group 2.																																				
	5	DH Group 5.																																				
	14	DH Group 14.																																				
	15	DH Group 15.																																				
	16	DH Group 16.																																				
	17	DH Group 17.																																				
	18	DH Group 18.																																				
	19	DH Group 19.																																				
	20	DH Group 20.																																				
	21	DH Group 21.																																				
	27	DH Group 27.																																				
	28	DH Group 28.																																				
	29	DH Group 29.																																				
	30	DH Group 30.																																				
	31	DH Group 31.																																				
	32	DH Group 32.																																				
replay	Enable/disable replay detection.	option	-	enable																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																															
	Option	Description																																				
	<i>enable</i>	Enable setting.																																				
<i>disable</i>	Disable setting.																																					
keepalive	Enable/disable keep alive.	option	-	disable																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																															
	Option	Description																																				
	<i>enable</i>	Enable setting.																																				
<i>disable</i>	Disable setting.																																					
auto-negotiate	Enable/disable IPsec SA auto-negotiation.	option	-	disable																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																															
	Option	Description																																				
	<i>enable</i>	Enable setting.																																				
<i>disable</i>	Disable setting.																																					

Parameter	Description	Type	Size	Default								
add-route	Enable/disable automatic route addition.	option	-	phase1								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>phase1</i></td><td>Add route according to phase1 add-route setting.</td></tr><tr><td><i>enable</i></td><td>Add route for remote proxy ID.</td></tr><tr><td><i>disable</i></td><td>Do not add route for remote proxy ID.</td></tr></table>	Option	Description	<i>phase1</i>	Add route according to phase1 add-route setting.	<i>enable</i>	Add route for remote proxy ID.	<i>disable</i>	Do not add route for remote proxy ID.			
Option	Description											
<i>phase1</i>	Add route according to phase1 add-route setting.											
<i>enable</i>	Add route for remote proxy ID.											
<i>disable</i>	Do not add route for remote proxy ID.											
inbound-dscp-copy	Enable/disable copying of the DSCP in the ESP header to the inner IP header.	option	-	phase1								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>phase1</i></td><td>copy the DCSP in the ESP header to the inner IP Header according to the phase1 inbound_dscp_copy setting.</td></tr><tr><td><i>enable</i></td><td>Enable copying of the DSCP in the ESP header to the inner IP header.</td></tr><tr><td><i>disable</i></td><td>Disable copying of the DSCP in the ESP header to the inner IP header.</td></tr></table>	Option	Description	<i>phase1</i>	copy the DCSP in the ESP header to the inner IP Header according to the phase1 inbound_dscp_copy setting.	<i>enable</i>	Enable copying of the DSCP in the ESP header to the inner IP header.	<i>disable</i>	Disable copying of the DSCP in the ESP header to the inner IP header.			
Option	Description											
<i>phase1</i>	copy the DCSP in the ESP header to the inner IP Header according to the phase1 inbound_dscp_copy setting.											
<i>enable</i>	Enable copying of the DSCP in the ESP header to the inner IP header.											
<i>disable</i>	Disable copying of the DSCP in the ESP header to the inner IP header.											
auto-discovery-sender	Enable/disable sending short-cut messages.	option	-	phase1								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>phase1</i></td><td>Send short-cut messages according to the phase1 auto-discovery-sender setting.</td></tr><tr><td><i>enable</i></td><td>Enable sending auto-discovery short-cut messages.</td></tr><tr><td><i>disable</i></td><td>Disable sending auto-discovery short-cut messages.</td></tr></table>	Option	Description	<i>phase1</i>	Send short-cut messages according to the phase1 auto-discovery-sender setting.	<i>enable</i>	Enable sending auto-discovery short-cut messages.	<i>disable</i>	Disable sending auto-discovery short-cut messages.			
Option	Description											
<i>phase1</i>	Send short-cut messages according to the phase1 auto-discovery-sender setting.											
<i>enable</i>	Enable sending auto-discovery short-cut messages.											
<i>disable</i>	Disable sending auto-discovery short-cut messages.											
auto-discovery-forwarder	Enable/disable forwarding short-cut messages.	option	-	phase1								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>phase1</i></td><td>Forward short-cut messages according to the phase1 auto-discovery-forwarder setting.</td></tr><tr><td><i>enable</i></td><td>Enable forwarding auto-discovery short-cut messages.</td></tr><tr><td><i>disable</i></td><td>Disable forwarding auto-discovery short-cut messages.</td></tr></table>	Option	Description	<i>phase1</i>	Forward short-cut messages according to the phase1 auto-discovery-forwarder setting.	<i>enable</i>	Enable forwarding auto-discovery short-cut messages.	<i>disable</i>	Disable forwarding auto-discovery short-cut messages.			
Option	Description											
<i>phase1</i>	Forward short-cut messages according to the phase1 auto-discovery-forwarder setting.											
<i>enable</i>	Enable forwarding auto-discovery short-cut messages.											
<i>disable</i>	Disable forwarding auto-discovery short-cut messages.											
keylifeseconds	Phase2 key life in time in seconds.	integer	Minimum value: 120 Maximum value: 172800	43200								

Parameter	Description	Type	Size	Default								
keylifekbs	Phase2 key life in number of kilobytes of traffic.	integer	Minimum value: 5120 Maximum value: 4294967295	5120								
keylife-type	Keylife type.	option	-	seconds								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>seconds</td><td>Key life in seconds.</td></tr><tr><td>kbs</td><td>Key life in kilobytes.</td></tr><tr><td>both</td><td>Key life both.</td></tr></table>	Option	Description	seconds	Key life in seconds.	kbs	Key life in kilobytes.	both	Key life both.			
Option	Description											
seconds	Key life in seconds.											
kbs	Key life in kilobytes.											
both	Key life both.											
single-source	Enable/disable single source IP restriction.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Only single source IP will be accepted.</td></tr><tr><td>disable</td><td>Source IP range will be accepted.</td></tr></table>	Option	Description	enable	Only single source IP will be accepted.	disable	Source IP range will be accepted.					
Option	Description											
enable	Only single source IP will be accepted.											
disable	Source IP range will be accepted.											
route-overlap	Action for overlapping routes.	option	-	use-new								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>use-old</td><td>Use the old route and do not add the new route.</td></tr><tr><td>use-new</td><td>Delete the old route and add the new route.</td></tr><tr><td>allow</td><td>Allow overlapping routes.</td></tr></table>	Option	Description	use-old	Use the old route and do not add the new route.	use-new	Delete the old route and add the new route.	allow	Allow overlapping routes.			
Option	Description											
use-old	Use the old route and do not add the new route.											
use-new	Delete the old route and add the new route.											
allow	Allow overlapping routes.											
comments	Comment.	var-string	Maximum length: 255									
protocol	Quick mode protocol selector.	integer	Minimum value: 0 Maximum value: 255	0								
src-name	Local proxy ID name.	string	Maximum length: 79									
src-name6	Local proxy ID name.	string	Maximum length: 79									
src-addr-type	Local proxy ID type.	option	-	subnet								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>subnet</td><td>IPv4 subnet.</td></tr></table>	Option	Description	subnet	IPv4 subnet.							
Option	Description											
subnet	IPv4 subnet.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>range</i>	IPv4 range.		
	<i>ip</i>	IPv4 IP.		
	<i>name</i>	IPv4 firewall address or group name.		
	<i>subnet6</i>	IPv6 subnet.		
	<i>range6</i>	IPv6 range.		
	<i>ip6</i>	IPv6 IP.		
	<i>name6</i>	IPv6 firewall address or group name.		
src-start-ip	Local proxy ID start.	ipv4-address-any	Not Specified	0.0.0.0
src-start-ip6	Local proxy ID IPv6 start.	ipv6-address	Not Specified	::
src-end-ip	Local proxy ID end.	ipv4-address-any	Not Specified	0.0.0.0
src-end-ip6	Local proxy ID IPv6 end.	ipv6-address	Not Specified	::
src-subnet	Local proxy ID subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
src-subnet6	Local proxy ID IPv6 subnet.	ipv6-prefix	Not Specified	::/0
src-port	Quick mode source port.	integer	Minimum value: 0 Maximum value: 65535	0
dst-name	Remote proxy ID name.	string	Maximum length: 79	
dst-name6	Remote proxy ID name.	string	Maximum length: 79	
dst-addr-type	Remote proxy ID type.	option	-	subnet
	Option	Description		
	<i>subnet</i>	IPv4 subnet.		
	<i>range</i>	IPv4 range.		
	<i>ip</i>	IPv4 IP.		
	<i>name</i>	IPv4 firewall address or group name.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>subnet6</i>	IPv6 subnet.		
	<i>range6</i>	IPv6 range.		
	<i>ip6</i>	IPv6 IP.		
	<i>name6</i>	IPv6 firewall address or group name.		
dst-start-ip	Remote proxy ID IPv4 start.	ipv4-address-any	Not Specified	0.0.0.0
dst-start-ip6	Remote proxy ID IPv6 start.	ipv6-address	Not Specified	::
dst-end-ip	Remote proxy ID IPv4 end.	ipv4-address-any	Not Specified	0.0.0.0
dst-end-ip6	Remote proxy ID IPv6 end.	ipv6-address	Not Specified	::
dst-subnet	Remote proxy ID IPv4 subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
dst-subnet6	Remote proxy ID IPv6 subnet.	ipv6-prefix	Not Specified	::/0
dst-port	Quick mode destination port.	integer	Minimum value: 0 Maximum value: 65535	0

waf

This section includes syntax for the following commands:

- [config waf main-class on page 1113](#)
- [config waf profile on page 1113](#)
- [config waf signature on page 1138](#)
- [config waf sub-class on page 1139](#)

config waf main-class

Hidden table for datasource.

```
config waf main-class
  Description: Hidden table for datasource.
  edit <id>
    set name {string}
  next
end
```

config waf main-class

Parameter	Description	Type	Size	Default
name	Main signature class name.	string	Maximum length: 127	
id	Main signature class ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config waf profile

Configure Web application firewall configuration.

```
config waf profile
  Description: Configure Web application firewall configuration.
  edit <name>
    set external [disable|enable]
    set extended-log [enable|disable]
    config signature
```

```

Description: WAF signatures.
config main-class
    Description: Main signature class.
    edit <id>
        set status [enable|disable]
        set action [allow|block|...]
        set log [enable|disable]
        set severity [high|medium|...]
    next
end
set disabled-sub-class <id1>, <id2>, ...
set disabled-signature <id1>, <id2>, ...
set credit-card-detection-threshold {integer}
config custom-signature
    Description: Custom signature.
    edit <name>
        set status [enable|disable]
        set action [allow|block|...]
        set log [enable|disable]
        set severity [high|medium|...]
        set direction [request|response]
        set case-sensitivity [disable|enable]
        set pattern {string}
        set target {option1}, {option2}, ...
    next
end
end
config constraint
    Description: WAF HTTP protocol restrictions.
    config header-length
        Description: HTTP header length in request.
        set status [enable|disable]
        set length {integer}
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config content-length
        Description: HTTP content length in request.
        set status [enable|disable]
        set length {integer}
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config param-length
        Description: Maximum length of parameter in URL, HTTP POST request or HTTP
body.
        set status [enable|disable]
        set length {integer}
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config line-length
        Description: HTTP line length in request.

```

```
        set status [enable|disable]
        set length {integer}
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config url-param-length
        Description: Maximum length of parameter in URL.
        set status [enable|disable]
        set length {integer}
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config version
        Description: Enable/disable HTTP version check.
        set status [enable|disable]
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config method
        Description: Enable/disable HTTP method check.
        set status [enable|disable]
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config hostname
        Description: Enable/disable hostname check.
        set status [enable|disable]
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config malformed
        Description: Enable/disable malformed HTTP request check.
        set status [enable|disable]
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config max-cookie
        Description: Maximum number of cookies in HTTP request.
        set status [enable|disable]
        set max-cookie {integer}
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config max-header-line
        Description: Maximum number of HTTP header line.
        set status [enable|disable]
        set max-header-line {integer}
        set action [allow|block]
        set log [enable|disable]
```

```
        set severity [high|medium|...]
    end
    config max-url-param
        Description: Maximum number of parameters in URL.
        set status [enable|disable]
        set max-url-param {integer}
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config max-range-segment
        Description: Maximum number of range segments in HTTP range line.
        set status [enable|disable]
        set max-range-segment {integer}
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config exception
        Description: HTTP constraint exception.
        edit <id>
            set pattern {string}
            set regex [enable|disable]
            set address {string}
            set header-length [enable|disable]
            set content-length [enable|disable]
            set param-length [enable|disable]
            set line-length [enable|disable]
            set url-param-length [enable|disable]
            set version [enable|disable]
            set method [enable|disable]
            set hostname [enable|disable]
            set malformed [enable|disable]
            set max-cookie [enable|disable]
            set max-header-line [enable|disable]
            set max-url-param [enable|disable]
            set max-range-segment [enable|disable]
        next
    end
end
config method
    Description: Method restriction.
    set status [enable|disable]
    set log [enable|disable]
    set severity [high|medium|...]
    set default-allowed-methods {option1}, {option2}, ...
    config method-policy
        Description: HTTP method policy.
        edit <id>
            set pattern {string}
            set regex [enable|disable]
            set address {string}
            set allowed-methods {option1}, {option2}, ...
        next
    end
end
```

```

config address-list
    Description: Address block and allow lists.
    set status [enable|disable]
    set blocked-log [enable|disable]
    set severity [high|medium|...]
    set trusted-address <name1>, <name2>, ...
    set blocked-address <name1>, <name2>, ...
end
config url-access
    Description: URL access list.
    edit <id>
        set address {string}
        set action [bypass|permit|...]
        set log [enable|disable]
        set severity [high|medium|...]
        config access-pattern
            Description: URL access pattern.
            edit <id>
                set srcaddr {string}
                set pattern {string}
                set regex [enable|disable]
                set negate [enable|disable]
            next
        end
    next
end
next
end
set comment {var-string}
next
end

```

config waf profile

Parameter	Description	Type	Size	Default
name	WAF Profile name.	string	Maximum length: 35	
external	Disable/Enable external HTTP Inspection.	option	-	disable
	Option Description			
	<i>disable</i>	Disable external inspection.		
	<i>enable</i>	Enable external inspection.		
extended-log	Enable/disable extended logging.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
comment	Comment.	var-string	Maximum length: 1023	

config signature

Parameter	Description	Type	Size	Default
disabled-sub-class <id>	Disabled signature subclasses. Signature subclass ID.	integer	Minimum value: 0 Maximum value: 4294967295	
disabled-signature <id>	Disabled signatures. Signature ID.	integer	Minimum value: 0 Maximum value: 4294967295	
credit-card-detection-threshold	The minimum number of Credit cards to detect violation.	integer	Minimum value: 0 Maximum value: 128	3

config main-class

Parameter	Description	Type	Size	Default
id	Main signature class ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Status.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
action	Action.	option	-	allow
	Option	Description		
	allow	Allow.		
	block	Block.		
	erase	Erase credit card numbers.		
log	Enable/disable logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

config custom-signature

Parameter	Description	Type	Size	Default
name	Signature name.	string	Maximum length: 35	
status	Status.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
	<i>erase</i>	Erase credit card numbers.		
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High severity.</td></tr><tr><td><i>medium</i></td><td>Medium severity.</td></tr><tr><td><i>low</i></td><td>Low severity.</td></tr></table>	Option	Description	<i>high</i>	High severity.	<i>medium</i>	Medium severity.	<i>low</i>	Low severity.																							
	Option	Description																														
	<i>high</i>	High severity.																														
	<i>medium</i>	Medium severity.																														
<i>low</i>	Low severity.																															
direction	Traffic direction.	option	-	request																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>request</i></td><td>Match HTTP request.</td></tr><tr><td><i>response</i></td><td>Match HTTP response.</td></tr></table>	Option	Description	<i>request</i>	Match HTTP request.	<i>response</i>	Match HTTP response.																									
	Option	Description																														
	<i>request</i>	Match HTTP request.																														
<i>response</i>	Match HTTP response.																															
case-sensitivity	Case sensitivity in pattern.	option	-	disable																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Case insensitive in pattern.</td></tr><tr><td><i>enable</i></td><td>Case sensitive in pattern.</td></tr></table>	Option	Description	<i>disable</i>	Case insensitive in pattern.	<i>enable</i>	Case sensitive in pattern.																									
	Option	Description																														
	<i>disable</i>	Case insensitive in pattern.																														
<i>enable</i>	Case sensitive in pattern.																															
pattern	Match pattern.	string	Maximum length: 511																													
target	Match HTTP target.	option	-																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>arg</i></td><td>HTTP arguments.</td></tr><tr><td><i>arg-name</i></td><td>Names of HTTP arguments.</td></tr><tr><td><i>req-body</i></td><td>HTTP request body.</td></tr><tr><td><i>req-cookie</i></td><td>HTTP request cookies.</td></tr><tr><td><i>req-cookie-name</i></td><td>HTTP request cookie names.</td></tr><tr><td><i>req-filename</i></td><td>HTTP request file name.</td></tr><tr><td><i>req-header</i></td><td>HTTP request headers.</td></tr><tr><td><i>req-header-name</i></td><td>HTTP request header names.</td></tr><tr><td><i>req-raw-uri</i></td><td>Raw URI of HTTP request.</td></tr><tr><td><i>req-uri</i></td><td>URI of HTTP request.</td></tr><tr><td><i>resp-body</i></td><td>HTTP response body.</td></tr><tr><td><i>resp-hdr</i></td><td>HTTP response headers.</td></tr><tr><td><i>resp-status</i></td><td>HTTP response status.</td></tr></table>	Option	Description	<i>arg</i>	HTTP arguments.	<i>arg-name</i>	Names of HTTP arguments.	<i>req-body</i>	HTTP request body.	<i>req-cookie</i>	HTTP request cookies.	<i>req-cookie-name</i>	HTTP request cookie names.	<i>req-filename</i>	HTTP request file name.	<i>req-header</i>	HTTP request headers.	<i>req-header-name</i>	HTTP request header names.	<i>req-raw-uri</i>	Raw URI of HTTP request.	<i>req-uri</i>	URI of HTTP request.	<i>resp-body</i>	HTTP response body.	<i>resp-hdr</i>	HTTP response headers.	<i>resp-status</i>	HTTP response status.			
	Option	Description																														
	<i>arg</i>	HTTP arguments.																														
	<i>arg-name</i>	Names of HTTP arguments.																														
	<i>req-body</i>	HTTP request body.																														
	<i>req-cookie</i>	HTTP request cookies.																														
	<i>req-cookie-name</i>	HTTP request cookie names.																														
	<i>req-filename</i>	HTTP request file name.																														
	<i>req-header</i>	HTTP request headers.																														
	<i>req-header-name</i>	HTTP request header names.																														
	<i>req-raw-uri</i>	Raw URI of HTTP request.																														
	<i>req-uri</i>	URI of HTTP request.																														
	<i>resp-body</i>	HTTP response body.																														
	<i>resp-hdr</i>	HTTP response headers.																														
<i>resp-status</i>	HTTP response status.																															

config header-length

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
length	Length of HTTP header in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	8192
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

config content-length

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default
length	Length of HTTP content in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	67108864
action	Action.	option	-	allow
	OptionDescription			
	allow	Allow.		
	block	Block.		
log	Enable/disable logging.	option	-	disable
	OptionDescription			
	enable	Enable setting.		
	disable	Disable setting.		
severity	Severity.	option	-	medium
	OptionDescription			
	high	High severity.		
	medium	Medium severity.		
	low	Low severity.		

