

Hybrid Mesh Network Security

02 November 2026

CLI

R81.20

Reference Guide

CHECK POINT™

Check Point Copyright Notice

© 2022 - 2026 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page for a list of our trademarks.

Refer to the Third Party copyright notices for a list of relevant copyrights and third-party licenses.

Important Information



Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.



Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.



Check Point R81.20

For more about this release, see the R81.20 home page.



Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.



Feedback

Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Revision History

Date	Description
02 November 2026	Updated: ■ *"mds_backup" on page 756* ■ *"mds_restore" on page 759*
14 January 2026	Updated: ■ *"fwaccel stats" on page 1473* ■ *"Example Outputs on the "fwaccel stats" Commands" on page 1484*
9 December 2025	Updated *"migrate_server" on page 787*
25 June 2025	Updated: ■ *"Viewing Cluster Correction Statistics" on page 1367*
08 April 2025	Added: ■ *"CPLogInvestigator" on page 164* ■ *"evstart" on page 264* (for Security Management Server) ■ *"evstop" on page 265* (for Security Management Server) ■ *"evstart" on page 629* (for Multi-Domain Security Management Server) ■ *"evstop" on page 631* (for Multi-Domain Security Management Server) ■ *"hcp" on page 43* Updated: ■ *"migrate_server" on page 391* (for Security Management Server) ■ *"migrate_server" on page 787* (for Multi-Domain Security Management Server) ■ *"fw sdwan" on page 1222*
24 January 2025	Added: ■ *"Configuring Duration of Forced Failover in High Availability Mode" on page 1317*

Date	Description
17 October 2024	Added: ■ *"tp_collector_cli" on page 1281* Updated: ■ *"cpwd_admin list" on page 1055* ■ *"pdp broker" on page 1707* - Identity Cache Mode ■ *"pep control" on page 1746* - Identity Cache Mode
26 October 2023	Added: ■ *"taskset_us_all" on page 1674* ■ *"fw sdwan" on page 1222* Updated: ■ *"ClusterXL Configuration Commands" on page 1290* - added Gaia Clish commands in "Configure the minimal number of required subordinate interfaces for Bond Load Sharing" ■ *"Configuring the Minimal Number of Required Subordinate Interfaces for Bond Load Sharing" on page 1310* - added the Gaia Clish commands ■ *"ClusterXL Monitoring Commands" on page 1318* - removed the "`cphaprob latency`" command as not supported ■ *"Viewing Critical Devices" on page 1329* - description of "Local Probing" ■ *"fw ctl multik prioq" on page 1633* - corrected the parameter descriptions ■ *"fwaccel conns" on page 1408* - added the "`fwaccel conns -z`" command ■ *"cpstart" on page 1018* (for Security Gateway) ■ *"fw monitor" on page 1151* - added the parameter "`-b <Size of Buffer>`" ■ *"fw tab" on page 1228* - added "`fw tab -t connections -z`"

Date	Description
09 September 2023	Updated: ■ *"cp_conf ca" on page 70* - for Security Management Server ■ *"cpca_client get_crldp" on page 109* - for Security Management Server ■ *"fwm dbload" on page 333* - for Security Management Server ■ *"cp_conf ca" on page 445* - for Multi-Domain Server ■ *"cpca_client get_crldp" on page 484* - for Multi-Domain Server ■ *"fwm dbload" on page 700* - for Multi-Domain Server ■ *"fw ctl conn" on page 1086* Removed: ■ "*ips pmstats*" - this command is not supported
05 July 2023	Updated *"vpn tu tlist" on page 1826*
15 February 2023	Updated *"ips stats" on page 2002*
13 February 2023	Updated *"cp_log_export" on page 457*
20 November 2022	First release of this document

Table of Contents

Introduction ... *36*

Syntax Legend ... *37*

Gaia Commands ... *39*

Common Commands ... *40*

cpinfo ... *40*

cpview ... *41*

Overview of CPView ... *41*

CPView User Interface ... *41*

Using CPView ... *42*

hcp ... *43*

Security Management Server Commands ... *44*

Managing Security through API ... *45*

API ... *45*

API Tools ... *45*

Configuring the API Server ... *46*

Discarding API Sessions with Locks or Pending Changes ... *48*

contract_util ... *50*

contract_util check ... *52*

contract_util cpmacro ... *53*

contract_util download ... *54*

contract_util mgmt ... *56*

contract_util print ... *57*

contract_util summary ... *58*

contract_util update ... *59*

contract_util verify ... *60*

cp_conf ... *61*

cp_conf admin ... *65*

cp_conf auto ... 68
cp_conf ca ... 70
cp_conf client ... 72
cp_conf finger ... 76
cp_conf lic ... 78
cp_log_export ... 82
cpca_client ... 103
cpca_client create_cert ... 105
cpca_client double_sign ... 107
cpca_client get_crldp ... 109
cpca_client get_pubkey ... 111
cpca_client init_certs ... 112
cpca_client lscert ... 113
cpca_client revoke_cert ... 116
cpca_client revoke_non_exist_cert ... 119
cpca_client search ... 120
cpca_client set_ca_services ... 123
cpca_client set_cert_validity ... 125
cpca_client set_mgmt_tool ... 126
cpca_client set_sign_hash ... 131
cpca_create ... 133
cpconfig ... 134
cplic ... 137
cplic check ... 140
cplic contract ... 142
cplic db_add ... 144
cplic db_print ... 146
cplic db_rm ... 148
cplic del ... 149
cplic del <object name> ... 150

cplic get ... 151
cplic print ... 153
cplic put ... 155
cplic put <object name> ... 158
cplic upgrade ... 161
CPLogInvestigator ... 164
cppkg ... 171
cppkg add ... 173
cppkg delete ... 174
cppkg get ... 176
cppkg getroot ... 177
cppkg print ... 178
cppkg setroot ... 179
cpprod_util ... 180
cprid ... 186
cprinstall ... 187
cprinstall boot ... 190
cprinstall cprestart ... 191
cprinstall cpstart ... 192
cprinstall cpstop ... 193
cprinstall delete ... 194
cprinstall get ... 195
cprinstall install ... 196
cprinstall revert ... 199
cprinstall show ... 200
cprinstall snapshot ... 201
cprinstall transfer ... 202
cprinstall uninstall ... 204
cprinstall verify ... 206
cpstart ... 208

cpstat ... 209
cpstop ... 219
cpwd_admin ... 220
cpwd_admin config ... 224
cpwd_admin del ... 229
cpwd_admin detach ... 231
cpwd_admin exist ... 233
cpwd_admin flist ... 234
cpwd_admin getpid ... 236
cpwd_admin kill ... 237
cpwd_admin list ... 238
cpwd_admin monitor_list ... 243
cpwd_admin start ... 244
cpwd_admin start_monitor ... 247
cpwd_admin stop ... 248
cpwd_admin stop_monitor ... 250
dbedit ... 251
evstart ... 264
evstop ... 265
fw ... 266
fw fetchlogs ... 268
fw hastat ... 272
fw kill ... 273
fw log ... 274
fw logswitch ... 284
fw lslogs ... 288
fw mergefiles ... 291
fw repairlog ... 294
fw sam ... 295
fw sam_policy ... 303

fw sam_policy add ... 306
fw sam_policy batch ... 319
fw sam_policy del ... 321
fw sam_policy get ... 324
fwm ... 330
fwm dbload ... 333
fwm exportcert ... 334
fwm fetchfile ... 335
fwm fingerprint ... 337
fwm getpcap ... 339
fwm ikecrypt ... 341
fwm load ... 342
fwm logexport ... 343
fwm mds ... 348
fwm printcert ... 350
fwm sic_reset ... 356
fwm snmp_trap ... 357
fwm unload ... 360
fwm ver ... 364
fwm verify ... 365
inet_alert ... 366
ldapcmd ... 369
ldapcompare ... 371
ldapmemberconvert ... 375
ldapmodify ... 381
ldapsearch ... 383
mgmt_cli ... 386
migrate ... 387
migrate_server ... 391
queryDB_util ... 402