config param-length

Parameter	Description	Type	Size	Default						
status	Enable/disable the constraint.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
length	Maximum length of parameter in URL, HTTP POST request or HTTP body in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	8192						
action	Action.	option	-	allow						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

config line-length

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
length	Length of HTTP line in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	1024
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

config url-param-length

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
length	Maximum length of URL parameter in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	8192
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

config version

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

config method

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

config method

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>high</i>	High severity		
	<i>medium</i>	medium severity		
	<i>low</i>	low severity		
default-allowed-methods	Methods.	option	-	
	Option	Description		
	<i>get</i>	HTTP GET method.		
	<i>post</i>	HTTP POST method.		
	<i>put</i>	HTTP PUT method.		
	<i>head</i>	HTTP HEAD method.		
	<i>connect</i>	HTTP CONNECT method.		
	<i>trace</i>	HTTP TRACE method.		
	<i>options</i>	HTTP OPTIONS method.		
	<i>delete</i>	HTTP DELETE method.		
	<i>others</i>	Other HTTP methods.		

config hostname

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

config malformed

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

config max-cookie

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
max-cookie	Maximum number of cookies in HTTP request (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	16
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

config max-header-line

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default
max-header-line	Maximum number HTTP header lines (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	32
action	Action.	option	-	allow
	Option		Description	
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	Option		Description	
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	Option		Description	
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

config max-url-param

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
max-url-param	Maximum number of parameters in URL (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	16
action	Action.	option	-	allow

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

config max-range-segment

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
max-range-segment	Maximum number of range segments in HTTP range line (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	5
action	Action.	option	-	allow
	Option	Description		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	Option	Description		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

config exception

Parameter	Description	Type	Size	Default
id	Exception ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
pattern	URL pattern.	string	Maximum length: 511	
regex	Enable/disable regular expression based pattern match.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
address	Host address.	string	Maximum length: 79	
header-length	HTTP header length in request.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
content-length	HTTP content length in request.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
param-length	Maximum length of parameter in URL, HTTP POST request or HTTP body.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
line-length	HTTP line length in request.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
url-param-length	Maximum length of parameter in URL.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
version	Enable/disable HTTP version check.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
method	Enable/disable HTTP method check.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
hostname	Enable/disable hostname check.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
malformed	Enable/disable malformed HTTP request check.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
max-cookie	Maximum number of cookies in HTTP request.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
max-header-line	Maximum number of HTTP header line.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
max-url-param	Maximum number of parameters in URL.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
max-range-segment	Maximum number of range segments in HTTP range line.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config method

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
action	Action.	option	-	allow
log	Enable/disable logging.	option	-	disable
severity	Severity.	option	-	medium

config method

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
log	Enable/disable logging.	option	-	disable
severity	Severity.	option	-	medium
default-allowed-methods	Methods.	option	-	

config method-policy

Parameter	Description	Type	Size	Default
id	HTTP method policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
pattern	URL pattern.	string	Maximum length: 511	
regex	Enable/disable regular expression based pattern match.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
address	Host address.	string	Maximum length: 79	
allowed-methods	Allowed Methods.	option	-	

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>get</i>	HTTP GET method.		
	<i>post</i>	HTTP POST method.		
	<i>put</i>	HTTP PUT method.		
	<i>head</i>	HTTP HEAD method.		
	<i>connect</i>	HTTP CONNECT method.		
	<i>trace</i>	HTTP TRACE method.		
	<i>options</i>	HTTP OPTIONS method.		
	<i>delete</i>	HTTP DELETE method.		
	<i>others</i>	Other HTTP methods.		

config address-list

Parameter	Description	Type	Size	Default								
status	Status.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
blocked-log	Enable/disable logging on blocked addresses.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
severity	Severity.	option	-	medium								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High severity.</td></tr><tr><td><i>medium</i></td><td>Medium severity.</td></tr><tr><td><i>low</i></td><td>Low severity.</td></tr></table>	Option	Description	<i>high</i>	High severity.	<i>medium</i>	Medium severity.	<i>low</i>	Low severity.			
	Option	Description										
	<i>high</i>	High severity.										
	<i>medium</i>	Medium severity.										
<i>low</i>	Low severity.											
trusted-address <name>	Trusted address. Address name.	string	Maximum length: 79									

Parameter	Description	Type	Size	Default
blocked-address <name>	Blocked address. Address name.	string	Maximum length: 79	

config url-access

Parameter	Description	Type	Size	Default								
id	URL access ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
address	Host address.	string	Maximum length: 79									
action	Action.	option	-	permit								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Allow the HTTP request, also bypass further WAF scanning.</td></tr><tr><td>permit</td><td>Allow the HTTP request, and continue further WAF scanning.</td></tr><tr><td>block</td><td>Block HTTP request.</td></tr></table>				Option	Description	bypass	Allow the HTTP request, also bypass further WAF scanning.	permit	Allow the HTTP request, and continue further WAF scanning.	block	Block HTTP request.
	Option	Description										
	bypass	Allow the HTTP request, also bypass further WAF scanning.										
	permit	Allow the HTTP request, and continue further WAF scanning.										
block	Block HTTP request.											
log	Enable/disable logging.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.		
	Option	Description										
	enable	Enable setting.										
disable	Disable setting.											
severity	Severity.	option	-	medium								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high</td><td>High severity.</td></tr><tr><td>medium</td><td>Medium severity.</td></tr><tr><td>low</td><td>Low severity.</td></tr></table>				Option	Description	high	High severity.	medium	Medium severity.	low	Low severity.
	Option	Description										
	high	High severity.										
	medium	Medium severity.										
low	Low severity.											

config access-pattern

Parameter	Description	Type	Size	Default						
id	URL access pattern ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
srcaddr	Source address.	string	Maximum length: 79							
pattern	URL pattern.	string	Maximum length: 511							
regex	Enable/disable regular expression based pattern match.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
negate	Enable/disable match negation.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									

config waf signature

Hidden table for datasource.

```
config waf signature
    Description: Hidden table for datasource.
    edit <id>
        set desc {string}
    next
end
```

config waf signature

Parameter	Description	Type	Size	Default
desc	Signature description.	string	Maximum length: 511	

Parameter	Description	Type	Size	Default
id	Signature ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config waf sub-class

Hidden table for datasource.

```
config waf sub-class
    Description: Hidden table for datasource.
    edit <id>
        set name {string}
    next
end
```

config waf sub-class

Parameter	Description	Type	Size	Default
name	Signature subclass name.	string	Maximum length: 127	
id	Signature subclass ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

wanopt

This section includes syntax for the following commands:

- [config wanopt auth-group on page 1140](#)
- [config wanopt cache-service on page 1141](#)
- [config wanopt content-delivery-network-rule on page 1143](#)
- [config wanopt peer on page 1148](#)
- [config wanopt profile on page 1149](#)
- [config wanopt remote-storage on page 1157](#)
- [config wanopt settings on page 1157](#)

config wanopt auth-group

Configure WAN optimization authentication groups.

```
config wanopt auth-group
  Description: Configure WAN optimization authentication groups.
  edit <name>
    set auth-method [cert|psk]
    set psk {password}
    set cert {string}
    set peer-accept [any|defined|...]
    set peer {string}
  next
end
```

config wanopt auth-group

Parameter	Description	Type	Size	Default
name	Auth-group name.	string	Maximum length: 35	
auth-method	Select certificate or pre-shared key authentication for this authentication group.	option	-	cert
		Option	Description	
		cert	Certificate authentication.	
		psk	Pre-shared secret key authentication.	
psk	Pre-shared key used by the peers in this authentication group.	password	Not Specified	

Parameter	Description	Type	Size	Default								
cert	Name of certificate to identify this peer.	string	Maximum length: 35									
peer-accept	Determine if this auth group accepts, any peer, a list of defined peers, or just one peer.	option	-	any								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Accept any peer that can authenticate with this auth group.</td></tr><tr><td><i>defined</i></td><td>Accept only the peers added with the wanopt peer command.</td></tr><tr><td><i>one</i></td><td>Accept the peer added to this auth group using the peer option.</td></tr></table>	Option	Description	<i>any</i>	Accept any peer that can authenticate with this auth group.	<i>defined</i>	Accept only the peers added with the wanopt peer command.	<i>one</i>	Accept the peer added to this auth group using the peer option.			
Option	Description											
<i>any</i>	Accept any peer that can authenticate with this auth group.											
<i>defined</i>	Accept only the peers added with the wanopt peer command.											
<i>one</i>	Accept the peer added to this auth group using the peer option.											
peer	If peer-accept is set to one, select the name of one peer to add to this authentication group. The peer must have added with the wanopt peer command.	string	Maximum length: 35									

config wanopt cache-service

Designate cache-service for wan-optimization and webcache.

```

config wanopt cache-service
    Description: Designate cache-service for wan-optimization and webcache.
    set prefer-scenario [balance|prefer-speed|...]
    set collaboration [enable|disable]
    set device-id {string}
    set acceptable-connections [any|peers]
    config dst-peer
        Description: Modify cache-service destination peer list.
        edit <device-id>
            set auth-type {integer}
            set encode-type {integer}
            set priority {integer}
            set ip {ipv4-address-any}
        next
    end
    config src-peer
        Description: Modify cache-service source peer list.
        edit <device-id>
            set auth-type {integer}
            set encode-type {integer}
            set priority {integer}
            set ip {ipv4-address-any}
        next
    end
end
end

```

config wanopt cache-service

Parameter	Description	Type	Size	Default
prefer-scenario	Set the preferred cache behavior towards the balance between latency and hit-ratio.	option	-	balance
	Option	Description		
	<i>balance</i>	Balance between speed and cache hit ratio.		
	<i>prefer-speed</i>	Prefer response speed at the expense of increased cache bypasses.		
	<i>prefer-cache</i>	Prefer improving hit-ratio through increasing latency tolerance.		
collaboration	Enable/disable cache-collaboration between cache-service clusters.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable cache cache-collaboration.		
	<i>disable</i>	Disable cache cache-collaboration.		
device-id	Set identifier for this cache device.	string	Maximum length: 35	default_dev_id
acceptable-connections	Set strategy when accepting cache collaboration connection.	option	-	any
	Option	Description		
	<i>any</i>	We can accept any cache-collaboration connection.		
	<i>peers</i>	We can only accept connections that are already in src-peers.		

config dst-peer

Parameter	Description	Type	Size	Default
device-id	Device ID of this peer.	string	Maximum length: 35	
auth-type	Set authentication type for this peer.	integer	Minimum value: 0 Maximum value: 255	0
encode-type	Set encode type for this peer.	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default
priority	Set priority for this peer.	integer	Minimum value: 0 Maximum value: 255	1
ip	Set cluster IP address of this peer.	ipv4-address-any	Not Specified	0.0.0.0

config src-peer

Parameter	Description	Type	Size	Default
device-id	Device ID of this peer.	string	Maximum length: 35	
auth-type	Set authentication type for this peer.	integer	Minimum value: 0 Maximum value: 255	0
encode-type	Set encode type for this peer.	integer	Minimum value: 0 Maximum value: 255	0
priority	Set priority for this peer.	integer	Minimum value: 0 Maximum value: 255	1
ip	Set cluster IP address of this peer.	ipv4-address-any	Not Specified	0.0.0.0

config wanopt content-delivery-network-rule

Configure WAN optimization content delivery network rules.

```
config wanopt content-delivery-network-rule
    Description: Configure WAN optimization content delivery network rules.
    edit <name>
        set comment {var-string}
        set status [enable|disable]
        set host-domain-name-suffix <name1>, <name2>, ...
        set category [vcache|youtube]
        set request-cache-control [enable|disable]
        set response-cache-control [enable|disable]
```

```

set response-expires [enable|disable]
set updateserver [enable|disable]
config rules
    Description: WAN optimization content delivery network rule entries.
    edit <name>
        set match-mode [all|any]
        set skip-rule-mode [all|any]
        config match-entries
            Description: List of entries to match.
            edit <id>
                set target [path|parameter|...]
                set pattern <string1>, <string2>, ...
            next
        end
        config skip-entries
            Description: List of entries to skip.
            edit <id>
                set target [path|parameter|...]
                set pattern <string1>, <string2>, ...
            next
        end
        config content-id
            Description: Content ID settings.
            set target [path|parameter|...]
            set start-str {string}
            set start-skip {integer}
            set start-direction [forward|backward]
            set end-str {string}
            set end-skip {integer}
            set end-direction [forward|backward]
            set range-str {string}
        end
    next
end
next
end

```

config wanopt content-delivery-network-rule

Parameter	Description	Type	Size	Default
name	Name of table.	string	Maximum length: 35	
comment	Comment about this CDN-rule.	var-string	Maximum length: 255	
status	Enable/disable WAN optimization content delivery network rules.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>disable</i>	Disable setting.					
Option	Description									
<i>disable</i>	Disable setting.									
host-domain-name-suffix <name>	Suffix portion of the fully qualified domain name. For example, fortinet.com in "www.fortinet.com". Suffix portion of the fully qualified domain name.	string	Maximum length: 79							
category	Content delivery network rule category.	option	-	vcache						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>vcache</i></td><td>Vcache content delivery network.</td></tr><tr><td><i>youtube</i></td><td>Youtube content delivery network.</td></tr></table>	Option	Description	<i>vcache</i>	Vcache content delivery network.	<i>youtube</i>	Youtube content delivery network.			
Option	Description									
<i>vcache</i>	Vcache content delivery network.									
<i>youtube</i>	Youtube content delivery network.									
request-cache-control	Enable/disable HTTP request cache control.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
response-cache-control	Enable/disable HTTP response cache control.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
response-expires	Enable/disable HTTP response cache expires.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
updateserver	Enable/disable update server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

config rules

Parameter	Description	Type	Size	Default
name	WAN optimization content delivery network rule name.	string	Maximum length: 35	
match-mode	Match criteria for collecting content ID.	option	-	all
	Option	Description		
	all	Must match all of the match entries.		
	any	Must match any of the match entries.		
skip-rule-mode	Skip mode when evaluating skip-rules.	option	-	all
	Option	Description		
	all	Must match all skip entries.		
	any	Must match any skip entries.		

config match-entries

Parameter	Description	Type	Size	Default
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
target	Option in HTTP header or URL parameter to match.	option	-	path
	Option	Description		
	<i>path</i>	Match with the URL path.		
	<i>parameter</i>	Match with the URL parameters.		
	<i>referrer</i>	Match with the Referrer option in HTTP header.		
	<i>youtube-map</i>	Match Youtube content-id collection.		
	<i>youtube-id</i>	Match Youtube content-id.		
	<i>youku-id</i>	Match Youku content-id.		
pattern <string>	Pattern string for matching target (Referrer or URL pattern). For example, a, a*c, *a*, a*c*e, and *. Pattern strings.	string	Maximum length: 79	

config skip-entries

Parameter	Description	Type	Size	Default
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
target	Option in HTTP header or URL parameter to match.	option	-	path
	Option	Description		
	path	Match with the URL path.		
	parameter	Match with the URL parameters.		
	referrer	Match with the Referrer option in HTTP header.		
	youtube-map	Match Youtube content-id collection.		
	youtube-id	Match Youtube content-id.		
	youku-id	Match Youku content-id.		
pattern <string>	Pattern string for matching target (Referrer or URL pattern). For example, a, a*c, *a*, a*c*e, and *. Pattern strings.	string	Maximum length: 79	

config content-id

Parameter	Description	Type	Size	Default
target	Option in HTTP header or URL parameter to match.	option	-	path
	Option	Description		
	path	Match with the URL path.		
	parameter	Match with the URL parameters.		
	referrer	Match with the Referrer option in HTTP header.		
	youtube-map	Match Youtube content-id collection.		
	youtube-id	Match Youtube content-id.		
	youku-id	Match Youku content-id.		
	hls-manifest	Match with HLS manifest.		
	dash-manifest	Match with DASH manifest.		
	hls-fragment	Match HLS stream fragment.		
	dash-fragment	Match DASH stream fragment.		

Parameter	Description	Type	Size	Default						
start-str	String from which to start search.	string	Maximum length: 35							
start-skip	Number of characters in URL to skip after start-str has been matched.	integer	Minimum value: 0 Maximum value: 4294967295	0						
start-direction	Search direction from start-str match.	option	-	forward						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>forward</i></td><td>Forward direction.</td></tr><tr><td><i>backward</i></td><td>Backward direction.</td></tr></table>				Option	Description	<i>forward</i>	Forward direction.	<i>backward</i>	Backward direction.
Option	Description									
<i>forward</i>	Forward direction.									
<i>backward</i>	Backward direction.									
end-str	String from which to end search.	string	Maximum length: 35							
end-skip	Number of characters in URL to skip after end-str has been matched.	integer	Minimum value: 0 Maximum value: 4294967295	0						
end-direction	Search direction from end-str match.	option	-	forward						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>forward</i></td><td>Forward direction.</td></tr><tr><td><i>backward</i></td><td>Backward direction.</td></tr></table>				Option	Description	<i>forward</i>	Forward direction.	<i>backward</i>	Backward direction.
Option	Description									
<i>forward</i>	Forward direction.									
<i>backward</i>	Backward direction.									
range-str	Name of content ID within the start string and end string.	string	Maximum length: 35							

config wanopt peer

Configure WAN optimization peers.

```

config wanopt peer
    Description: Configure WAN optimization peers.
    edit <peer-host-id>
        set ip {ipv4-address-any}
    next
end

```

config wanopt peer

Parameter	Description	Type	Size	Default
peer-host-id	Peer host ID.	string	Maximum length: 35	
ip	Peer IP address.	ipv4-address-any	Not Specified	0.0.0.0

config wanopt profile

Configure WAN optimization profiles.

```

config wanopt profile
    Description: Configure WAN optimization profiles.
    edit <name>
        set transparent [enable|disable]
        set comments {var-string}
        set auth-group {string}
        config http
            Description: Enable/disable HTTP WAN Optimization and configure HTTP WAN
            Optimization features.
            set status [enable|disable]
            set secure-tunnel [enable|disable]
            set byte-caching [enable|disable]
            set ssl [enable|disable]
            set prefer-chunking [dynamic|fix]
            set protocol-opt [protocol|tcp]
            set tunnel-sharing [shared|express-shared|...]
        end
        config cifs
            Description: Enable/disable CIFS (Windows sharing) WAN Optimization and
            configure CIFS WAN Optimization features.
            set status [enable|disable]
            set secure-tunnel [enable|disable]
            set byte-caching [enable|disable]
            set prefer-chunking [dynamic|fix]
            set protocol-opt [protocol|tcp]
            set tunnel-sharing [shared|express-shared|...]
        end
        config mapi
            Description: Enable/disable MAPI email WAN Optimization and configure MAPI WAN
            Optimization features.
            set status [enable|disable]
            set secure-tunnel [enable|disable]
            set byte-caching [enable|disable]
            set tunnel-sharing [shared|express-shared|...]
        end
        config ftp
            Description: Enable/disable FTP WAN Optimization and configure FTP WAN

```

```

Optimization features.
    set status [enable|disable]
    set secure-tunnel [enable|disable]
    set byte-caching [enable|disable]
    set prefer-chunking [dynamic|fix]
    set protocol-opt [protocol|tcp]
    set tunnel-sharing [shared|express-shared|...]
end
config tcp
    Description: Enable/disable TCP WAN Optimization and configure TCP WAN
Optimization features.
    set status [enable|disable]
    set secure-tunnel [enable|disable]
    set byte-caching [enable|disable]
    set byte-caching-opt [mem-only|mem-disk]
    set tunnel-sharing [shared|express-shared|...]
    set port {user}
    set ssl [enable|disable]
    set ssl-port {user}
end
next
end

```

config wanopt profile

Parameter	Description	Type	Size	Default
name	Profile name.	string	Maximum length: 35	
transparent	Enable/disable transparent mode.	option	-	enable
	Option	Description		
	<i>enable</i>	Determine if WAN Optimization changes client packet source addresses. Affects the routing configuration on the server network.		
	<i>disable</i>	Disable transparent mode. Client packets source addresses are changed to the source address of the FortiProxy internal interface. Similar to source NAT.		
comments	Comment.	var-string	Maximum length: 255	
auth-group	Optionally add an authentication group to restrict access to the WAN Optimization tunnel to peers in the authentication group.	string	Maximum length: 35	

config http

Parameter	Description	Type	Size	Default
status	Enable/disable WAN Optimization.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable WAN Optimization.		
	<i>disable</i>	Disable WAN Optimization.		
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable SSL-secured tunnelling.		
	<i>disable</i>	Disable SSL-secured tunnelling.		
byte-caching	Enable/disable byte-caching. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving it from the cache.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable byte-caching.		
	<i>disable</i>	Disable byte-caching.		
ssl	Enable/disable SSL/TLS offloading (hardware acceleration) for traffic in this tunnel.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable SSL/TLS offloading.		
	<i>disable</i>	Disable SSL/TLS offloading.		
prefer-chunking	Select dynamic or fixed-size data chunking for WAN Optimization.	option	-	fix
	Option	Description		
	<i>dynamic</i>	Select dynamic data chunking to help to detect persistent data chunks in a changed file or in an embedded unknown protocol.		
	<i>fix</i>	Select fixed data chunking.		
protocol-opt	Select protocol specific optimization or generic TCP optimization.	option	-	protocol
	Option	Description		
	<i>protocol</i>	Using protocol-specific optimization.		
	<i>tcp</i>	Using generic TCP optimization.		