rs_db_tool ... 403
sam_alert ... 405
stattest ... 409
threshold_config ... 412
Multi-Domain Security Management Commands ... **418**
Managing Security through API ... 419
API ... 419
API Tools ... 419
Configuring the API Server ... 420
Discarding API Sessions with Locks or Pending Changes ... 422
cma_migrate ... 424
contract_util ... 425
contract_util check ... 427
contract_util cpmacro ... 428
contract_util download ... 429
contract_util mgmt ... 431
contract_util print ... 432
contract_util summary ... 433
contract_util update ... 434
contract_util verify ... 435
cp_conf ... 436
cp_conf admin ... 440
cp_conf auto ... 443
cp_conf ca ... 445
cp_conf client ... 447
cp_conf finger ... 451
cp_conf lic ... 453
cp_log_export ... 457
cpca_client ... 478
cpca_client create_cert ... 480

cpca_client double_sign 482
cpca_client get_crldp 484
cpca_client get_pubkey 486
cpca_client init_certs 487
cpca_client lscert 488
cpca_client revoke_cert 491
cpca_client revoke_non_exist_cert 494
cpca_client search 495
cpca_client set_ca_services 498
cpca_client set_cert_validity 500
cpca_client set_mgmt_tool 501
cpca_client set_sign_hash 506
cpca_create 508
cplic 509
cplic check 512
cplic contract 514
cplic db_add 516
cplic db_print 518
cplic db_rm 520
cplic del 521
cplic del <object name> 522
cplic get 523
cplic print 525
cplic put 527
cplic put <object name> 530
cplic upgrade 533
cpmiquerybin 536
cppkg 538
cppkg add 540
ppkg delete 541

cppkg get ... 543
cppkg getroot ... 544
cppkg print ... 545
cppkg setroot ... 546
cpprod_util ... 547
cprid ... 553
cprinstall ... 554
cprinstall boot ... 557
cprinstall cprestart ... 558
cprinstall cpstart ... 559
cprinstall cpstop ... 560
cprinstall delete ... 561
cprinstall get ... 562
cprinstall install ... 563
cprinstall revert ... 566
cprinstall show ... 567
cprinstall snapshot ... 568
cprinstall transfer ... 569
cprinstall uninstall ... 571
cprinstall verify ... 573
cpstat ... 575
cpwd_admin ... 585
cpwd_admin config ... 589
cpwd_admin del ... 594
cpwd_admin detach ... 596
cpwd_admin exist ... 598
cpwd_admin flist ... 599
cpwd_admin getpid ... 601
cpwd_admin kill ... 602
cpwd_admin list ... 603

cpwd_admin monitor_list ... 608
cpwd_admin start ... 609
cpwd_admin start_monitor ... 612
cpwd_admin stop ... 613
cpwd_admin stop_monitor ... 615
dbedit ... 616
evstart ... 629
evstop ... 631
fw ... 633
fw fetchlogs ... 635
fw hastat ... 639
fw kill ... 640
fw log ... 641
fw logswitch ... 651
fw lslogs ... 655
fw mergefiles ... 658
fw repairlog ... 661
fw sam ... 662
fw sam_policy ... 670
fw sam_policy add ... 673
fw sam_policy batch ... 686
fw sam_policy del ... 688
fw sam_policy get ... 691
fwm ... 697
fwm dbload ... 700
fwm exportcert ... 701
fwm fetchfile ... 702
fwm fingerprint ... 704
fwm getpcap ... 706
fwm ikecrypt ... 708