Parameter	Description	Type	Size	Default
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-	private
	Option Description			
	<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.		
	<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.		
	<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.		

config cifs

Parameter	Description	Type	Size	Default
status	Enable/disable WAN Optimization.	option	-	disable
	Option Description			
	<i>enable</i>	Enable WAN Optimization.		
	<i>disable</i>	Disable WAN Optimization.		
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-	disable
	Option Description			
	<i>enable</i>	Enable SSL-secured tunnelling.		
	<i>disable</i>	Disable SSL-secured tunnelling.		
byte-caching	Enable/disable byte-caching. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache.	option	-	enable
	Option Description			
	<i>enable</i>	Enable byte-caching.		
	<i>disable</i>	Disable byte-caching.		
prefer-chunking	Select dynamic or fixed-size data chunking for WAN Optimization.	option	-	fix

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>dynamic</i>	Select dynamic data chunking to help to detect persistent data chunks in a changed file or in an embedded unknown protocol.		
	<i>fix</i>	Select fixed data chunking.		
protocol-opt	Select protocol specific optimization or generic TCP optimization.	option	-	protocol
	Option	Description		
	<i>protocol</i>	Using protocol-specific optimization.		
	<i>tcp</i>	Using generic TCP optimization.		
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-	private
	Option	Description		
	<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.		
	<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.		
	<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.		

config mapi

Parameter	Description	Type	Size	Default
status	Enable/disable WAN Optimization.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable WAN Optimization.		
	<i>disable</i>	Disable WAN Optimization.		
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable SSL-secured tunnelling.		
	<i>disable</i>	Disable SSL-secured tunnelling.		

Parameter	Description	Type	Size	Default								
byte-caching	Enable/disable byte-caching. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable byte-caching.</td></tr><tr><td><i>disable</i></td><td>Disable byte-caching.</td></tr></table>	Option	Description	<i>enable</i>	Enable byte-caching.	<i>disable</i>	Disable byte-caching.					
Option	Description											
<i>enable</i>	Enable byte-caching.											
<i>disable</i>	Disable byte-caching.											
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-	private								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>shared</i></td><td>For profiles that accept nonaggressive and non-interactive protocols.</td></tr><tr><td><i>express-shared</i></td><td>For profiles that accept interactive protocols such as Telnet.</td></tr><tr><td><i>private</i></td><td>For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.</td></tr></table>	Option	Description	<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.	<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.	<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.			
Option	Description											
<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.											
<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.											
<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.											

config ftp

Parameter	Description	Type	Size	Default
status	Enable/disable WAN Optimization.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable WAN Optimization.		
	<i>disable</i>	Disable WAN Optimization.		
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable SSL-secured tunnelling.		
	<i>disable</i>	Disable SSL-secured tunnelling.		
byte-caching	Enable/disable byte-caching. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable byte-caching.		
	<i>disable</i>	Disable byte-caching.		
prefer-chunking	Select dynamic or fixed-size data chunking for WAN Optimization.	option	-	fix
	Option	Description		
	<i>dynamic</i>	Select dynamic data chunking to help to detect persistent data chunks in a changed file or in an embedded unknown protocol.		
	<i>fix</i>	Select fixed data chunking.		
protocol-opt	Select protocol specific optimization or generic TCP optimization.	option	-	protocol
	Option	Description		
	<i>protocol</i>	Using protocol-specific optimization.		
	<i>tcp</i>	Using generic TCP optimization.		
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-	private
	Option	Description		
	<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.		
	<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.		
	<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.		

config tcp

Parameter	Description	Type	Size	Default
status	Enable/disable WAN Optimization.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable WAN Optimization.		
	<i>disable</i>	Disable WAN Optimization.		

Parameter	Description	Type	Size	Default								
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL-secured tunnelling.</td></tr><tr><td><i>disable</i></td><td>Disable SSL-secured tunnelling.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSL-secured tunnelling.	<i>disable</i>	Disable SSL-secured tunnelling.					
Option	Description											
<i>enable</i>	Enable SSL-secured tunnelling.											
<i>disable</i>	Disable SSL-secured tunnelling.											
byte-caching	Enable/disable byte-caching. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable byte-caching.</td></tr><tr><td><i>disable</i></td><td>Disable byte-caching.</td></tr></table>	Option	Description	<i>enable</i>	Enable byte-caching.	<i>disable</i>	Disable byte-caching.					
Option	Description											
<i>enable</i>	Enable byte-caching.											
<i>disable</i>	Disable byte-caching.											
byte-caching-opt	Select whether TCP byte-caching uses system memory only or both memory and disk space.	option	-	mem-only								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mem-only</i></td><td>Byte caching with memory only.</td></tr><tr><td><i>mem-disk</i></td><td>Byte caching with memory and disk.</td></tr></table>	Option	Description	<i>mem-only</i>	Byte caching with memory only.	<i>mem-disk</i>	Byte caching with memory and disk.					
Option	Description											
<i>mem-only</i>	Byte caching with memory only.											
<i>mem-disk</i>	Byte caching with memory and disk.											
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-	private								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>shared</i></td><td>For profiles that accept nonaggressive and non-interactive protocols.</td></tr><tr><td><i>express-shared</i></td><td>For profiles that accept interactive protocols such as Telnet.</td></tr><tr><td><i>private</i></td><td>For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.</td></tr></table>	Option	Description	<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.	<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.	<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.			
Option	Description											
<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.											
<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.											
<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.											
port	Port numbers or port number ranges for TCP. Only packets with a destination port number that matches this port number or range are accepted by this profile.	user	Not Specified									
ssl	Enable/disable SSL/TLS offloading (hardware acceleration) for traffic in this tunnel.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL/TLS offloading.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSL/TLS offloading.							
Option	Description											
<i>enable</i>	Enable SSL/TLS offloading.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable SSL/TLS offloading.		
ssl-port	Port numbers or port number ranges on which to expect HTTPS traffic for SSL/TLS offloading.	user	Not Specified	

config wanopt remote-storage

Configure a remote cache device as Web cache storage.

```
config wanopt remote-storage
    Description: Configure a remote cache device as Web cache storage.
    set status [disable|enable]
    set local-cache-id {string}
    set remote-cache-id {string}
    set remote-cache-ip {ipv4-address-any}
end
```

config wanopt remote-storage

Parameter	Description	Type	Size	Default
status	Enable/disable using remote device as Web cache storage.	option	-	disable
	Option	Description		
	<i>disable</i>	Use local disks as Web cache storage.		
	<i>enable</i>	Use a remote device as Web cache storage.		
local-cache-id	ID that this device uses to connect to the remote device.	string	Maximum length: 35	
remote-cache-id	ID of the remote device to which the device connects.	string	Maximum length: 35	
remote-cache-ip	IP address of the remote device to which the device connects.	ipv4-address-any	Not Specified	0.0.0.0

config wanopt settings

Configure WAN optimization settings.

```

config wanopt settings
    Description: Configure WAN optimization settings.
    set host-id {string}
    set tunnel-ssl-algorithm [high|medium|...]
    set auto-detect-algorithm [simple|diff-req-resp]
    set tunnel-optimization [memory-usage|balanced|...]
end

```

config wanopt settings

Parameter	Description	Type	Size	Default								
host-id	Local host ID (must also be entered in the remote FortiProxy's peer list).	string	Maximum length: 35	default-id								
tunnel-ssl-algorithm	Relative strength of encryption algorithms accepted during tunnel negotiation.	option	-	high								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high</td><td>High encryption. Allow only AES and ChaCha.</td></tr><tr><td>medium</td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td>low</td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr></table>				Option	Description	high	High encryption. Allow only AES and ChaCha.	medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.
Option	Description											
high	High encryption. Allow only AES and ChaCha.											
medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.											
low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.											
auto-detect-algorithm	Auto detection algorithms used in tunnel negotiations.	option	-	simple								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>simple</td><td>Use the same TCP option value in SYN/SYNACK packets. Backward compatible.</td></tr><tr><td>diff-req-resp</td><td>Use different TCP option values in SYN/SYNACK packets to avoid false positive detection.</td></tr></table>				Option	Description	simple	Use the same TCP option value in SYN/SYNACK packets. Backward compatible.	diff-req-resp	Use different TCP option values in SYN/SYNACK packets to avoid false positive detection.		
Option	Description											
simple	Use the same TCP option value in SYN/SYNACK packets. Backward compatible.											
diff-req-resp	Use different TCP option values in SYN/SYNACK packets to avoid false positive detection.											
tunnel-optimization	WANOpt tunnel optimization option.	option	-	balanced								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>memory-usage</td><td>Optimize tunnel for low system memory usage.</td></tr><tr><td>balanced</td><td>Optimize tunnel to balance between system memory usage and throughput.</td></tr><tr><td>throughput</td><td>Optimize tunnel for throughput.</td></tr></table>				Option	Description	memory-usage	Optimize tunnel for low system memory usage.	balanced	Optimize tunnel to balance between system memory usage and throughput.	throughput	Optimize tunnel for throughput.
Option	Description											
memory-usage	Optimize tunnel for low system memory usage.											
balanced	Optimize tunnel to balance between system memory usage and throughput.											
throughput	Optimize tunnel for throughput.											

web-proxy

This section includes syntax for the following commands:

- [config web-proxy debug-url on page 1159](#)
- [config web-proxy dynamic-bypass on page 1160](#)
- [config web-proxy explicit-proxy on page 1161](#)
- [config web-proxy forward-server-group on page 1167](#)
- [config web-proxy forward-server on page 1168](#)
- [config web-proxy global on page 1170](#)
- [config web-proxy implicit-proxy-rule on page 1175](#)
- [config web-proxy implicit-proxy-setting on page 1177](#)
- [config web-proxy isolator-server on page 1177](#)
- [config web-proxy pac-policy on page 1179](#)
- [config web-proxy profile on page 1180](#)
- [config web-proxy redirect-profile on page 1184](#)
- [config web-proxy url-list on page 1185](#)
- [config web-proxy url-match on page 1187](#)
- [config web-proxy wisp on page 1188](#)

config web-proxy debug-url

Configure debug URL addresses.

```
config web-proxy debug-url
  Description: Configure debug URL addresses.
  edit <name>
    set url-pattern {string}
    set status [enable|disable]
    set exact [enable|disable]
  next
end
```

config web-proxy debug-url

Parameter	Description	Type	Size	Default
name	Debug URL name.	string	Maximum length: 63	
url-pattern	URL exemption pattern.	string	Maximum length: 511	

Parameter	Description	Type	Size	Default
status	Enable/disable this URL exemption.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable this URL exemption.		
	<i>disable</i>	Disable this URL exemption.		
exact	Enable/disable matching the exact path.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable matching the exact path.		
	<i>disable</i>	Disable matching the exact path.		

config web-proxy dynamic-bypass

Configure dynamic bypass settings.

```

config web-proxy dynamic-bypass
    Description: Configure dynamic bypass settings.
    set status [enable|disable]
    set errors {option1}, {option2}, ...
    set total-max {integer}
    set server-max {integer}
    set timeout {integer}
end

```

config web-proxy dynamic-bypass

Parameter	Description	Type	Size	Default
status	Enable/disable dynamic bypass.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable dynamic bypass.		
	<i>disable</i>	Disable dynamic bypass.		
errors	Configure bypass errors.	option	-	
	Option	Description		
	<i>connect-error</i>	Connect error.		
	<i>receive-error</i>	HTTP response is not received.		

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>non-http</i></td><td>HTTP protocol is not detected.</td></tr><tr><td><i>400</i></td><td>HTTP response code is 400.</td></tr><tr><td><i>401</i></td><td>HTTP response code is 401.</td></tr><tr><td><i>403</i></td><td>HTTP response code is 403.</td></tr><tr><td><i>405</i></td><td>HTTP response code is 405.</td></tr><tr><td><i>406</i></td><td>HTTP response code is 406.</td></tr><tr><td><i>500</i></td><td>HTTP response code is 500.</td></tr><tr><td><i>502</i></td><td>HTTP response code is 502.</td></tr><tr><td><i>503</i></td><td>HTTP response code is 503.</td></tr><tr><td><i>504</i></td><td>HTTP response code is 504.</td></tr></table>	Option	Description	<i>non-http</i>	HTTP protocol is not detected.	<i>400</i>	HTTP response code is 400.	<i>401</i>	HTTP response code is 401.	<i>403</i>	HTTP response code is 403.	<i>405</i>	HTTP response code is 405.	<i>406</i>	HTTP response code is 406.	<i>500</i>	HTTP response code is 500.	<i>502</i>	HTTP response code is 502.	<i>503</i>	HTTP response code is 503.	<i>504</i>	HTTP response code is 504.			
	Option	Description																								
	<i>non-http</i>	HTTP protocol is not detected.																								
	<i>400</i>	HTTP response code is 400.																								
	<i>401</i>	HTTP response code is 401.																								
	<i>403</i>	HTTP response code is 403.																								
	<i>405</i>	HTTP response code is 405.																								
	<i>406</i>	HTTP response code is 406.																								
	<i>500</i>	HTTP response code is 500.																								
	<i>502</i>	HTTP response code is 502.																								
	<i>503</i>	HTTP response code is 503.																								
	<i>504</i>	HTTP response code is 504.																								
total-max	Maximum numbers of entries in dynamic bypass list.	integer	Minimum value: 10 Maximum value: 50000	5000																						
server-max	Maximum numbers of entries in dynamic bypass list belongs to one server, all requests to this server will be bypassed once server-max is reached.	integer	Minimum value: 1 Maximum value: 255	16																						
timeout	Maximum time.	integer	Minimum value: 1 Maximum value: 21600	60																						

config web-proxy explicit-proxy

Configure explicit Web proxy settings.

```
config web-proxy explicit-proxy
    Description: Configure explicit Web proxy settings.
    edit <name>
        set status [enable|disable]
        set interface {string}
        set secure-web-proxy [disable|enable|...]
        set http [enable|disable]
        set ftp-over-http [enable|disable]
        set socks [enable|disable]
```

```

set http-incoming-port {user}
set http-connection-mode [static|multiplex|...]
set https-incoming-port {user}
set ftp-incoming-port {user}
set socks-incoming-port {user}
set secure-web-proxy-cert <name1>, <name2>, ...
set ssl-dh-bits [768|1024|...]
set incoming-ip {ipv4-address-any}
set ipv6-status [enable|disable]
set incoming-ip6 {ipv6-address}
set pref-dns-result [ipv4|ipv6|...]
set unknown-http-version [reject|best-effort]
set realm {string}
set sec-default-action [accept|deny]
set pac-file-server-status [enable|disable]
set pac-file-url {user}
set pac-file-server-port {user}
set pac-file-through-https [enable|disable]
set pac-file-name {string}
set pac-file-data {user}
set ssl-algorithm [high|medium|...]
set return-to-sender [enable|disable]
set learn-dst-from-sni [enable|disable]
set dstport-from-incoming [enable|disable]
set header-proxy-agent [enable|disable]
set dns-mode [recursive|non-recursive|...]
next
end

```

config web-proxy explicit-proxy

Parameter	Description	Type	Size	Default						
name	object name	string	Maximum length: 35							
status	Enable/disable the explicit Web proxy for HTTP and HTTPS session.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the explicit web proxy.</td></tr><tr><td><i>disable</i></td><td>Disable the explicit web proxy.</td></tr></table>				Option	Description	<i>enable</i>	Enable the explicit web proxy.	<i>disable</i>	Disable the explicit web proxy.
	Option	Description								
	<i>enable</i>	Enable the explicit web proxy.								
<i>disable</i>	Disable the explicit web proxy.									
interface	interface name	string	Maximum length: 15							
secure-web-proxy	Enable/disable/require the secure web proxy for HTTP and HTTPS session.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable secure webproxy.</td></tr></table>				Option	Description	<i>disable</i>	Disable secure webproxy.		
	Option	Description								
<i>disable</i>	Disable secure webproxy.									

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable secure webproxy access.		
	<i>secure</i>	Require secure webproxy access.		
http	Enable/disable the HTTP & HTTPS proxy.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable the HTTP & HTTPS proxy.		
	<i>disable</i>	Disable the HTTP & HTTPS proxy.		
ftp-over-http	Enable to proxy FTP-over-HTTP sessions sent from a web browser.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable FTP-over-HTTP sessions.		
	<i>disable</i>	Disable FTP-over-HTTP sessions.		
socks	Enable/disable the SOCKS proxy.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable the SOCKS proxy.		
	<i>disable</i>	Disable the SOCKS proxy.		
http-incoming-port	Accept incoming HTTP requests on one or more ports.	user	Not Specified	
http-connection-mode	HTTP connection mode.	option	-	static
	Option	Description		
	<i>static</i>	Only one server connection exists during the proxy session.		
	<i>multiplex</i>	Established connections are held until the proxy session ends.		
	<i>serverpool</i>	Established connections are shared with other proxy sessions.		
https-incoming-port	Accept incoming HTTPS requests on one or more ports.	user	Not Specified	
ftp-incoming-port	Accept incoming FTP-over-HTTP requests on one or more ports.	user	Not Specified	

Parameter	Description	Type	Size	Default										
socks-incoming-port	Accept incoming SOCKS proxy requests on one or more ports.	user	Not Specified											
secure-web-proxy-cert <name>	Name of certificates for secure web proxy. Certificate list.	string	Maximum length: 79											
ssl-dh-bits	Bit-size of Diffie-Hellman.	option	-	2048										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>768</td><td>768-bit Diffie-Hellman prime.</td></tr><tr><td>1024</td><td>1024-bit Diffie-Hellman prime.</td></tr><tr><td>1536</td><td>1536-bit Diffie-Hellman prime.</td></tr><tr><td>2048</td><td>2048-bit Diffie-Hellman prime.</td></tr></table>				Option	Description	768	768-bit Diffie-Hellman prime.	1024	1024-bit Diffie-Hellman prime.	1536	1536-bit Diffie-Hellman prime.	2048	2048-bit Diffie-Hellman prime.
Option	Description													
768	768-bit Diffie-Hellman prime.													
1024	1024-bit Diffie-Hellman prime.													
1536	1536-bit Diffie-Hellman prime.													
2048	2048-bit Diffie-Hellman prime.													
incoming-ip	Restrict the explicit HTTP proxy to only accept sessions from this IP address. An interface must have this IP address.	ipv4-address-any	Not Specified	0.0.0.0										
ipv6-status	Enable/disable allowing an IPv6 web proxy destination in policies and all IPv6 related entries in this command.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable allowing an IPv6 web proxy destination.</td></tr><tr><td>disable</td><td>Disable allowing an IPv6 web proxy destination.</td></tr></table>				Option	Description	enable	Enable allowing an IPv6 web proxy destination.	disable	Disable allowing an IPv6 web proxy destination.				
Option	Description													
enable	Enable allowing an IPv6 web proxy destination.													
disable	Disable allowing an IPv6 web proxy destination.													
incoming-ipv6	Restrict the explicit web proxy to only accept sessions from this IPv6 address. An interface must have this IPv6 address.	ipv6-address	Not Specified	::										
pref-dns-result	Prefer resolving addresses using the configured IPv4 or IPv6 DNS server.	option	-	ipv4										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4</td><td>Send the IPv4 request first and then the IPv6 request. Use the DNS response that returns to the FortiGate first.</td></tr><tr><td>ipv6</td><td>Send the IPv6 request first and then the IPv4 request. Use the DNS response that returns to the FortiGate first.</td></tr><tr><td>ipv4-strict</td><td>Use the IPv4 DNS response. If the IPv6 DNS response arrives first, wait 50ms for the IPv4 response and then use the IPv4 response, otherwise the IPv6.</td></tr><tr><td>ipv6-strict</td><td>Use the IPv6 DNS response. If the IPv4 DNS response arrives first, wait 50ms for the IPv6 response and then use the IPv6 response, otherwise the IPv4.</td></tr></table>				Option	Description	ipv4	Send the IPv4 request first and then the IPv6 request. Use the DNS response that returns to the FortiGate first.	ipv6	Send the IPv6 request first and then the IPv4 request. Use the DNS response that returns to the FortiGate first.	ipv4-strict	Use the IPv4 DNS response. If the IPv6 DNS response arrives first, wait 50ms for the IPv4 response and then use the IPv4 response, otherwise the IPv6.	ipv6-strict	Use the IPv6 DNS response. If the IPv4 DNS response arrives first, wait 50ms for the IPv6 response and then use the IPv6 response, otherwise the IPv4.
Option	Description													
ipv4	Send the IPv4 request first and then the IPv6 request. Use the DNS response that returns to the FortiGate first.													
ipv6	Send the IPv6 request first and then the IPv4 request. Use the DNS response that returns to the FortiGate first.													
ipv4-strict	Use the IPv4 DNS response. If the IPv6 DNS response arrives first, wait 50ms for the IPv4 response and then use the IPv4 response, otherwise the IPv6.													
ipv6-strict	Use the IPv6 DNS response. If the IPv4 DNS response arrives first, wait 50ms for the IPv6 response and then use the IPv6 response, otherwise the IPv4.													

Parameter	Description	Type	Size	Default
unknown-http-version	How to handle HTTP sessions that do not comply with HTTP 0.9, 1.0, or 1.1.	option	-	reject
	Option	Description		
	reject	Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.		
	best-effort	Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.		
realm	Authentication realm used to identify the explicit web proxy (maximum of 63 characters).	string	Maximum length: 63	default
sec-default-action	Accept or deny explicit web proxy sessions when no web proxy firewall policy exists.	option	-	deny
	Option	Description		
	accept	Accept requests. All explicit web proxy traffic is accepted whether there is an explicit web proxy policy or not.		
	deny	Deny requests unless there is a matching explicit web proxy policy.		
pac-file-server-status	Enable/disable Proxy Auto-Configuration (PAC) for users of this explicit proxy profile.	option	-	disable
	Option	Description		
	enable	Enable Proxy Auto-Configuration (PAC).		
	disable	Disable Proxy Auto-Configuration (PAC).		
pac-file-url	PAC file access URL.	user	Not Specified	
pac-file-server-port	Port number that PAC traffic from client web browsers uses to connect to the explicit web proxy.	user	Not Specified	
pac-file-through-https	Enable/disable to get Proxy Auto-Configuration (PAC) through HTTPS.	option	-	disable
	Option	Description		
	enable	Enable to get Proxy Auto-Configuration (PAC) through HTTPS.		
	disable	Disable to get Proxy Auto-Configuration (PAC) through HTTPS.		
pac-file-name	Pac file name.	string	Maximum length: 63	proxy.pac
pac-file-data	PAC file contents enclosed in quotes (maximum of 256K bytes).	user	Not Specified	

Parameter	Description	Type	Size	Default								
ssl-algorithm	Relative strength of encryption algorithms accepted in HTTPS deep scan: high, medium, or low.	option	-	low								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High encription. Allow only AES and ChaCha.</td></tr><tr><td><i>medium</i></td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td><i>low</i></td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr></table>	Option	Description	<i>high</i>	High encription. Allow only AES and ChaCha.	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.			
Option	Description											
<i>high</i>	High encription. Allow only AES and ChaCha.											
<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.											
<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.											
return-to-sender	Enable/disable return-to-sender.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
learn-dst-from-sni	Enable/disable learning destination from SNI in client hello.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable learning destination from SNI in client hello.</td></tr><tr><td><i>disable</i></td><td>Disable learning destination from SNI in client hello.</td></tr></table>	Option	Description	<i>enable</i>	Enable learning destination from SNI in client hello.	<i>disable</i>	Disable learning destination from SNI in client hello.					
Option	Description											
<i>enable</i>	Enable learning destination from SNI in client hello.											
<i>disable</i>	Disable learning destination from SNI in client hello.											
dstport-from-incoming	Enable/disable reusing incoming port to connect to server.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable reusing incoming port to connect to server.</td></tr><tr><td><i>disable</i></td><td>Disable reusing incoming port to connect to server.</td></tr></table>	Option	Description	<i>enable</i>	Enable reusing incoming port to connect to server.	<i>disable</i>	Disable reusing incoming port to connect to server.					
Option	Description											
<i>enable</i>	Enable reusing incoming port to connect to server.											
<i>disable</i>	Disable reusing incoming port to connect to server.											
header-proxy-agent	Enable/disable HTTP CONNECT response header Proxy-Agent.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP CONNECT response header Proxy-Agent.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP CONNECT response header Proxy-Agent.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP CONNECT response header Proxy-Agent.	<i>disable</i>	Disable HTTP CONNECT response header Proxy-Agent.					
Option	Description											
<i>enable</i>	Enable HTTP CONNECT response header Proxy-Agent.											
<i>disable</i>	Disable HTTP CONNECT response header Proxy-Agent.											
dns-mode	DNS lookup mode.	option	-	recursive								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>recursive</i></td><td>Shadow DNS database and forward.</td></tr></table>	Option	Description	<i>recursive</i>	Shadow DNS database and forward.							
Option	Description											
<i>recursive</i>	Shadow DNS database and forward.											

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>non-recursive</i>	Public DNS database only.		
	<i>forward-only</i>	Forward only.		

config web-proxy forward-server-group

Configure a forward server group consisting of multiple forward servers. Supports failover and load balancing.

```
config web-proxy forward-server-group
    Description: Configure a forward server group consisting of multiple forward servers.
    Supports failover and load balancing.
    edit <name>
        set affinity [enable|disable]
        set ldb-method [weighted|least-session|...]
        set group-down-option [block|pass]
        config server-list
            Description: Add web forward servers to a list to form a server group.
            Optionally assign weights to each server.
            edit <name>
                set weight {integer}
            next
        end
    next
end
```

config web-proxy forward-server-group

Parameter	Description	Type	Size	Default
name	Configure a forward server group consisting of one or multiple forward servers. Supports failover and load balancing.	string	Maximum length: 63	
affinity	Enable/disable affinity, attaching a source-ip's traffic to the assigned forwarding server until the forward-server-affinity-timeout is reached (under web-proxy global).	option	-	enable
	Option	Description		
	<i>enable</i>	Enable affinity.		
	<i>disable</i>	Disable affinity.		
ldb-method	Load balance method: weighted or least-session.	option	-	weighted

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>weighted</i>	Load balance traffic to forward servers based on assigned weights. Weights are ratios of total number of sessions.		
	<i>least-session</i>	Send new sessions to the server with lowest session count.		
	<i>active-passive</i>	Send new sessions to the next active server in the list. Servers are selected with highest weight first and then in order as they are configured. Traffic switches back to the first server upon failure recovery.		
group-down-option	Action to take when all of the servers in the forward server group are down: block sessions until at least one server is back up or pass sessions to their destination.	option	-	block
	Option	Description		
	<i>block</i>	Block sessions until at least one server in the group is back up.		
	<i>pass</i>	Pass sessions to their destination bypassing servers in the forward server group.		

config server-list

Parameter	Description	Type	Size	Default
name	Forward server name.	string	Maximum length: 63	
weight	Optionally assign a weight of the forwarding server for weighted load balancing.	integer	Minimum value: 1 Maximum value: 100	10

config web-proxy forward-server

Configure forward-server addresses.

```
config web-proxy forward-server
  Description: Configure forward-server addresses.
  edit <name>
    set addr-type [ip|ipv6|...]
    set ip {ipv4-address-any}
    set ipv6 {ipv6-address}
    set fqdn {string}
    set port {integer}
    set comment {string}
    set masquerade [enable|disable]
```



```

    set protocol {option1}, {option2}, ...
    set ippool <name1>, <name2>, ...
    set healthcheck [disable|enable]
    set monitor {string}
    set server-down-option [block|pass]
    set username {string}
    set password {password}
  next
end

```

config web-proxy forward-server

Parameter	Description	Type	Size	Default
name	Server name.	string	Maximum length: 63	
addr-type	Address type of the forwarding proxy server: IP or FQDN.	option	-	ip
	Option	Description		
	ip	Use an IPv4 address for the forwarding proxy server.		
	ipv6	Use an IPv6 address for the forwarding proxy server.		
	fqdn	Use the FQDN for the forwarding proxy server.		
ip	Forward proxy server IPv4 address.	ipv4-address-any	Not Specified	0.0.0.0
ipv6	Forward proxy server IPv6 address.	ipv6-address	Not Specified	::
fqdn	Forward server Fully Qualified Domain Name (FQDN).	string	Maximum length: 255	
port	Port number that the forwarding server expects to receive HTTP sessions on.	integer	Minimum value: 1 Maximum value: 65535	3128
comment	Comment.	string	Maximum length: 63	
masquerade	set webproxy to use device address to connect proxy server.	option	-	disable
	Option	Description		
	enable	Enable using device address to connect proxy server.		
	disable	Disable using device address to connect proxy server.		

Parameter	Description	Type	Size	Default
protocol	Supported proxy protocols.	option	-	http socks
	Option	Description		
	http	Support forwarding through HTTP proxy.		
	socks	Support forwarding through SOCKS.		
	ftp	Support forwarding through FTP proxy.		
ippool <name>	Name of IP pool object. IP pool name.	string	Maximum length: 79	
healthcheck	Enable/disable forward server health checking. Attempts to connect through the remote forwarding server to a destination to verify that the forwarding server is operating normally.	option	-	disable
	Option	Description		
	disable	Disable health checking.		
	enable	Enable health checking.		
monitor	URL for forward server health check monitoring.	string	Maximum length: 255	www.google.com
server-down-option	Action to take when the forward server is found to be down: block sessions until the server is back up or pass sessions to their destination.	option	-	block
	Option	Description		
	block	Block sessions until the server is back up.		
	pass	Pass sessions to their destination bypassing the forward server.		
username	HTTP authentication user name.	string	Maximum length: 64	
password	HTTP authentication password.	password	Not Specified	

config web-proxy global

Configure Web proxy global settings.

```
config web-proxy global
  Description: Configure Web proxy global settings.
  set ssl-cert {string}
  set ssl-ca-cert {string}
```

```

set fast-policy-match [enable|disable]
set ldap-user-cache [enable|disable]
set use-dynamic-pkey [enable|disable]
set proxy-fqdn {string}
set max-request-length {integer}
set max-message-length {integer}
set strict-web-check [enable|disable]
set forward-proxy-auth [enable|disable]
set forward-server-affinity-timeout {integer}
set webproxy-profile {string}
set learn-client-ip [disable|traffic-process|...]
set learn-client-ip-from-header {option1}, {option2}, ...
set learn-client-ip-srcaddr <name1>, <name2>, ...
set learn-client-ip-srcaddr6 <name1>, <name2>, ...
set src-affinity-exempt-addr {ipv4-address-any}
set src-affinity-exempt-addr6 {ipv6-address}
set strict-guest [enable|disable]
set https-replacement-message [enable|disable]
set message-upon-server-error [enable|disable]
set trace-auth-no-rsp [enable|disable]
set policy-category-deep-inspect [enable|disable]
set log-policy-pending [enable|disable]
set extended-log [enable|disable]
set log-http-transaction [disable|enable]
set log-app-id [enable|disable]
set explicit-outgoing-ip {ipv4-address-any}
set explicit-outgoing-ip6 {ipv6-address}
set realm {string}

```

end

config web-proxy global

Parameter	Description	Type	Size	Default						
ssl-cert	SSL certificate for SSL interception.	string	Maximum length: 35	default-server-cert						
ssl-ca-cert	SSL CA certificate for SSL interception.	string	Maximum length: 35	default-ca						
fast-policy-match	Enable/disable fast matching algorithm for explicit and transparent proxy policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
ldap-user-cache	Enable/disable ldap user cache for explicit and transparent proxy user.	option	-	enable						

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
use-dynamic-pkey	Enable/disable use dynamic private key in the resigned cert.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
proxy-fqdn	Fully Qualified Domain Name to connect to the explicit web proxy.	string	Maximum length: 255	default.fqdn
max-request-length	Maximum length of HTTP request line.	integer	Minimum value: 2 Maximum value: 64	8
max-message-length	Maximum length of HTTP message, not including body.	integer	Minimum value: 16 Maximum value: 256	32
strict-web-check	Enable/disable strict web checking to block web sites that send incorrect headers that don't conform to HTTP 1.1.	option	-	disable
	Option Description			
	<i>enable</i>	Enable strict web checking.		
	<i>disable</i>	Disable strict web checking.		
forward-proxy-auth	Enable/disable forwarding proxy authentication headers.	option	-	disable
	Option Description			
	<i>enable</i>	Enable forwarding proxy authentication headers.		
	<i>disable</i>	Disable forwarding proxy authentication headers.		
forward-server-affinity-timeout	Period of time before the source IP's traffic is no longer assigned to the forwarding server.	integer	Minimum value: 6 Maximum value: 60	30

Parameter	Description	Type	Size	Default								
webproxy-profile	Name of the web proxy profile to apply when explicit proxy traffic is allowed by default and traffic is accepted that does not match an explicit proxy policy.	string	Maximum length: 63									
learn-client-ip	Learn the client's IP address from headers.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not learn the client's IP address from headers.</td></tr><tr><td><i>traffic-process</i></td><td>Learn the client's IP address from headers and use it for both policy-matching and logging.</td></tr><tr><td><i>log-only</i></td><td>Learn the client's IP address from headers and use it only for logging.</td></tr></table>	Option	Description	<i>disable</i>	Do not learn the client's IP address from headers.	<i>traffic-process</i>	Learn the client's IP address from headers and use it for both policy-matching and logging.	<i>log-only</i>	Learn the client's IP address from headers and use it only for logging.			
Option	Description											
<i>disable</i>	Do not learn the client's IP address from headers.											
<i>traffic-process</i>	Learn the client's IP address from headers and use it for both policy-matching and logging.											
<i>log-only</i>	Learn the client's IP address from headers and use it only for logging.											
learn-client-ip-from-header	Learn client IP address from the specified headers.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>true-client-ip</i></td><td>Learn the client IP address from the True-Client-IP header.</td></tr><tr><td><i>x-real-ip</i></td><td>Learn the client IP address from the X-Real-IP header.</td></tr><tr><td><i>x-forwarded-for</i></td><td>Learn the client IP address from the X-Forwarded-For header.</td></tr></table>	Option	Description	<i>true-client-ip</i>	Learn the client IP address from the True-Client-IP header.	<i>x-real-ip</i>	Learn the client IP address from the X-Real-IP header.	<i>x-forwarded-for</i>	Learn the client IP address from the X-Forwarded-For header.			
Option	Description											
<i>true-client-ip</i>	Learn the client IP address from the True-Client-IP header.											
<i>x-real-ip</i>	Learn the client IP address from the X-Real-IP header.											
<i>x-forwarded-for</i>	Learn the client IP address from the X-Forwarded-For header.											
learn-client-ip-srcaddr <name>	Source address name (srcaddr or srcaddr6 must be set). Address name.	string	Maximum length: 79									
learn-client-ip-srcaddr6 <name>	IPv6 Source address name (srcaddr or srcaddr6 must be set). Address name.	string	Maximum length: 79									
src-affinity-exempt-addr	IPv4 source addresses to exempt proxy affinity.	ipv4-address-any	Not Specified									
src-affinity-exempt-addr6	IPv6 source addresses to exempt proxy affinity.	ipv6-address	Not Specified									
strict-guest	Enable/disable strict guest user checking by the explicit web proxy.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable strict guest user checking.</td></tr><tr><td><i>disable</i></td><td>Disable strict guest user checking.</td></tr></table>	Option	Description	<i>enable</i>	Enable strict guest user checking.	<i>disable</i>	Disable strict guest user checking.					
Option	Description											
<i>enable</i>	Enable strict guest user checking.											
<i>disable</i>	Disable strict guest user checking.											