fwm load ... 709
fwm logexport ... 710
fwm mds ... 715
fwm printcert ... 717
fwm sic_reset ... 723
fwm snmp_trap ... 724
fwm unload ... 727
fwm ver ... 731
fwm verify ... 732
inet_alert ... 733
ldapcmd ... 736
ldapcompare ... 738
ldapmemberconvert ... 742
ldapmodify ... 748
ldapsearch ... 750
mcd ... 753
mds_backup ... 756
mds_restore ... 759
mdscmd ... 760
mdsconfig ... 762
mdsenv ... 766
mdsquerydb ... 768
mdsstart ... 770
mdsstart_customer ... 774
mdsstat ... 775
mdsstop ... 777
mdsstop_customer ... 781
mgmt_cli ... 782
migrate ... 783
migrate_server ... 787

migrate_global_policies ... 798
queryDB_util ... 799
rs_db_tool ... 800
sam_alert ... 802
stattest ... 806
threshold_config ... 809
$MDSVERUTIL ... 815
$MDSVERUTIL AllCMAs ... 826
$MDSVERUTIL AllVersions ... 827
$MDSVERUTIL CMAAddonDir ... 830
$MDSVERUTIL CMACompDir ... 831
$MDSVERUTIL CMAFgDir ... 832
$MDSVERUTIL CMAFw40Dir ... 833
$MDSVERUTIL CMAFw41Dir ... 834
$MDSVERUTIL CMAFwConfDir ... 835
$MDSVERUTIL CMAFwDir ... 836
$MDSVERUTIL CMAIp ... 837
$MDSVERUTIL CMAIp6 ... 838
$MDSVERUTIL CMALogExporterDir ... 839
$MDSVERUTIL CMALogIndexerDir ... 840
$MDSVERUTIL CMANameByFwDir ... 841
$MDSVERUTIL CMANameByIp ... 842
$MDSVERUTIL CMARegistryDir ... 843
$MDSVERUTIL CMAReporterDir ... 844
$MDSVERUTIL CMASmartLogDir ... 845
$MDSVERUTIL CMASvnConfDir ... 846
$MDSVERUTIL CMASvnDir ... 847
$MDSVERUTIL ConfDirVersion ... 848
$MDSVERUTIL CpdbUpParam ... 849
$MDSVERUTIL CPprofileDir ... 850

$MDSVERUTIL CPVer ... 851
$MDSVERUTIL CustomersBaseDir ... 852
$MDSVERUTIL DiskSpaceFactor ... 853
$MDSVERUTIL InstallationLogDir ... 854
$MDSVERUTIL IsIPv6Enabled ... 855
$MDSVERUTIL IsLegalVersion ... 856
$MDSVERUTIL IsOsSupportsIPv6 ... 857
$MDSVERUTIL LatestVersion ... 858
$MDSVERUTIL MDSAddonDir ... 859
$MDSVERUTIL MDSCompDir ... 860
$MDSVERUTIL MDSDir ... 861
$MDSVERUTIL MDSFgDir ... 862
$MDSVERUTIL MDSFwbcDir ... 863
$MDSVERUTIL MDSFwDir ... 864
$MDSVERUTIL MDSIp ... 865
$MDSVERUTIL MDSIp6 ... 866
$MDSVERUTIL MDSLogExporterDir ... 867
$MDSVERUTIL MDSLogIndexerDir ... 868
$MDSVERUTIL MDSPkgName ... 869
$MDSVERUTIL MDSRegistryDir ... 870
$MDSVERUTIL MDSReporterDir ... 871
$MDSVERUTIL MDSSmartLogDir ... 872
$MDSVERUTIL MDSSvnDir ... 873
$MDSVERUTIL MDSVarCompDir ... 874
$MDSVERUTIL MDSVarDir ... 875
$MDSVERUTIL MDSVarFwbcDir ... 876
$MDSVERUTIL MDSVarFwDir ... 877
$MDSVERUTIL MDSVarSvnDir ... 878
$MDSVERUTIL MSP ... 879
$MDSVERUTIL OfficialName ... 880