Parameter	Description	Type	Size	Default						
https-replacement-message	Default action to enable or disable return replacement message for HTTPS requests.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Display a replacement message for HTTPS requests.</td></tr><tr><td>disable</td><td>Do not display a replacement message for HTTPS requests.</td></tr></table>	Option	Description	enable	Display a replacement message for HTTPS requests.	disable	Do not display a replacement message for HTTPS requests.			
Option	Description									
enable	Display a replacement message for HTTPS requests.									
disable	Do not display a replacement message for HTTPS requests.									
message-upon-server-error	Enable/disable return of replacement message upon server error detection.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Display a replacement message when a server error is detected.</td></tr><tr><td>disable</td><td>Do not display a replacement message when a server error is detected.</td></tr></table>	Option	Description	enable	Display a replacement message when a server error is detected.	disable	Do not display a replacement message when a server error is detected.			
Option	Description									
enable	Display a replacement message when a server error is detected.									
disable	Do not display a replacement message when a server error is detected.									
trace-auth-no-rsp	Enable/disable logging timed-out authentication requests.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable logging timed-out authentication requests.</td></tr><tr><td>disable</td><td>Disable logging timed-out authentication requests.</td></tr></table>	Option	Description	enable	Enable logging timed-out authentication requests.	disable	Disable logging timed-out authentication requests.			
Option	Description									
enable	Enable logging timed-out authentication requests.									
disable	Disable logging timed-out authentication requests.									
policy-category-deep-inspect	Enable/disable deep inspection for application level category policy matching.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable deep inspection for application level category policy matching.</td></tr><tr><td>disable</td><td>Disable deep inspection for application level category policy matching.</td></tr></table>	Option	Description	enable	Enable deep inspection for application level category policy matching.	disable	Disable deep inspection for application level category policy matching.			
Option	Description									
enable	Enable deep inspection for application level category policy matching.									
disable	Disable deep inspection for application level category policy matching.									
log-policy-pending	Enable/disable logging sessions that are pending on policy matching.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable logging sessions that are pending on policy matching.</td></tr><tr><td>disable</td><td>Disable logging sessions that are pending on policy matching.</td></tr></table>	Option	Description	enable	Enable logging sessions that are pending on policy matching.	disable	Disable logging sessions that are pending on policy matching.			
Option	Description									
enable	Enable logging sessions that are pending on policy matching.									
disable	Disable logging sessions that are pending on policy matching.									
extended-log	Enable/disable extended log of http transaction for implicit policy.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable logging extended http information for implicit policy.		
	<i>disable</i>	Disable logging extended http information for implicit policy.		
log-http-transaction	Enable/disable http transaction log for implicit policy.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable HTTP transaction log.		
	<i>enable</i>	Enable HTTP transaction log		
log-app-id	Enable/disable always log application type in traffic log.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging application type in traffic log.		
	<i>disable</i>	Disable logging application type in traffic log.		
explicit-outgoing-ip	Outgoing HTTP requests by explicit webproxy will have this IP address as their source address. An interface must have this IP address.	ipv4-address-any	Not Specified	
explicit-outgoing-ip6	Outgoing HTTP requests by explicit webproxy will leave this IP. An interface must have this IP address.	ipv6-address	Not Specified	
realm	Authentication realm.	string	Maximum length: 63	default

config web-proxy implicit-proxy-rule

Configure implicit webproxy rule.

```

config web-proxy implicit-proxy-rule
  Description: Configure implicit webproxy rule.
  edit <name>
    set load-balance-method [static|round-robin|...]
    set bypass-list <name1>, <name2>, ...
    config proxy-servers
      Description: Rule proxy server entries.
      edit <id>
        set ip {ipv4-address-any}
        set port {integer}
        set weight {integer}
      next
    end
  end

```

```

    next
end

```

config web-proxy implicit-proxy-rule

Parameter	Description	Type	Size	Default
name	Rule name.	string	Maximum length: 63	
load-balance-method	Method used to distribute sessions to proxies.	option	-	static
	Option	Description		
	static	Distribute to server based on source IP.		
	round-robin	Distribute to server based round robin order.		
	first-alive	Distribute to the first server that is alive.		
	weighted	Distribute to server based on weight.		
bypass-list <name>	Addresses for which you do not want to use any proxy Address name.	string	Maximum length: 79	

config proxy-servers

Parameter	Description	Type	Size	Default
id	Server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	Proxy IP address.	ipv4-address-any	Not Specified	0.0.0.0
port	Proxy port number.	integer	Minimum value: 1 Maximum value: 65535	8080
weight	Weight of the proxy server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255	1

config web-proxy implicit-proxy-setting

Configure implicit proxy browser extension setting.

```
config web-proxy implicit-proxy-setting
  Description: Configure implicit proxy browser extension setting.
  edit <name>
    set interface {string}
    set implicit-proxy-rule {string}
  next
end
```

config web-proxy implicit-proxy-setting

Parameter	Description	Type	Size	Default
name	object name	string	Maximum length: 35	
interface	interface name	string	Maximum length: 15	
implicit-proxy-rule	Implicit proxy rule name	string	Maximum length: 63	

config web-proxy isolator-server

Configure forward-server addresses.

```
config web-proxy isolator-server
  Description: Configure forward-server addresses.
  edit <name>
    set addr-type [ip|ipv6|...]
    set ip {ipv4-address-any}
    set ipv6 {ipv6-address}
    set fqdn {string}
    set port {integer}
    set comment {string}
    set masquerade [enable|disable]
    set protocol {option1}, {option2}, ...
    set ippool <name1>, <name2>, ...
  next
end
```

config web-proxy isolator-server

Parameter	Description	Type	Size	Default
name	Server name.	string	Maximum length: 63	
addr-type	Address type of the forwarding proxy server: IP or FQDN.	option	-	ip
	Option	Description		
	<i>ip</i>	Use an IPv4 address for the forwarding proxy server.		
	<i>ipv6</i>	Use an IPv6 address for the forwarding proxy server.		
	<i>fqdn</i>	Use the FQDN for the forwarding proxy server.		
ip	Forward proxy server IPv4 address.	ipv4-address-any	Not Specified	0.0.0.0
ipv6	Forward proxy server IPv6 address.	ipv6-address	Not Specified	::
fqdn	Forward server Fully Qualified Domain Name (FQDN).	string	Maximum length: 255	
port	Port number that the forwarding server expects to receive HTTP sessions on.	integer	Minimum value: 1 Maximum value: 65535	3128
comment	Comment.	string	Maximum length: 63	
masquerade	set webproxy to use device address to connect proxy server.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable using device address to connect proxy server.		
	<i>disable</i>	Disable using device address to connect proxy server.		
protocol	Supported proxy protocols.	option	-	http socks
	Option	Description		
	<i>http</i>	Support forwarding through HTTP proxy.		
	<i>socks</i>	Support forwarding through SOCKS.		
ippool <name>	Name of IP pool object. IP pool name.	string	Maximum length: 79	

config web-proxy pac-policy

Configure explicit Web proxy pac policy.

```
config web-proxy pac-policy
    Description: Configure explicit Web proxy pac policy.
    edit <policyid>
        set status [enable|disable]
        set srcaddr <name1>, <name2>, ...
        set srcaddr6 <name1>, <name2>, ...
        set dstaddr <name1>, <name2>, ...
        set pac-file-name {string}
        set pac-file-data {user}
        set comments {var-string}
    next
end
```

config web-proxy pac-policy

Parameter	Description	Type	Size	Default
policyid	Policy ID.	integer	Minimum value: 1 Maximum value: 100	0
status	Enable/disable policy.	option	-	enable
	Option	Description		
	enable	Enable policy.		
	disable	Disable policy.		
srcaddr <name>	Source address objects. Address name.	string	Maximum length: 79	
srcaddr6 <name>	Source address6 objects. Address name.	string	Maximum length: 79	
dstaddr <name>	Destination address objects. Address name.	string	Maximum length: 79	
pac-file-name	Pac file name.	string	Maximum length: 63	proxy.pac
pac-file-data	PAC file contents enclosed in quotes (maximum of 256K bytes).	user	Not Specified	
comments	Optional comments.	var-string	Maximum length: 1023	

config web-proxy profile

Configure web proxy profiles.

```
config web-proxy profile
  Description: Configure web proxy profiles.
  edit <name>
    set max-cache-object-size {integer}
    set header-client-ip [pass|add|...]
    set header-via-request [pass|add|...]
    set header-via-response [pass|add|...]
    set header-x-forwarded-for [pass|add|...]
    set header-x-forwarded-client-cert [pass|add|...]
    set header-front-end-https [pass|add|...]
    set header-x-authenticated-user [pass|add|...]
    set header-x-authenticated-groups [pass|add|...]
    set strip-encoding [enable|disable]
    set log-header-change [enable|disable]
  config headers
    Description: Configure HTTP forwarded requests headers.
    edit <id>
      set name {string}
      set dstaddr <name1>, <name2>, ...
      set dstaddr6 <name1>, <name2>, ...
      set action [add-to-request|add-to-response|...]
      set content {string}
      set base64-encoding [disable|enable]
      set add-option [append|new-on-not-found|...]
      set protocol {option1}, {option2}, ...
    next
  end
next
end
```

config web-proxy profile

Parameter	Description	Type	Size	Default
name	Profile name.	string	Maximum length: 63	
max-cache-object-size	Maximum cacheable object size in KB. When the value is set to 0, the max cache object size will be max-object-size under webcache settings.	integer	Minimum value: 0 Maximum value: 3984384	0
header-client-ip	Action to take on the HTTP client-IP header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>pass</i>	Forward the same HTTP header.		
	<i>add</i>	Add the HTTP header.		
	<i>remove</i>	Remove the HTTP header.		
header-via-request	Action to take on the HTTP via header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass
	Option	Description		
	<i>pass</i>	Forward the same HTTP header.		
	<i>add</i>	Add the HTTP header.		
	<i>remove</i>	Remove the HTTP header.		
header-via-response	Action to take on the HTTP via header in forwarded responses: forwards (pass), adds, or removes the HTTP header.	option	-	pass
	Option	Description		
	<i>pass</i>	Forward the same HTTP header.		
	<i>add</i>	Add the HTTP header.		
	<i>remove</i>	Remove the HTTP header.		
header-x-forwarded-for	Action to take on the HTTP x-forwarded-for header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass
	Option	Description		
	<i>pass</i>	Forward the same HTTP header.		
	<i>add</i>	Add the HTTP header.		
	<i>remove</i>	Remove the HTTP header.		
header-x-forwarded-client-cert	Action to take on the HTTP x-forwarded-client-cert header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass
	Option	Description		
	<i>pass</i>	Forward the same HTTP header.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>add</i></td><td>Add the HTTP header.</td></tr><tr><td><i>remove</i></td><td>Remove the HTTP header.</td></tr></table>	Option	Description	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.					
	Option	Description										
	<i>add</i>	Add the HTTP header.										
<i>remove</i>	Remove the HTTP header.											
header-front-end-https	Action to take on the HTTP front-end-HTTPS header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Forward the same HTTP header.</td></tr><tr><td><i>add</i></td><td>Add the HTTP header.</td></tr><tr><td><i>remove</i></td><td>Remove the HTTP header.</td></tr></table>	Option	Description	<i>pass</i>	Forward the same HTTP header.	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.			
	Option	Description										
	<i>pass</i>	Forward the same HTTP header.										
	<i>add</i>	Add the HTTP header.										
<i>remove</i>	Remove the HTTP header.											
header-x-authenticated-user	Action to take on the HTTP x-authenticated-user header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Forward the same HTTP header.</td></tr><tr><td><i>add</i></td><td>Add the HTTP header.</td></tr><tr><td><i>remove</i></td><td>Remove the HTTP header.</td></tr></table>	Option	Description	<i>pass</i>	Forward the same HTTP header.	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.			
	Option	Description										
	<i>pass</i>	Forward the same HTTP header.										
	<i>add</i>	Add the HTTP header.										
<i>remove</i>	Remove the HTTP header.											
header-x-authenticated-groups	Action to take on the HTTP x-authenticated-groups header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Forward the same HTTP header.</td></tr><tr><td><i>add</i></td><td>Add the HTTP header.</td></tr><tr><td><i>remove</i></td><td>Remove the HTTP header.</td></tr></table>	Option	Description	<i>pass</i>	Forward the same HTTP header.	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.			
	Option	Description										
	<i>pass</i>	Forward the same HTTP header.										
	<i>add</i>	Add the HTTP header.										
<i>remove</i>	Remove the HTTP header.											
strip-encoding	Enable/disable stripping unsupported encoding from the request header.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable stripping of unsupported encoding from the request header.</td></tr><tr><td><i>disable</i></td><td>Disable stripping of unsupported encoding from the request header.</td></tr></table>	Option	Description	<i>enable</i>	Enable stripping of unsupported encoding from the request header.	<i>disable</i>	Disable stripping of unsupported encoding from the request header.					
	Option	Description										
	<i>enable</i>	Enable stripping of unsupported encoding from the request header.										
<i>disable</i>	Disable stripping of unsupported encoding from the request header.											
log-header-change	Enable/disable logging HTTP header changes.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable Enable/disable logging HTTP header changes.		
	<i>disable</i>	Disable Enable/disable logging HTTP header changes.		

config headers

Parameter	Description	Type	Size	Default
id	HTTP forwarded header id.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	HTTP forwarded header name.	string	Maximum length: 79	
dstaddr <name>	Destination address and address group names. Address name.	string	Maximum length: 79	
dstaddr6 <name>	Destination address and address group names (IPv6). Address name.	string	Maximum length: 79	
action	Action when the HTTP header is forwarded.	option	-	add-to-request
	Option	Description		
	<i>add-to-request</i>	Add the HTTP header to request.		
	<i>add-to-response</i>	Add the HTTP header to response.		
	<i>remove-from-request</i>	Remove the HTTP header from request.		
	<i>remove-from-response</i>	Remove the HTTP header from response.		
content	HTTP header content.	string	Maximum length: 1023	
base64-encoding	Enable/disable use of base64 encoding of HTTP content.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable use of base64 encoding of HTTP content.		
	<i>enable</i>	Enable use of base64 encoding of HTTP content.		

Parameter	Description	Type	Size	Default												
add-option	Configure options to append content to existing HTTP header or add new HTTP header.	option	-	new												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>append</i></td><td>Append content to existing HTTP header or create new header if HTTP header is not found.</td></tr><tr><td><i>new-on-not-found</i></td><td>Create new header only if existing HTTP header is not found.</td></tr><tr><td><i>new</i></td><td>Create new header regardless if existing HTTP header is found or not.</td></tr><tr><td><i>replace</i></td><td>Replace content to existing HTTP header or create new header if HTTP header is not found.</td></tr><tr><td><i>replace-when-match</i></td><td>Replace content to existing HTTP header.</td></tr></table>	Option	Description	<i>append</i>	Append content to existing HTTP header or create new header if HTTP header is not found.	<i>new-on-not-found</i>	Create new header only if existing HTTP header is not found.	<i>new</i>	Create new header regardless if existing HTTP header is found or not.	<i>replace</i>	Replace content to existing HTTP header or create new header if HTTP header is not found.	<i>replace-when-match</i>	Replace content to existing HTTP header.			
	Option	Description														
	<i>append</i>	Append content to existing HTTP header or create new header if HTTP header is not found.														
	<i>new-on-not-found</i>	Create new header only if existing HTTP header is not found.														
	<i>new</i>	Create new header regardless if existing HTTP header is found or not.														
	<i>replace</i>	Replace content to existing HTTP header or create new header if HTTP header is not found.														
<i>replace-when-match</i>	Replace content to existing HTTP header.															
protocol	Configure protocol(s) to take add-option action on (HTTP, HTTPS, or both).	option	-	https http												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>https</i></td><td>Perform add-option action on HTTPS.</td></tr><tr><td><i>http</i></td><td>Perform add-option action on HTTP.</td></tr></table>	Option	Description	<i>https</i>	Perform add-option action on HTTPS.	<i>http</i>	Perform add-option action on HTTP.									
	Option	Description														
	<i>https</i>	Perform add-option action on HTTPS.														
<i>http</i>	Perform add-option action on HTTP.															

config web-proxy redirect-profile

URL redirect profile.

```

config web-proxy redirect-profile
  Description: URL redirect profile.
  edit <name>
    config entries
      Description: URL redirect entries.
      edit <id>
        set type [simple|regex|...]
        set url {var-string}
        set redirect-url {var-string}
        set redirect-code [auto|301|...]
      next
    end
  next
end

```


config web-proxy redirect-profile

Parameter	Description	Type	Size	Default
name	Name of the redirect profile.	string	Maximum length: 35	

config entries

Parameter	Description	Type	Size	Default
id	Id.	integer	Minimum value: 0 Maximum value: 4294967295	0
type	URL match type (simple, regex or wildcard).	option	-	simple
	OptionDescription			
	simple	Simple URL string.		
	regex	Regular expression URL string.		
	wildcard	Wildcard URL string.		
url	URL to be redirected.	var-string	Maximum length: 1023	
redirect-url	Redirect URL for further web proxy processing.	var-string	Maximum length: 1023	
redirect-code	Redirect code.	option	-	auto
	OptionDescription			
	auto	Auto select status code.		
	301	Status code 301 Move Permanently.		
	302	Status code 302 Move.		
	303	Status code 303 See Other.		
	307	Status code 307 Temporary Redirect.		
	308	Status code 308 Permanent Redirect.		

config web-proxy url-list

URLs for web proxy.

```

config web-proxy url-list
  Description: URLs for web proxy.
  edit <name>
    set comment {var-string}
    config entries
      Description: URL list entries.
      edit <id>
        set status [enable|disable]
        set url {string}
        set type [simple|wildcard]
      next
    end
  next
end

```

config web-proxy url-list

Parameter	Description	Type	Size	Default
name	Configure a name for the URL list.	string	Maximum length: 63	
comment	Comment.	var-string	Maximum length: 255	

config entries

Parameter	Description	Type	Size	Default						
id	Id.	integer	Minimum value: 0 Maximum value: 4294967295	0						
status	Enable/disable the entry.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable The URL.</td></tr><tr><td><i>disable</i></td><td>Disable The URL.</td></tr></table>				Option	Description	<i>enable</i>	Enable The URL.	<i>disable</i>	Disable The URL.
	Option	Description								
	<i>enable</i>	Enable The URL.								
<i>disable</i>	Disable The URL.									
url	URL.	string	Maximum length: 511							
type	URL type (simple, wildcard).	option	-	simple						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>simple</i></td><td>Simple URL string.</td></tr><tr><td><i>wildcard</i></td><td>Wildcard URL string (only **).</td></tr></table>				Option	Description	<i>simple</i>	Simple URL string.	<i>wildcard</i>	Wildcard URL string (only **).
	Option	Description								
	<i>simple</i>	Simple URL string.								
<i>wildcard</i>	Wildcard URL string (only **).									

config web-proxy url-match

URLs to be exempted from caching and/or to be redirected to forward server.

```
config web-proxy url-match
  Description: URLs to be exempted from caching and/or to be redirected to forward server.
  edit <name>
    set status [enable|disable]
    set explicit-web-proxy <name1>, <name2>, ...
    set type [simple|wildcard|...]
    set url-pattern {string}
    set url-list {string}
    set forward-server {string}
    set ftp-forward-server {string}
    set cache-exemption [enable|disable]
    set comment {var-string}
  next
end
```

config web-proxy url-match

Parameter	Description	Type	Size	Default								
name	Configure a name for the URL to be exempted.	string	Maximum length: 63									
status	Enable/disable URLs to be exempted from caching and/or to be redirected to forward server.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable exempting the matching URLs.</td></tr><tr><td><i>disable</i></td><td>Disable exempting the matching URLs.</td></tr></table>	Option	Description	<i>enable</i>	Enable exempting the matching URLs.	<i>disable</i>	Disable exempting the matching URLs.					
Option	Description											
<i>enable</i>	Enable exempting the matching URLs.											
<i>disable</i>	Disable exempting the matching URLs.											
explicit-web-proxy <name>	Explicit Web proxy names. Explicit Web proxy name.	string	Maximum length: 79									
type	URL type (simple, wildcard, list).	option	-	simple								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>simple</i></td><td>Simple URL string.</td></tr><tr><td><i>wildcard</i></td><td>Wildcard URL string (only '*').</td></tr><tr><td><i>list</i></td><td>URL list.</td></tr></table>	Option	Description	<i>simple</i>	Simple URL string.	<i>wildcard</i>	Wildcard URL string (only '*').	<i>list</i>	URL list.			
Option	Description											
<i>simple</i>	Simple URL string.											
<i>wildcard</i>	Wildcard URL string (only '*').											
<i>list</i>	URL list.											
url-pattern	URL pattern to be exempted from caching and/or to be redirected to forward server.	string	Maximum length: 511									
url-list	URL list to be exempted from caching and/or to be redirected to forward server.	string	Maximum length: 63									

Parameter	Description	Type	Size	Default
forward-server	Forward server name.	string	Maximum length: 63	
ftp-forward-server	ftp forward server name.	string	Maximum length: 63	
cache-exemption	Enable/disable exempting this URL pattern from caching.	option	-	disable
	Option	Description		
	enable	Enable exempting this URL pattern from caching.		
	disable	Disable exempting this URL pattern from caching.		
comment	Comment.	var-string	Maximum length: 255	

config web-proxy wisp

Configure Websense Integrated Services Protocol (WISP) servers.

```

config web-proxy wisp
    Description: Configure Websense Integrated Services Protocol (WISP) servers.
    edit <name>
        set comment {var-string}
        set outgoing-ip {ipv4-address-any}
        set server-ip {ipv4-address-any}
        set server-port {integer}
        set max-connections {integer}
        set timeout {integer}
    next
end

```

config web-proxy wisp

Parameter	Description	Type	Size	Default
name	Server name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
outgoing-ip	WISP outgoing IP address.	ipv4-address-any	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
server-ip	WISP server IP address.	ipv4-address-any	Not Specified	0.0.0.0
server-port	WISP server port.	integer	Minimum value: 1 Maximum value: 65535	15868
max-connections	Maximum number of web proxy WISP connections.	integer	Minimum value: 4 Maximum value: 4096	64
timeout	Period of time before WISP requests time out.	integer	Minimum value: 1 Maximum value: 15	5

webcache

This section includes syntax for the following commands:

- [config webcache prefetch on page 1190](#)
- [config webcache reverse-cache-server on page 1191](#)
- [config webcache settings on page 1192](#)
- [config webcache user-agent on page 1196](#)

config webcache prefetch

Configure cache prefetch.

```
config webcache prefetch
  Description: Configure cache prefetch.
  edit <name>
    set url {string}
    set crawl-depth {integer}
    set ignore-robots [enable|disable]
    set interval {integer}
    set start-delay {integer}
    set repeat {integer}
    set user {string}
    set password {password}
    set user-agent <name1>, <name2>, ...
  next
end
```

config webcache prefetch

Parameter	Description	Type	Size	Default
name	Name of the prefetch item.	string	Maximum length: 35	
url	URL of the target.	string	Maximum length: 1023	
crawl-depth	Depth to crawl the whole url.	integer	Minimum value: 0 Maximum value: 16	0
ignore-robots	Ignore robots.txt specification.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Ignore robots.txt config while crawling the url.		
	<i>disable</i>	Obey robots.txt config while crawling the url.		
interval	Time interval (in seconds) to fetch the url.	integer	Minimum value: 0 Maximum value: 608400	43200
start-delay	Delay period to start the fetching (in secondss).	integer	Minimum value: 0 Maximum value: 2422800	0
repeat	How many times repeat to fetch the url.	integer	Minimum value: 0 Maximum value: 4294967295	0
user	Username for the Web resource.	string	Maximum length: 64	
password	Password for the Web resource.	password	Not Specified	
user-agent <name>	User agents can be used by this prefetch. User agent.	string	Maximum length: 79	

config webcache reverse-cache-server

Configure reverse cache server.

```

config webcache reverse-cache-server
    Description: Configure reverse cache server.
    edit <name>
        set ip {ipv4-address-any}
        set port {integer}
        set status [enable|disable]
        set priority {integer}
    next
end

```

config webcache reverse-cache-server

Parameter	Description	Type	Size	Default
name	Name of the reverse cache server	string	Maximum length: 35	
ip	Server IP address.	ipv4-address-any	Not Specified	0.0.0.0
port	Server port.	integer	Minimum value: 1 Maximum value: 65535	80
status	Enable/disable the cache server.	option	-	enable
	Option		Description	
	enable		Enable the reverse-cache-server.	
	disable		Disable the reverse-cache-server.	
priority	Priority of the cache server (reserved).	integer	Minimum value: 0 Maximum value: 15	0

config webcache settings

Configure global Web cache settings.

```
config webcache settings
    Description: Configure global Web cache settings.
    set max-object-size {integer}
    set neg-resp-time {integer}
    set fresh-factor {integer}
    set max-ttl {integer}
    set min-ttl {integer}
    set default-ttl {integer}
    set ignore-ims [enable|disable]
    set ignore-conditional [enable|disable]
    set ignore-pnc [enable|disable]
    set ignore-ie-reload [enable|disable]
    set cache-expired [enable|disable]
    set cache-cookie [enable|disable]
    set reval-pnc [enable|disable]
    set always-revalidate [enable|disable]
    set cache-by-default [enable|disable]
    set host-validate [enable|disable]
```



```

set add-x-cache [enable|disable]
set x-cache-message {string}
set external [enable|disable]
set crawler-user-agent {string}
end

```

config webcache settings

Parameter	Description	Type	Size	Default
max-object-size	Maximum cacheable object size in kB. All objects that exceed this are delivered to the client but not stored in the web cache.	integer	Minimum value: 1 Maximum value: 2147483	512000
neg-resp-time	Time in minutes to cache negative responses or errors.	integer	Minimum value: 0 Maximum value: 4294967295	0
fresh-factor	Frequency that the server is checked to see if any objects have expired. The higher the fresh factor, the less often the checks occur.	integer	Minimum value: 1 Maximum value: 100	100
max-ttl	Maximum time an object can stay in the web cache without checking to see if it has expired on the server.	integer	Minimum value: 1 Maximum value: 5256000	7200
min-ttl	Minimum time an object can stay in the web cache without checking to see if it has expired on the server.	integer	Minimum value: 1 Maximum value: 5256000	5
default-ttl	Default object expiry time. This only applies to those objects that do not have an expiry time set by the web server.	integer	Minimum value: 1 Maximum value: 5256000	1440
ignore-ims	Enable/disable ignoring the if-modified-since (IMS) header.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable ignoring the if-modified-since (IMS) header.	
		<i>disable</i>	Disable ignoring the if-modified-since (IMS) header.	

Parameter	Description	Type	Size	Default						
ignore-conditional	Enable/disable controlling the behavior of cache-control HTTP 1.1 header values.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ignoring cache-control HTTP 1.1 header values.</td></tr><tr><td><i>disable</i></td><td>Disable ignoring cache-control HTTP 1.1 header values.</td></tr></table>	Option	Description	<i>enable</i>	Enable ignoring cache-control HTTP 1.1 header values.	<i>disable</i>	Disable ignoring cache-control HTTP 1.1 header values.			
Option	Description									
<i>enable</i>	Enable ignoring cache-control HTTP 1.1 header values.									
<i>disable</i>	Disable ignoring cache-control HTTP 1.1 header values.									
ignore-pnc	Enable/disable ignoring the pragma no-cache (PNC) header.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ignoring the pragma no-cache (PNC) header.</td></tr><tr><td><i>disable</i></td><td>Disable ignoring the pragma no-cache (PNC) header.</td></tr></table>	Option	Description	<i>enable</i>	Enable ignoring the pragma no-cache (PNC) header.	<i>disable</i>	Disable ignoring the pragma no-cache (PNC) header.			
Option	Description									
<i>enable</i>	Enable ignoring the pragma no-cache (PNC) header.									
<i>disable</i>	Disable ignoring the pragma no-cache (PNC) header.									
ignore-ie-reload	Enable/disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.</td></tr><tr><td><i>disable</i></td><td>Disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.</td></tr></table>	Option	Description	<i>enable</i>	Enable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.	<i>disable</i>	Disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.			
Option	Description									
<i>enable</i>	Enable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.									
<i>disable</i>	Disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.									
cache-expired	Enable/disable caching type-1 objects that are already expired on arrival.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable caching type-1 objects that have expired.</td></tr><tr><td><i>disable</i></td><td>Disable caching type-1 objects that have expired.</td></tr></table>	Option	Description	<i>enable</i>	Enable caching type-1 objects that have expired.	<i>disable</i>	Disable caching type-1 objects that have expired.			
Option	Description									
<i>enable</i>	Enable caching type-1 objects that have expired.									
<i>disable</i>	Disable caching type-1 objects that have expired.									
cache-cookie	Enable/disable caching cookies. Since cookies contain information for or about individual users, they not usually cached.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Cache cookies.</td></tr><tr><td><i>disable</i></td><td>Do not cache cookies.</td></tr></table>	Option	Description	<i>enable</i>	Cache cookies.	<i>disable</i>	Do not cache cookies.			
Option	Description									
<i>enable</i>	Cache cookies.									
<i>disable</i>	Do not cache cookies.									
reval-pnc	Enable/disable revalidation of pragma-no-cache (PNC) to address bandwidth concerns.	option	-	disable						

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable revalidation of pragma-no-cache (PNC).		
	<i>disable</i>	Disable revalidation of pragma-no-cache (PNC).		
always-revalidate	Enable/disable revalidation of requested cached objects, which have content on the server, before serving it to the client.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable revalidation of requested cached objects.		
	<i>disable</i>	Disable revalidation of requested cached objects.		
cache-by-default	Enable/disable caching content that lacks explicit caching policies from the server.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable caching content that lacks explicit caching policies.		
	<i>disable</i>	Disable caching content that lacks explicit caching policies.		
host-validate	Enable/disable validating "Host:" with original server IP.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable validating "Host:" with original server IP.		
	<i>disable</i>	Disable validating "Host:" with original server IP.		
add-x-cache	Enable/disable appending local "X-Cache: HIT/MISS" information when http-request is cacheable.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
x-cache-message	Config customized x-cache header message.	string	Maximum length: 400	
external	Enable/disable external Web caching.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable external Web caching		
	<i>disable</i>	Disable external Web caching		

Parameter	Description	Type	Size	Default
crawler-user-agent	The user agent that the web crawler will use.	string	Maximum length: 255	fpx

config webcache user-agent

Configure reverse cache user agent.

```
config webcache user-agent
  Description: Configure reverse cache user agent.
  edit <name>
    set value {string}
  next
end
```

config webcache user-agent

Parameter	Description	Type	Size	Default
name	Name of the user agent item.	string	Maximum length: 35	
value	User agent of the URL.	string	Maximum length: 255	

webfilter

This section includes syntax for the following commands:

- [config webfilter categories on page 1197](#)
- [config webfilter content-header on page 1197](#)
- [config webfilter content on page 1199](#)
- [config webfilter domain-list on page 1200](#)
- [config webfilter fortiguard on page 1201](#)
- [config webfilter ftgd-local-cat on page 1204](#)
- [config webfilter ftgd-local-rating on page 1204](#)
- [config webfilter ftgd-local-risk on page 1205](#)
- [config webfilter ftgd-risk-level on page 1206](#)
- [config webfilter ftgd-statistics on page 1206](#)
- [config webfilter ips-urlfilter-cache-setting on page 1207](#)
- [config webfilter ips-urlfilter-setting on page 1207](#)
- [config webfilter ips-urlfilter-setting6 on page 1208](#)
- [config webfilter override-usr on page 1209](#)
- [config webfilter override on page 1209](#)
- [config webfilter profile on page 1210](#)
- [config webfilter search-engine on page 1227](#)
- [config webfilter status on page 1229](#)
- [config webfilter url-list on page 1229](#)
- [config webfilter urlfilter on page 1230](#)

config webfilter categories

List the FortiGuard Web Filter category descriptions.

```
config webfilter categories
    Description: List the FortiGuard Web Filter category descriptions.
end
```

config webfilter content-header

Configure content types used by Web filter.

```
config webfilter content-header
    Description: Configure content types used by Web filter.
    edit <id>
```

```

set name {string}
set comment {var-string}
config entries
    Description: Configure content types used by web filter.
    edit <pattern>
        set action [block|allow|...]
        set category {user}
    next
end
next
end

```

config webfilter content-header

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

config entries

Parameter	Description	Type	Size	Default
pattern	Content type (regular expression).	string	Maximum length: 31	
action	Action to take for this content type.	option	-	allow
	Option Description			
	<i>block</i>	Block content type.		
	<i>allow</i>	Allow content type.		
	<i>exempt</i>	Exempt content type.		
category	Categories that this content type applies to.	user	Not Specified	all

config webfilter content

Configure Web filter banned word table.

```
config webfilter content
  Description: Configure Web filter banned word table.
  edit <id>
    set name {string}
    set comment {var-string}
    config entries
      Description: Configure banned word entries.
      edit <name>
        set pattern-type [wildcard|regexp]
        set status [enable|disable]
        set lang [western|simch|...]
        set score {integer}
        set action [block|exempt]
      next
    end
  next
end
```

config webfilter content

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table.	string	Maximum length: 63	
comment	Optional comments.	var-string	Maximum length: 255	

config entries

Parameter	Description	Type	Size	Default
name	Banned word.	string	Maximum length: 127	
pattern-type	Banned word pattern type: wildcard pattern or Perl regular expression.	option	-	wildcard

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>wildcard</i>	Wildcard pattern.		
	<i>regex</i>	Perl regular expression.		
status	Enable/disable banned word.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
lang	Language of banned word.	option	-	western
	Option	Description		
	<i>western</i>	Western.		
	<i>simch</i>	Simplified Chinese.		
	<i>trach</i>	Traditional Chinese.		
	<i>japanese</i>	Japanese.		
	<i>korean</i>	Korean.		
	<i>french</i>	French.		
	<i>thai</i>	Thai.		
	<i>spanish</i>	Spanish.		
	<i>cyrillic</i>	Cyrillic.		
score	Score, to be applied every time the word appears on a web page.	integer	Minimum value: 0 Maximum value: 4294967295	10
action	Block or exempt word when a match is found.	option	-	block
	Option	Description		
	<i>block</i>	Block matches.		
	<i>exempt</i>	Exempt matches.		

config webfilter domain-list

Configure Web filter Domain list.


```

config webfilter domain-list
    Description: Configure Web filter Domain list.
    edit <name>
        set uuid {uuid}
        set status [enable|disable]
        set comment {var-string}
        config entries
            Description: Domain list entries.
            edit <domain>
                next
            end
        next
    end
end

```

config webfilter domain-list

Parameter	Description	Type	Size	Default						
name	Domain list name.	string	Maximum length: 35							
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
status	Enable/disable Domain list.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Domain list.</td></tr><tr><td><i>disable</i></td><td>Disable Domain list.</td></tr></table>				Option	Description	<i>enable</i>	Enable Domain list.	<i>disable</i>	Disable Domain list.
	Option	Description								
	<i>enable</i>	Enable Domain list.								
<i>disable</i>	Disable Domain list.									
comment	Comment.	var-string	Maximum length: 255							

config entries

Parameter	Description	Type	Size	Default
domain	Domain.	string	Maximum length: 511	

config webfilter fortiguard

Configure FortiGuard Web Filter service.

```

config webfilter fortiguard
    Description: Configure FortiGuard Web Filter service.
    set cache-mode [ttl|db-ver]

```

```

set cache-prefix-match [enable|disable]
set cache-mem-percent {integer}
set ovr-auth-port-http {integer}
set ovr-auth-port-https {integer}
set ovr-auth-port-https-flow {integer}
set ovr-auth-port-warning {integer}
set ovr-auth-https [enable|disable]
set warn-auth-https [enable|disable]
set close-ports [enable|disable]
set request-packet-size-limit {integer}
set embed-image [enable|disable]

```

end

config webfilter fortiguard

Parameter	Description	Type	Size	Default
cache-mode	Cache entry expiration mode.	option	-	tll
	Option	Description		
	<i>tll</i>	Expire cache items by time-to-live.		
	<i>db-ver</i>	Expire cache items when the server DB version changes.		
cache-prefix-match	Enable/disable prefix matching in the cache.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
cache-mem-percent	Maximum percentage of available memory allocated to caching.	integer	Minimum value: 1 Maximum value: 15	2
ovrd-auth-port-http	Port to use for FortiGuard Web Filter HTTP override authentication.	integer	Minimum value: 0 Maximum value: 65535	8008
ovrd-auth-port-https	Port to use for FortiGuard Web Filter HTTPS override authentication in proxy mode.	integer	Minimum value: 0 Maximum value: 65535	8010

Parameter	Description	Type	Size	Default						
ovrd-auth-port-https-flow	Port to use for FortiGuard Web Filter HTTPS override authentication in flow mode.	integer	Minimum value: 0 Maximum value: 65535	8015						
ovrd-auth-port-warning	Port to use for FortiGuard Web Filter Warning override authentication.	integer	Minimum value: 0 Maximum value: 65535	8020						
ovrd-auth-https	Enable/disable use of HTTPS for override authentication.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
warn-auth-https	Enable/disable use of HTTPS for warning and authentication.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
close-ports	Close ports used for HTTP/HTTPS override authentication and disable user overrides.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
request-packet-size-limit	Limit size of URL request packets sent to FortiGuard server.	integer	Minimum value: 576 Maximum value: 10000	0						
embed-image	Enable/disable embedding images into replacement messages.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

config webfilter ftgd-local-cat

Configure FortiGuard Web Filter local categories.

```
config webfilter ftgd-local-cat
    Description: Configure FortiGuard Web Filter local categories.
    edit <desc>
        set status [enable|disable]
        set id {integer}
    next
end
```

config webfilter ftgd-local-cat

Parameter	Description	Type	Size	Default
status	Enable/disable the local category.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable the local category.		
	<i>disable</i>	Disable the local category.		
id	Local category ID.	integer	Minimum value: 140 Maximum value: 191	0
desc	Local category description.	string	Maximum length: 79	

config webfilter ftgd-local-rating

Configure local FortiGuard Web Filter local ratings.

```
config webfilter ftgd-local-rating
    Description: Configure local FortiGuard Web Filter local ratings.
    edit <url>
        set status [enable|disable]
        set comment {var-string}
        set rating {user}
    next
end
```

config webfilter ftgd-local-rating

Parameter	Description	Type	Size	Default
url	URL to rate locally.	string	Maximum length: 511	
status	Enable/disable local rating.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local rating.		
	<i>disable</i>	Disable local rating.		
comment	Comment.	var-string	Maximum length: 255	
rating	Local rating.	user	Not Specified	

config webfilter ftgd-local-risk

Configure FortiGuard Web Filter local risk score.

```
config webfilter ftgd-local-risk
    Description: Configure FortiGuard Web Filter local risk score.
    edit <url>
        set status [enable|disable]
        set comment {var-string}
        set risk-score {integer}
    next
end
```

config webfilter ftgd-local-risk

Parameter	Description	Type	Size	Default
url	URL to rate locally.	string	Maximum length: 511	
status	Enable/disable local risk score.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable local risk level.		
	<i>disable</i>	Disable local risk level.		