$MDSVERUTIL OptionPack ... 881
$MDSVERUTIL ProductName ... 882
$MDSVERUTIL RegistryCurrentVer ... 883
$MDSVERUTIL ShortOfficialName ... 884
$MDSVERUTIL SmartCenterPuvUpgradeParam ... 885
$MDSVERUTIL SP ... 886
$MDSVERUTIL SVNPkgName ... 887
$MDSVERUTIL SvrDirectory ... 888
$MDSVERUTIL SvrParam ... 889
Creating a Domain Management Server with the 'mgmt_cli' Command ... 890
SmartProvisioning Commands ... 891
Managing Security through API ... 892
API ... 892
API Tools ... 892
Configuring the API Server ... 893
Discarding API Sessions with Locks or Pending Changes ... 895
Check Point LSMcli Overview ... 897
SmartLSM Security Gateway Management Actions ... 899
LSMcli AddROBO VPN1 ... 900
LSMcli ModifyROBO VPN1 ... 902
LSMcli ModifyROBOManualVPNDomain ... 904
LSMcli ModifyROBOTopology VPN1 ... 906
LSMcli ModifyROBOInterface VPN1 ... 907
LSMcli AddROBOInterface VPN1 ... 908
LSMcli DeleteROBOInterface VPN1 ... 909
LSMcli ExportIke ... 910
LSMcli ResetIke ... 911
LSMcli Remove ... 912
LSMcli ResetSic ... 913
LSMcli Show ... 915

LSMcli ShowROBOTopology ... 917
LSMcli UpdateCO ... 918
SmartUpdate Actions ... 919
LSMcli Install ... 920
LSMcli Uninstall ... 922
LSMcli Distribute ... 923
LSMcli VerifyInstall ... 924
LSMcli VerifyUpgrade ... 925
LSMcli Upgrade ... 926
LSMcli GetInfo ... 927
LSMcli ShowInfo ... 928
LSMcli ShowRepository ... 929
LSMcli Stop ... 930
LSMcli Start ... 931
LSMcli Restart ... 932
LSMcli Reboot ... 933
LSMcli Push Actions ... 934
LSMcli PushPolicy ... 935
LSMcli PushDOs ... 936
LSMcli GetStatus ... 937
Managing SmartLSM Clusters with LSMcli ... 938
LSMcli AddROBO VPN1Cluster ... 939
LSMcli ModifyROBO VPN1Cluster ... 941
LSMcli ModifyROBOTopology VPN1Cluster ... 942
LSMcli ModifyROBONetaccess VPN1Cluster ... 943
LSMcli AddClusterSubnetOverride VPN1Cluster ... 945
LSMcli ModifyClusterSubnetOverride VPN1Cluster ... 947
LSMcli DeleteClusterSubnetOverride VPN1Cluster ... 949
LSMcli AddPrivateSubnetOverride VPN1ClusterMember ... 951
LSMcli ModifyPrivateSubnetOverride VPN1ClusterMember ... 953

LSMcli DeletePrivateSubnetOverride VPN1ClusterMember ... 955
LSMcli RemoveCluster ... 957
Using LSMcli Commands for Small Office Appliances ... 958
LSMcli AddROBO <Appliance_Model> ... 959
LSMcli AddROBO <Appliance_Model>Cluster ... 961
Other LSMcli Commands for Small Office Appliances ... 963
Security Gateway Commands ... 964
comp_init_policy ... 965
connection_pipelining ... 969
control_bootsec ... 973
cp_conf ... 977
cp_conf auto ... 981
cp_conf corexl ... 983
cp_conf fullha ... 986
cp_conf ha ... 987
cp_conf intfs ... 989
cp_conf lic ... 990
cp_conf sic ... 994
cpconfig ... 996
cplic ... 1000
cplic check ... 1002
cplic contract ... 1004
cplic del ... 1006
cplic print ... 1007
cplic put ... 1009
cpprod_util ... 1012
cpstart ... 1018
cpstat ... 1019
cpstop ... 1029
dynamic_objects ... 1030