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
risk-score	Local risk score.	integer	Minimum value: 0 Maximum value: 100	0

config webfilter ftgd-risk-level

Configure FortiGuard Web Filter risk level.

```
config webfilter ftgd-risk-level
    Description: Configure FortiGuard Web Filter risk level.
    edit <name>
        set high {integer}
        set low {integer}
    next
end
```

config webfilter ftgd-risk-level

Parameter	Description	Type	Size	Default
name	Risk level name.	string	Maximum length: 35	
high	Risk level high.	integer	Minimum value: 0 Maximum value: 100	0
low	Risk level low.	integer	Minimum value: 0 Maximum value: 100	0

config webfilter ftgd-statistics

Display rating cache and daemon statistics.

```
config webfilter ftgd-statistics
    Description: Display rating cache and daemon statistics.
end
```

config webfilter ips-urlfilter-cache-setting

Configure IPS URL filter cache settings.

```
config webfilter ips-urlfilter-cache-setting
    Description: Configure IPS URL filter cache settings.
    set dns-retry-interval {integer}
    set extended-ttl {integer}
end
```

config webfilter ips-urlfilter-cache-setting

Parameter	Description	Type	Size	Default
dns-retry-interval	Retry interval. Refresh DNS faster than TTL to capture multiple IPs for hosts. 0 means use DNS server's TTL only.	integer	Minimum value: 0 Maximum value: 2147483	0
extended-ttl	Extend time to live beyond reported by DNS. Use of 0 means use DNS server's TTL.	integer	Minimum value: 0 Maximum value: 2147483	0

config webfilter ips-urlfilter-setting

Configure IPS URL filter settings.

```
config webfilter ips-urlfilter-setting
    Description: Configure IPS URL filter settings.
    set device {string}
    set distance {integer}
    set gateway {ipv4-address}
    set geo-filter {var-string}
end
```

config webfilter ips-urlfilter-setting

Parameter	Description	Type	Size	Default
device	Interface for this route.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
distance	Administrative distance for this route.	integer	Minimum value: 1 Maximum value: 255	1
gateway	Gateway IP address for this route.	ipv4-address	Not Specified	0.0.0.0
geo-filter	Filter based on geographical location. Route will NOT be installed if the resolved IP address belongs to the country in the filter.	var-string	Maximum length: 255	

config webfilter ips-urlfilter-setting6

Configure IPS URL filter settings for IPv6.

```
config webfilter ips-urlfilter-setting6
    Description: Configure IPS URL filter settings for IPv6.
    set device {string}
    set distance {integer}
    set gateway6 {ipv6-address}
    set geo-filter {var-string}
end
```

config webfilter ips-urlfilter-setting6

Parameter	Description	Type	Size	Default
device	Interface for this route.	string	Maximum length: 35	
distance	Administrative distance for this route.	integer	Minimum value: 1 Maximum value: 255	1
gateway6	Gateway IPv6 address for this route.	ipv6-address	Not Specified	::
geo-filter	Filter based on geographical location. Route will NOT be installed if the resolved IPv6 address belongs to the country in the filter.	var-string	Maximum length: 255	

config webfilter override-usr

Display list of user overrides.

```
config webfilter override-usr
    Description: Display list of user overrides.
end
```

config webfilter override

Configure FortiGuard Web Filter administrative overrides.

```
config webfilter override
    Description: Configure FortiGuard Web Filter administrative overrides.
    edit <id>
        set status [enable|disable]
        set scope [user|user-group|...]
        set ip {ipv4-address}
        set user {string}
        set user-group {string}
        set old-profile {string}
        set new-profile {string}
        set ip6 {ipv6-address}
        set expires {user}
        set initiator {string}
    next
end
```

config webfilter override

Parameter	Description	Type	Size	Default
id	Override rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Enable/disable override rule.	option	-	disable
	Option	Description		
	enable	Enable override rule.		
	disable	Disable override rule.		
scope	Override either the specific user, user group, IPv4 address, or IPv6 address.	option	-	user

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>user</i>	Override the specified user.		
	<i>user-group</i>	Override the specified user group.		
	<i>ip</i>	Override the specified IP address.		
	<i>ip6</i>	Override the specified IPv6 address.		
ip	IPv4 address which the override applies.	ipv4-address	Not Specified	0.0.0.0
user	Name of the user which the override applies.	string	Maximum length: 64	
user-group	Specify the user group for which the override applies.	string	Maximum length: 63	
old-profile	Name of the web filter profile which the override applies.	string	Maximum length: 35	
new-profile	Name of the new web filter profile used by the override.	string	Maximum length: 35	
ip6	IPv6 address which the override applies.	ipv6-address	Not Specified	::
expires	Override expiration date and time, from 5 minutes to 365 from now (format: yyyy/mm/dd hh:mm:ss).	user	Not Specified	1970/01/01 12:00:00
initiator	Initiating user of override (read-only setting).	string	Maximum length: 64	

config webfilter profile

Configure Web filter profiles.

```
config webfilter profile
    Description: Configure Web filter profiles.
    edit <name>
        set comment {var-string}
        set replacemsg-group {string}
        set options {option1}, {option2}, ...
        set https-replacemsg [enable|disable]
        set ovr-d-perm {option1}, {option2}, ...
        set post-action [normal|block]
        config override
            Description: Web Filter override settings.
            set ovr-d-cookie [allow|deny]
            set ovr-d-scope [user|user-group|...]
            set profile-type [list|radius]
```

```
    set ovr-dur-mode [constant|ask]
    set ovr-dur {user}
    set profile-attribute [User-Name|NAS-IP-Address|...]
    set ovr-user-group <name1>, <name2>, ...
    set profile <name1>, <name2>, ...
end
config web
    Description: Web content filtering settings.
    set bword-threshold {integer}
    set bword-table {integer}
    set urlfilter-table {integer}
    set content-header-list {integer}
    set blocklist [enable|disable]
    set allowlist {option1}, {option2}, ...
    set safe-search {option1}, {option2}, ...
    set youtube-restrict [none|strict|...]
    set qwant-restrict [none|strict|...]
    set vimeo-restrict {string}
    set log-search [enable|disable]
    set keyword-match <pattern1>, <pattern2>, ...
end
config ftgd-wf
    Description: FortiGuard Web Filter settings.
    set options {option1}, {option2}, ...
    set exempt-quota {user}
    set ovr {user}
    config filters
        Description: FortiGuard filters.
        edit <id>
            set category {integer}
            set action [block|authenticate|...]
            set warn-duration {user}
            set auth-usr-grp <name1>, <name2>, ...
            set log [enable|disable]
            set override-replacemsg {string}
            set warning-prompt [per-domain|per-category]
            set warning-duration-type [session|timeout]
        next
    end
    config risk
        Description: FortiGuard risk level settings.
        edit <id>
            set risk-level {string}
            set action [block|monitor]
            set log [enable|disable]
        next
    end
    config quota
        Description: FortiGuard traffic quota settings.
        edit <id>
            set category {user}
            set type [time|traffic]
            set unit [B|KB|...]
            set value {integer}
            set duration {user}
            set override-replacemsg {string}
```

```
        next
    end
    set max-quota-timeout {integer}
    set rate-javascript-urls [disable|enable]
    set rate-css-urls [disable|enable]
    set rate-crl-urls [disable|enable]
end
config antiphish
    Description: AntiPhishing profile.
    set status [enable|disable]
    set default-action [exempt|log|...]
    set check-uri [enable|disable]
    set check-basic-auth [enable|disable]
    set check-username-only [enable|disable]
    set max-body-len {integer}
    config inspection-entries
        Description: AntiPhishing entries.
        edit <name>
            set fortiguard-category {user}
            set action [exempt|log|...]
        next
    end
    config custom-patterns
        Description: Custom username and password regex patterns.
        edit <pattern>
            set category [username|password]
            set type [regex|literal]
        next
    end
    set authentication [domain-controller|ldap]
    set domain-controller {string}
    set ldap {string}
end
set wisp [enable|disable]
set wisp-servers <name1>, <name2>, ...
set wisp-algorithm [primary-secondary|round-robin|...]
set ia-categorization [enable|disable]
set log-all-url [enable|disable]
set web-content-log [enable|disable]
set web-filter-activex-log [enable|disable]
set web-filter-command-block-log [enable|disable]
set web-filter-cookie-log [enable|disable]
set web-filter-applet-log [enable|disable]
set web-filter-jscript-log [enable|disable]
set web-filter-js-log [enable|disable]
set web-filter-vbs-log [enable|disable]
set web-filter-unknown-log [enable|disable]
set web-filter-referer-log [enable|disable]
set web-filter-cookie-removal-log [enable|disable]
set web-url-log [enable|disable]
set web-invalid-domain-log [enable|disable]
set web-ftgd-err-log [enable|disable]
set web-ftgd-quota-usage [enable|disable]
set web-antiphishing-log [enable|disable]
next
end
```

config webfilter profile

Parameter	Description	Type	Size	Default
name	Profile name.	string	Maximum length: 35	
comment	Optional comments.	var-string	Maximum length: 255	
replacemsg-group	Replacement message group.	string	Maximum length: 35	
options	Options.	option	-	
	OptionDescription			
	activexfilter	ActiveX filter.		
	cookiefilter	Cookie filter.		
	javafilter	Java applet filter.		
	block-invalid-url	Block sessions contained an invalid domain name.		
	jscript	Javascript block.		
	js	JS block.		
	vbs	VB script block.		
	unknown	Unknown script block.		
	intrinsic	Intrinsic script block.		
	wf-referer	Referring block.		
	wf-cookie	Cookie block.		
	per-user-bal	Per-user block/allow list filter		
https-replacemsg	Enable replacement messages for HTTPS.	option	-	enable
	OptionDescription			
	enable	Enable setting.		
	disable	Disable setting.		
ovrd-perm	Permitted override types.	option	-	
	OptionDescription			
	bannedword-override	Banned word override.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>urlfilter-override</i>	URL filter override.		
	<i>fortiguard-wf-override</i>	FortiGuard Web Filter override.		
	<i>contenttype-check-override</i>	Content-type header override.		
post-action	Action taken for HTTP POST traffic.	option	-	normal
	Option	Description		
	<i>normal</i>	Normal, POST requests are allowed.		
	<i>block</i>	POST requests are blocked.		
wisp	Enable/disable web proxy WISP.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable web proxy WISP.		
	<i>disable</i>	Disable web proxy WISP.		
wisp-servers <name>	WISP servers. Server name.	string	Maximum length: 79	
wisp-algorithm	WISP server selection algorithm.	option	-	auto-learning
	Option	Description		
	<i>primary-secondary</i>	Select the first healthy server in order.		
	<i>round-robin</i>	Select the next healthy server.		
	<i>auto-learning</i>	Select the lightest loading healthy server.		
ia-categorization	Enable/Disable use of image-analyzer engine to help categorize images with unknown category.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
log-all-url	Enable/disable logging all URLs visited.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-content-log	Enable/disable logging logging blocked web content.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-activex-log	Enable/disable logging ActiveX.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-command-block-log	Enable/disable logging blocked commands.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-cookie-log	Enable/disable logging cookie filtering.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-applet-log	Enable/disable logging Java applets.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-jscript-log	Enable/disable logging JScripts.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-js-log	Enable/disable logging Java scripts.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-vbs-log	Enable/disable logging VBS scripts.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-unknown-log	Enable/disable logging unknown scripts.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-referer-log	Enable/disable logging referrers.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-cookie-removal-log	Enable/disable logging blocked cookies.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-url-log	Enable/disable logging URL filtering.	option	-	enable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-invalid-domain-log	Enable/disable logging invalid domain names.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-ftgd-err-log	Enable/disable logging rating errors.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-ftgd-quota-usage	Enable/disable logging daily quota usage.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-antiphishing-log	Enable/disable logging of AntiPhishing checks.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config override

Parameter	Description	Type	Size	Default
ovrd-cookie	Allow/deny browser-based (cookie) overrides.	option	-	deny
	Option	Description		
	<i>allow</i>	Allow browser-based (cookie) override.		
	<i>deny</i>	Deny browser-based (cookie) override.		

Parameter	Description	Type	Size	Default																
ovrd-scope	Override scope.	option	-	user																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>user</i></td><td>Override for the user.</td></tr><tr><td><i>user-group</i></td><td>Override for the user's group.</td></tr><tr><td><i>ip</i></td><td>Override for the initiating IP.</td></tr><tr><td><i>browser</i></td><td>Create browser-based (cookie) override.</td></tr><tr><td><i>ask</i></td><td>Prompt for scope when initiating an override.</td></tr></table>	Option	Description	<i>user</i>	Override for the user.	<i>user-group</i>	Override for the user's group.	<i>ip</i>	Override for the initiating IP.	<i>browser</i>	Create browser-based (cookie) override.	<i>ask</i>	Prompt for scope when initiating an override.							
Option	Description																			
<i>user</i>	Override for the user.																			
<i>user-group</i>	Override for the user's group.																			
<i>ip</i>	Override for the initiating IP.																			
<i>browser</i>	Create browser-based (cookie) override.																			
<i>ask</i>	Prompt for scope when initiating an override.																			
profile-type	Override profile type.	option	-	list																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>list</i></td><td>Profile chosen from list.</td></tr><tr><td><i>radius</i></td><td>Profile determined by RADIUS server.</td></tr></table>	Option	Description	<i>list</i>	Profile chosen from list.	<i>radius</i>	Profile determined by RADIUS server.													
Option	Description																			
<i>list</i>	Profile chosen from list.																			
<i>radius</i>	Profile determined by RADIUS server.																			
ovrd-dur-mode	Override duration mode.	option	-	constant																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>constant</i></td><td>Constant mode.</td></tr><tr><td><i>ask</i></td><td>Prompt for duration when initiating an override.</td></tr></table>	Option	Description	<i>constant</i>	Constant mode.	<i>ask</i>	Prompt for duration when initiating an override.													
Option	Description																			
<i>constant</i>	Constant mode.																			
<i>ask</i>	Prompt for duration when initiating an override.																			
ovrd-dur	Override duration.	user	Not Specified	15m																
profile-attribute	Profile attribute to retrieve from the RADIUS server.	option	-	Login-LAT-Service																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>User-Name</i></td><td>Use this attribute.</td></tr><tr><td><i>NAS-IP-Address</i></td><td>Use this attribute.</td></tr><tr><td><i>Framed-IP-Address</i></td><td>Use this attribute.</td></tr><tr><td><i>Framed-IP-Netmask</i></td><td>Use this attribute.</td></tr><tr><td><i>Filter-Id</i></td><td>Use this attribute.</td></tr><tr><td><i>Login-IP-Host</i></td><td>Use this attribute.</td></tr><tr><td><i>Reply-Message</i></td><td>Use this attribute.</td></tr></table>	Option	Description	<i>User-Name</i>	Use this attribute.	<i>NAS-IP-Address</i>	Use this attribute.	<i>Framed-IP-Address</i>	Use this attribute.	<i>Framed-IP-Netmask</i>	Use this attribute.	<i>Filter-Id</i>	Use this attribute.	<i>Login-IP-Host</i>	Use this attribute.	<i>Reply-Message</i>	Use this attribute.			
Option	Description																			
<i>User-Name</i>	Use this attribute.																			
<i>NAS-IP-Address</i>	Use this attribute.																			
<i>Framed-IP-Address</i>	Use this attribute.																			
<i>Framed-IP-Netmask</i>	Use this attribute.																			
<i>Filter-Id</i>	Use this attribute.																			
<i>Login-IP-Host</i>	Use this attribute.																			
<i>Reply-Message</i>	Use this attribute.																			

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>Callback-Number</i>	Use this attribute.		
	<i>Callback-Id</i>	Use this attribute.		
	<i>Framed-Route</i>	Use this attribute.		
	<i>Framed-IPX-Network</i>	Use this attribute.		
	<i>Class</i>	Use this attribute.		
	<i>Called-Station-Id</i>	Use this attribute.		
	<i>Calling-Station-Id</i>	Use this attribute.		
	<i>NAS-Identifier</i>	Use this attribute.		
	<i>Proxy-State</i>	Use this attribute.		
	<i>Login-LAT-Service</i>	Use this attribute.		
	<i>Login-LAT-Node</i>	Use this attribute.		
	<i>Login-LAT-Group</i>	Use this attribute.		
	<i>Framed-AppleTalk-Zone</i>	Use this attribute.		
	<i>Acct-Session-Id</i>	Use this attribute.		
	<i>Acct-Multi-Session-Id</i>	Use this attribute.		
ovrd-user-group <name>	User groups with permission to use the override. User group name.	string	Maximum length: 79	
profile <name>	Web filter profile with permission to create overrides. Web profile.	string	Maximum length: 79	

config web

Parameter	Description	Type	Size	Default												
bword-threshold	Banned word score threshold.	integer	Minimum value: 0 Maximum value: 2147483647	10												
bword-table	Banned word table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0												
urlfilter-table	URL filter table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0												
content-header-list	Content header list.	integer	Minimum value: 0 Maximum value: 4294967295	0												
blocklist	Enable/disable automatic addition of URLs detected by FortiSandbox to blocklist.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.						
Option	Description															
enable	Enable setting.															
disable	Disable setting.															
allowlist	FortiGuard allowlist settings.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>exempt-av</td><td>Exempt antivirus.</td></tr><tr><td>exempt-webcontent</td><td>Exempt web content.</td></tr><tr><td>exempt-activex-java-cookie</td><td>Exempt ActiveX-JAVA-Cookie.</td></tr><tr><td>exempt-dlp</td><td>Exempt DLP.</td></tr><tr><td>exempt-rangeblock</td><td>Exempt RangeBlock.</td></tr></table>				Option	Description	exempt-av	Exempt antivirus.	exempt-webcontent	Exempt web content.	exempt-activex-java-cookie	Exempt ActiveX-JAVA-Cookie.	exempt-dlp	Exempt DLP.	exempt-rangeblock	Exempt RangeBlock.
Option	Description															
exempt-av	Exempt antivirus.															
exempt-webcontent	Exempt web content.															
exempt-activex-java-cookie	Exempt ActiveX-JAVA-Cookie.															
exempt-dlp	Exempt DLP.															
exempt-rangeblock	Exempt RangeBlock.															

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>extended-log-others</i></td><td>Support extended log.</td></tr></table>				Option	Description	<i>extended-log-others</i>	Support extended log.				
Option	Description											
<i>extended-log-others</i>	Support extended log.											
safe-search	Safe search type.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>url</i></td><td>Insert safe search string into URL.</td></tr><tr><td><i>header</i></td><td>Insert safe search header.</td></tr></table>				Option	Description	<i>url</i>	Insert safe search string into URL.	<i>header</i>	Insert safe search header.		
Option	Description											
<i>url</i>	Insert safe search string into URL.											
<i>header</i>	Insert safe search header.											
youtube-restrict	YouTube EDU filter level.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Full access for YouTube.</td></tr><tr><td><i>strict</i></td><td>Strict access for YouTube.</td></tr><tr><td><i>moderate</i></td><td>Moderate access for YouTube.</td></tr></table>				Option	Description	<i>none</i>	Full access for YouTube.	<i>strict</i>	Strict access for YouTube.	<i>moderate</i>	Moderate access for YouTube.
Option	Description											
<i>none</i>	Full access for YouTube.											
<i>strict</i>	Strict access for YouTube.											
<i>moderate</i>	Moderate access for YouTube.											
qwant-restrict	Qwant safe search level.	option	-	strict								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Full access for Qwant.</td></tr><tr><td><i>strict</i></td><td>Strict access for Qwant.</td></tr><tr><td><i>moderate</i></td><td>Moderate access for Qwant.</td></tr></table>				Option	Description	<i>none</i>	Full access for Qwant.	<i>strict</i>	Strict access for Qwant.	<i>moderate</i>	Moderate access for Qwant.
Option	Description											
<i>none</i>	Full access for Qwant.											
<i>strict</i>	Strict access for Qwant.											
<i>moderate</i>	Moderate access for Qwant.											
vimeo-restrict	Set Vimeo-restrict ("7" = don't show mature content, "134" = don't show unrated and mature content). A value of cookie "content_rating".	string	Maximum length: 63									
log-search	Enable/disable logging all search phrases.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
keyword-match <pattern>	Search keywords to log when match is found. Pattern/keyword to search for.	string	Maximum length: 79									

config ftgd-wf

Parameter	Description	Type	Size	Default										
options	Options for FortiGuard Web Filter.	option	-	ftgd-disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>error-allow</i></td><td>Allow web pages with a rating error to pass through.</td></tr><tr><td><i>rate-server-ip</i></td><td>Rate the server IP in addition to the domain name.</td></tr><tr><td><i>connect-request-bypass</i></td><td>Bypass connection which has CONNECT request.</td></tr><tr><td><i>ftgd-disable</i></td><td>Disable FortiGuard scanning.</td></tr></table>	Option	Description	<i>error-allow</i>	Allow web pages with a rating error to pass through.	<i>rate-server-ip</i>	Rate the server IP in addition to the domain name.	<i>connect-request-bypass</i>	Bypass connection which has CONNECT request.	<i>ftgd-disable</i>	Disable FortiGuard scanning.			
	Option	Description												
	<i>error-allow</i>	Allow web pages with a rating error to pass through.												
	<i>rate-server-ip</i>	Rate the server IP in addition to the domain name.												
	<i>connect-request-bypass</i>	Bypass connection which has CONNECT request.												
<i>ftgd-disable</i>	Disable FortiGuard scanning.													
exempt-quota	Do not stop quota for these categories.	user	Not Specified	17										
ovrd	Allow web filter profile overrides.	user	Not Specified											
max-quota-timeout	Maximum FortiGuard quota used by single page view in seconds (excludes streams).	integer	Minimum value: 1 Maximum value: 86400	300										
rate-javascript-urls	Enable/disable rating JavaScript by URL.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable rating JavaScript by URL.</td></tr><tr><td><i>enable</i></td><td>Enable rating JavaScript by URL.</td></tr></table>	Option	Description	<i>disable</i>	Disable rating JavaScript by URL.	<i>enable</i>	Enable rating JavaScript by URL.							
	Option	Description												
	<i>disable</i>	Disable rating JavaScript by URL.												
<i>enable</i>	Enable rating JavaScript by URL.													
rate-css-urls	Enable/disable rating CSS by URL.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable rating CSS by URL.</td></tr><tr><td><i>enable</i></td><td>Enable rating CSS by URL.</td></tr></table>	Option	Description	<i>disable</i>	Disable rating CSS by URL.	<i>enable</i>	Enable rating CSS by URL.							
	Option	Description												
	<i>disable</i>	Disable rating CSS by URL.												
<i>enable</i>	Enable rating CSS by URL.													
rate-crl-urls	Enable/disable rating CRL by URL.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable rating CRL by URL.</td></tr><tr><td><i>enable</i></td><td>Enable rating CRL by URL.</td></tr></table>	Option	Description	<i>disable</i>	Disable rating CRL by URL.	<i>enable</i>	Enable rating CRL by URL.							
	Option	Description												
	<i>disable</i>	Disable rating CRL by URL.												
<i>enable</i>	Enable rating CRL by URL.													

config filters

Parameter	Description	Type	Size	Default										
id	ID number.	integer	Minimum value: 0 Maximum value: 255	0										
category	Categories and groups the filter examines.	integer	Minimum value: 0 Maximum value: 255	0										
action	Action to take for matches.	option	-	monitor										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Block access.</td></tr><tr><td><i>authenticate</i></td><td>Authenticate user before allowing access.</td></tr><tr><td><i>monitor</i></td><td>Allow access while logging the action.</td></tr><tr><td><i>warning</i></td><td>Allow access after warning the user.</td></tr></table>	Option	Description	<i>block</i>	Block access.	<i>authenticate</i>	Authenticate user before allowing access.	<i>monitor</i>	Allow access while logging the action.	<i>warning</i>	Allow access after warning the user.			
Option	Description													
<i>block</i>	Block access.													
<i>authenticate</i>	Authenticate user before allowing access.													
<i>monitor</i>	Allow access while logging the action.													
<i>warning</i>	Allow access after warning the user.													
warn-duration	Duration of warnings.	user	Not Specified	5m										
auth-usr-grp <name>	Groups with permission to authenticate. User group name.	string	Maximum length: 79											
log	Enable/disable logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
override-replacemsg	Override replacement message.	string	Maximum length: 28											
warning-prompt	Warning prompts in each category or each domain.	option	-	per-category										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>per-domain</i></td><td>Per-domain warnings.</td></tr><tr><td><i>per-category</i></td><td>Per-category warnings.</td></tr></table>	Option	Description	<i>per-domain</i>	Per-domain warnings.	<i>per-category</i>	Per-category warnings.							
Option	Description													
<i>per-domain</i>	Per-domain warnings.													
<i>per-category</i>	Per-category warnings.													
warning-duration-type	Re-display warning after closing browser or after a timeout.	option	-	timeout										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>session</i>	After session ends.		
	<i>timeout</i>	After timeout occurs.		

config risk

Parameter	Description	Type	Size	Default
id	ID number.	integer	Minimum value: 0 Maximum value: 255	0
risk-level	Risk level to be examined.	string	Maximum length: 35	
action	Action to take for matches.	option	-	monitor
	Option	Description		
	<i>block</i>	Block access.		
	<i>monitor</i>	Allow access while logging the action.		
log	Enable/disable logging.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

config quota

Parameter	Description	Type	Size	Default
id	ID number.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	FortiGuard categories to apply quota to (category action must be set to monitor).	user	Not Specified	
type	Quota type.	option	-	time

Parameter	Description	Type	Size	Default
	Option	Description		
	time	Use a time-based quota.		
	traffic	Use a traffic-based quota.		
unit	Traffic quota unit of measurement.	option	-	MB
	Option	Description		
	B	Quota in bytes.		
	KB	Quota in kilobytes.		
	MB	Quota in megabytes.		
	GB	Quota in gigabytes.		
value	Traffic quota value.	integer	Minimum value: 1 Maximum value: 4294967295	1024
duration	Duration of quota.	user	Not Specified	5m
override-replacemsg	Override replacement message.	string	Maximum length: 28	

config antiphish

Parameter	Description	Type	Size	Default								
status	Toggle AntiPhishing functionality.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AntiPhishing functionality.</td></tr><tr><td><i>disable</i></td><td>Disable AntiPhishing functionality.</td></tr></table>				Option	Description	<i>enable</i>	Enable AntiPhishing functionality.	<i>disable</i>	Disable AntiPhishing functionality.		
	Option	Description										
	<i>enable</i>	Enable AntiPhishing functionality.										
	<i>disable</i>	Disable AntiPhishing functionality.										
default-action	Action to be taken when there is no matching rule.	option	-	exempt								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>exempt</i></td><td>Exempt requests from matching.</td></tr><tr><td><i>log</i></td><td>Log all matched requests.</td></tr><tr><td><i>block</i></td><td>Block all matched requests.</td></tr></table>				Option	Description	<i>exempt</i>	Exempt requests from matching.	<i>log</i>	Log all matched requests.	<i>block</i>	Block all matched requests.
	Option	Description										
	<i>exempt</i>	Exempt requests from matching.										
	<i>log</i>	Log all matched requests.										
<i>block</i>	Block all matched requests.											
check-uri	Enable/disable checking of GET URI parameters for known credentials.	option	-	disable								

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable checking of GET URI for username and password fields.		
	<i>disable</i>	Disable checking of GET URI for username and password fields.		
check-basic-auth	Enable/disable checking of HTTP Basic Auth field for known credentials.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable checking of HTTP Basic Auth field for known credentials.		
	<i>disable</i>	Disable checking of HTTP Basic Auth field for known credentials.		
check-username-only	Enable/disable username only matching of credentials. Action will be taken for valid usernames regardless of password validity.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable username only credential matches.		
	<i>disable</i>	Disable username only credential matches.		
max-body-len	Maximum size of a POST body to check for credentials.	integer	Minimum value: 0 Maximum value: 4294967295	65536
authentication	Authentication methods.	option	-	domain-controller
	Option	Description		
	<i>domain-controller</i>	Domain Controller to verify user credential.		
	<i>ldap</i>	LDAP to verify user credential.		
domain-controller	Domain for which to verify received credentials against.	string	Maximum length: 63	
ldap	LDAP server for which to verify received credentials against.	string	Maximum length: 63	

config inspection-entries

Parameter	Description	Type	Size	Default								
name	Inspection target name.	string	Maximum length: 63									
fortiguard-category	FortiGuard category to match.	user	Not Specified	0								
action	Action to be taken upon an AntiPhishing match.	option	-	exempt								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>exempt</i></td><td>Exempt requests from matching.</td></tr><tr><td><i>log</i></td><td>Log all matched requests.</td></tr><tr><td><i>block</i></td><td>Block all matched requests.</td></tr></table>				Option	Description	<i>exempt</i>	Exempt requests from matching.	<i>log</i>	Log all matched requests.	<i>block</i>	Block all matched requests.
Option	Description											
<i>exempt</i>	Exempt requests from matching.											
<i>log</i>	Log all matched requests.											
<i>block</i>	Block all matched requests.											

config custom-patterns

Parameter	Description	Type	Size	Default						
pattern	Target pattern.	string	Maximum length: 255							
category	Category that the pattern matches.	option	-	username						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>username</i></td><td>Pattern matches username fields.</td></tr><tr><td><i>password</i></td><td>Pattern matches password fields.</td></tr></table>				Option	Description	<i>username</i>	Pattern matches username fields.	<i>password</i>	Pattern matches password fields.
	Option	Description								
	<i>username</i>	Pattern matches username fields.								
<i>password</i>	Pattern matches password fields.									
type	Pattern will be treated either as a regex pattern or literal string.	option	-	regex						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>regex</i></td><td>Pattern will be treated as a regex pattern.</td></tr><tr><td><i>literal</i></td><td>Pattern will be treated as a literal string.</td></tr></table>				Option	Description	<i>regex</i>	Pattern will be treated as a regex pattern.	<i>literal</i>	Pattern will be treated as a literal string.
	Option	Description								
	<i>regex</i>	Pattern will be treated as a regex pattern.								
<i>literal</i>	Pattern will be treated as a literal string.									

config webfilter search-engine

Configure web filter search engines.

```
config webfilter search-engine
  Description: Configure web filter search engines.
  edit <name>
    set hostname {string}
```

```

        set url {string}
        set query {string}
        set safesearch [disable|url|...]
        set charset [utf-8|gb2312]
        set source-url [enable|disable]
        set safesearch-str {string}
    next
end

```

config webfilter search-engine

Parameter	Description	Type	Size	Default
name	Search engine name.	string	Maximum length: 35	
hostname	Hostname (regular expression).	string	Maximum length: 127	
url	URL (regular expression).	string	Maximum length: 127	
query	Code used to prefix a query (must end with an equals character).	string	Maximum length: 15	
safesearch	Safe search method. You can disable safe search, add the safe search string to URLs, or insert a safe search header.	option	-	disable
	Option	Description		
	<i>disable</i>	Site does not support safe search.		
	<i>url</i>	Safe search selected with a parameter in the URL.		
	<i>header</i>	Safe search selected by search header (i.e. youtube.edu).		
	<i>translate</i>	Perform URL FortiGuard check on translated URL.		
	<i>yt-pattern</i>	Pattern to match YouTube channel ID.		
	<i>yt-scan</i>	Perform IPS scan.		
	<i>yt-video</i>	Pattern to match YouTube video name.		
	<i>yt-channel</i>	Pattern to match YouTube channel name.		
charset	Search engine charset.	option	-	utf-8
	Option	Description		
	<i>utf-8</i>	UTF-8 encoding.		
	<i>gb2312</i>	GB2312 encoding.		
source-url	Enable/disable source url in the image search result.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable source url in image search.		
	<i>disable</i>	Disable source url in image search.		
safesearch-str	Safe search parameter used in the URL in URL mode. In translate mode, it provides either the regex to translate the URL or the special case to translate the URL.	string	Maximum length: 255	

config webfilter status

Display rating info.

```
config webfilter status
    Description: Display rating info.
    set <refresh-rate> {string}
end
```

config webfilter status

Parameter	Description	Type	Size	Default
<refresh-rate>	Frequency to refresh the server list (sec).	string	Maximum length: -	

config webfilter url-list

Configure Web filter URL list.

```
config webfilter url-list
    Description: Configure Web filter URL list.
    edit <name>
        set uuid {uuid}
        set status [enable|disable]
        set comment {var-string}
        config entries
            Description: URL list entries.
            edit <url>
                next
            end
        end
    next
end
```

config webfilter url-list

Parameter	Description	Type	Size	Default						
name	URL list name.	string	Maximum length: 35							
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
status	Enable/disable URL list.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable URL list.</td></tr><tr><td><i>disable</i></td><td>Disable URL list.</td></tr></table>				Option	Description	<i>enable</i>	Enable URL list.	<i>disable</i>	Disable URL list.
	Option	Description								
	<i>enable</i>	Enable URL list.								
<i>disable</i>	Disable URL list.									
comment	Comment.	var-string	Maximum length: 255							

config entries

Parameter	Description	Type	Size	Default
url	URL.	string	Maximum length: 511	

config webfilter urlfilter

Configure URL filter lists.

```
config webfilter urlfilter
  Description: Configure URL filter lists.
  edit <id>
    set name {string}
    set comment {var-string}
    set one-arm-ips-urlfilter [enable|disable]
    set ip-addr-block [enable|disable]
    set ip4-mapped-ip6 [enable|disable]
    config entries
      Description: URL filter entries.
      edit <id>
        set url {string}
        set type [simple|regex|...]
        set action [exempt|block|...]
        set antiphish-action [block|log]
        set status [enable|disable]
        set exempt {option1}, {option2}, ...
```

```

        set web-proxy-profile {string}
        set referrer-host {string}
        set dns-address-family [ipv4|ipv6|...]
    next
end
next
end

```

config webfilter urlfilter

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
name	Name of URL filter list.	string	Maximum length: 63							
comment	Optional comments.	var-string	Maximum length: 255							
one-arm-ips-urlfilter	Enable/disable DNS resolver for one-arm IPS URL filter operation.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DNS resolver for one-arm IPS URL filter operation.</td></tr><tr><td><i>disable</i></td><td>Disable DNS resolver for one-arm IPS URL filter operation.</td></tr></table>				Option	Description	<i>enable</i>	Enable DNS resolver for one-arm IPS URL filter operation.	<i>disable</i>	Disable DNS resolver for one-arm IPS URL filter operation.
Option	Description									
<i>enable</i>	Enable DNS resolver for one-arm IPS URL filter operation.									
<i>disable</i>	Disable DNS resolver for one-arm IPS URL filter operation.									
ip-addr-block	Enable/disable blocking URLs when the hostname appears as an IP address.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable blocking URLs when the hostname appears as an IP address.</td></tr><tr><td><i>disable</i></td><td>Disable blocking URLs when the hostname appears as an IP address.</td></tr></table>				Option	Description	<i>enable</i>	Enable blocking URLs when the hostname appears as an IP address.	<i>disable</i>	Disable blocking URLs when the hostname appears as an IP address.
Option	Description									
<i>enable</i>	Enable blocking URLs when the hostname appears as an IP address.									
<i>disable</i>	Disable blocking URLs when the hostname appears as an IP address.									
ip4-mapped-ip6	Enable/disable matching of IPv4 mapped IPv6 URLs.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable matching IPv4 mapped IPv6 URLs.</td></tr><tr><td><i>disable</i></td><td>Disable matching IPv4 mapped IPv6 URLs.</td></tr></table>				Option	Description	<i>enable</i>	Enable matching IPv4 mapped IPv6 URLs.	<i>disable</i>	Disable matching IPv4 mapped IPv6 URLs.
Option	Description									
<i>enable</i>	Enable matching IPv4 mapped IPv6 URLs.									
<i>disable</i>	Disable matching IPv4 mapped IPv6 URLs.									

config entries

Parameter	Description	Type	Size	Default										
id	Id.	integer	Minimum value: 0 Maximum value: 4294967295	0										
url	URL to be filtered.	string	Maximum length: 511											
type	Filter type (simple, regex, or wildcard).	option	-	simple										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>simple</i></td><td>Simple URL string.</td></tr><tr><td><i>regex</i></td><td>Regular expression URL string.</td></tr><tr><td><i>wildcard</i></td><td>Wildcard URL string.</td></tr></table>				Option	Description	<i>simple</i>	Simple URL string.	<i>regex</i>	Regular expression URL string.	<i>wildcard</i>	Wildcard URL string.		
Option	Description													
<i>simple</i>	Simple URL string.													
<i>regex</i>	Regular expression URL string.													
<i>wildcard</i>	Wildcard URL string.													
action	Action to take for URL filter matches.	option	-	exempt										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>exempt</i></td><td>Exempt matches.</td></tr><tr><td><i>block</i></td><td>Block matches.</td></tr><tr><td><i>allow</i></td><td>Allow matches (no log).</td></tr><tr><td><i>monitor</i></td><td>Allow matches (with log).</td></tr></table>				Option	Description	<i>exempt</i>	Exempt matches.	<i>block</i>	Block matches.	<i>allow</i>	Allow matches (no log).	<i>monitor</i>	Allow matches (with log).
Option	Description													
<i>exempt</i>	Exempt matches.													
<i>block</i>	Block matches.													
<i>allow</i>	Allow matches (no log).													
<i>monitor</i>	Allow matches (with log).													
antiphish-action	Action to take for AntiPhishing matches.	option	-	block										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Block matches.</td></tr><tr><td><i>log</i></td><td>Allow matches with log.</td></tr></table>				Option	Description	<i>block</i>	Block matches.	<i>log</i>	Allow matches with log.				
Option	Description													
<i>block</i>	Block matches.													
<i>log</i>	Allow matches with log.													
status	Enable/disable this URL filter.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this URL filter.</td></tr><tr><td><i>disable</i></td><td>Disable this URL filter.</td></tr></table>				Option	Description	<i>enable</i>	Enable this URL filter.	<i>disable</i>	Disable this URL filter.				
Option	Description													
<i>enable</i>	Enable this URL filter.													
<i>disable</i>	Disable this URL filter.													

Parameter	Description	Type	Size	Default
exempt	If action is set to exempt, select the security profile operations that exempt URLs skip. Separate multiple options with a space.	option	-	av web-content activex-java-cookie dlp fortiguard range-block antiphish all
	Option	Description		
	av	AntiVirus scanning.		
	web-content	Web filter content matching.		
	activex-java-cookie	ActiveX, Java, and cookie filtering.		
	dlp	DLP scanning.		
	fortiguard	FortiGuard web filtering.		
	range-block	Range block feature.		
	pass	Pass single connection from all.		
	antiphish	AntiPhish credential checking.		
all	Exempt from all security profiles.			
web-proxy-profile	Web proxy profile.	string	Maximum length: 63	
referrer-host	Referrer host name.	string	Maximum length: 255	
dns-address-family	Resolve IPv4 address, IPv6 address, or both from DNS server.	option	-	ipv4
	Option	Description		
	ipv4	Resolve IPv4 address from DNS server.		
	ipv6	Resolve IPv6 address from DNS server.		
	both	Resolve both IPv4 and IPv6 addresses from DNS server.		



www.fortinet.com

Copyright© 2024 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.