cpwd_admin 1034
cpwd_admin config 1038
cpwd_admin del 1046
cpwd_admin detach 1048
cpwd_admin exist 1050
cpwd_admin flist 1051
cpwd_admin getpid 1053
cpwd_admin kill 1054
cpwd_admin list 1055
cpwd_admin monitor_list 1060
cpwd_admin start 1061
cpwd_admin start_monitor 1064
cpwd_admin stop 1065
cpwd_admin stop_monitor 1067
fw 1068
fw -i 1073
fw amw 1074
fw ctl 1077
fw ctl arp 1080
fw ctl bench 1081
fw ctl block 1083
fw ctl chain 1084
fw ctl conn 1086
fw ctl conntab 1088
fw ctl cpasstat 1097
'fw ctl debug' and 'fw ctl kdebug' 1098
fw ctl dlpkstat 1099
fw ctl get 1100
fw ctl iflist 1102
fw ctl install 1103

fw ctl leak ... 1104
fw ctl pstat ... 1107
fw ctl set ... 1110
fw ctl tcpstrstat ... 1114
fw ctl uninstall ... 1116
fw defaultgen ... 1117
fw fetch ... 1119
fw fetchlogs ... 1122
fw getifs ... 1126
fw hastat ... 1127
fw isp_link ... 1128
fw kill ... 1129
fw lichosts ... 1130
fw log ... 1131
fw logswitch ... 1141
fw lslogs ... 1145
fw mergefiles ... 1148
fw monitor ... 1151
fw repairlog ... 1186
fw sam ... 1187
fw sam_policy ... 1195
fw sam_policy add ... 1198
fw sam_policy batch ... 1211
fw sam_policy del ... 1213
fw sam_policy get ... 1216
fw sdwan ... 1222
fw showuptables ... 1224
fw stat ... 1225
fw tab ... 1228
fw unloadlocal ... 1242

fw up_execute ... 1246
fw ver ... 1249
fwboot ... 1251
fwboot bootconf ... 1253
fwboot corexl ... 1257
fwboot cpuid ... 1264
fwboot default ... 1266
fwboot fwboot_ipv6 ... 1267
fwboot fwdefault ... 1268
fwboot ha_conf ... 1269
fwboot ht ... 1270
fwboot multik_reg ... 1271
fwboot post_drv ... 1273
sam_alert ... 1274
stattest ... 1278
tp_collector_cli ... 1281
usrchk ... 1285
ClusterXL Commands ... ***1289***
ClusterXL Configuration Commands ... 1290
Configuring the Cluster Member ID Mode in Local Logs ... 1294
Registering a Critical Device ... 1295
Unregistering a Critical Device ... 1299
Reporting the State of a Critical Device ... 1300
Registering Critical Devices Listed in a File ... 1302
Unregistering All Critical Devices ... 1304
Configuring the Cluster Control Protocol (CCP) Settings ... 1305
Initiating Manual Cluster Failover ... 1306
Configuring the Minimal Number of Required Subordinate Interfaces for Bond Load Sharing ... 1310
Configuring Link Monitoring on the Cluster Interfaces ... 1313

Configuring the Multi-Version Cluster Mechanism ... 1316
Configuring Duration of Forced Failover in High Availability Mode ... 1317
ClusterXL Monitoring Commands ... 1318
Viewing Cluster State ... 1323
Viewing Critical Devices ... 1329
Viewing Cluster Interfaces ... 1341
Viewing Bond Interfaces ... 1346
Viewing Cluster Failover Statistics ... 1351
Viewing Software Versions on Cluster Members ... 1353
Viewing Delta Synchronization ... 1354
Viewing IGMP Status ... 1361
Viewing Cluster Delta Sync Statistics for Connections Table ... 1362
Viewing Cluster IP Addresses ... 1363
Viewing the Cluster Member ID Mode in Local Logs ... 1364
Viewing Interfaces Monitored by RouteD ... 1365
Viewing Roles of RouteD Daemon on Cluster Members ... 1366
Viewing Cluster Correction Statistics ... 1367
Viewing the Cluster Control Protocol (CCP) Settings ... 1371
Viewing the State of the Multi-Version Cluster Mechanism ... 1372
Viewing Full Connectivity Upgrade Statistics ... 1373
cpconfig ... 1374
cphastart ... 1378
cphastop ... 1379
cp_conf fullha ... 1380
cp_conf ha ... 1381
fw hastat ... 1383
fwboot ha_conf ... 1385
The clusterXL_admin Script ... 1386
The clusterXL_monitor_ips Script ... 1390
The clusterXL_monitor_process Script ... 1394

SecureXL Commands *1398*
'fwaccel' and 'fwaccel6' *1399*
fwaccel cfg *1404*
fwaccel conns *1408*
fwaccel dbg *1412*
fwaccel dos *1426*
fwaccel dos whitelist *1428*
fwaccel dos config *1432*
fwaccel dos deny *1438*
fwaccel dos pbox *1441*
fwaccel dos rate *1446*
fwaccel dos stats *1448*
fwaccel feature *1450*
fwaccel ip_mr_cache *1453*
fwaccel off *1454*
fwaccel on *1459*
fwaccel ranges *1464*
fwaccel stat *1471*
fwaccel stats *1473*
Description of the Statistics Counters in the "fwaccel stats" Output *1475*
Example Outputs on the "fwaccel stats" Commands *1484*
fwaccel synatk *1492*
fwaccel synatk -a *1495*
fwaccel synatk -c <Configuration File> *1496*
fwaccel synatk -d *1497*
fwaccel synatk -e *1498*
fwaccel synatk -g *1499*
fwaccel synatk -m *1500*
fwaccel synatk -t <Threshold> *1501*
fwaccel synatk allow *1503*

fwaccel synatk config ... 1508
fwaccel synatk monitor ... 1511
fwaccel synatk state ... 1516
fwaccel tab ... 1518
fwaccel templates ... 1521
fwaccel ver ... 1526
fw sam_policy ... 1527
fw sam_policy add ... 1530
fw sam_policy batch ... 1543
fw sam_policy del ... 1545
fw sam_policy get ... 1548
The /proc/ppk/ and /proc/ppk6/ entries ... 1554
/proc/ppk/affinity ... 1556
/proc/ppk/conf ... 1557
/proc/ppk/conns ... 1558
/proc/ppk/cpls ... 1559
/proc/ppk/cqstats ... 1560
/proc/ppk/drop_statistics ... 1561
/proc/ppk/ifs ... 1562
/proc/ppk/mcast_statistics ... 1567
/proc/ppk/nac ... 1568
/proc/ppk/notify_statistics ... 1569
/proc/ppk/profile_cpu_stat ... 1571
/proc/ppk/rlc ... 1572
/proc/ppk/statistics ... 1573
/proc/ppk/stats ... 1575
/proc/ppk/viol_statistics ... 1576
SecureXL Debug ... 1577
fwaccel dbg ... 1578
SecureXL Debug Procedure ... 1592

SecureXL Debug Modules and Debug Flags ... 1598
CoreXL Commands ... **1609**
cp_conf corexl ... 1610
dynamic_balancing ... 1613
fw ctl multik ... 1617
fw ctl multik add_bypass_port ... 1619
fw ctl multik del_bypass_port ... 1621
fw ctl multik dynamic_dispatching ... 1623
fw ctl multik gconn ... 1624
fw ctl multik get_instance ... 1629
fw ctl multik print_heavy_conn ... 1631
fw ctl multik prioq ... 1633
fw ctl multik show_bypass_ports ... 1634
fw ctl multik stat ... 1635
fw ctl multik start ... 1637
fw ctl multik stop ... 1638
fw ctl multik utilize ... 1639
fw ctl affinity ... 1640
Running the 'fw ctl affinity -l' command in Gateway Mode ... 1641
Running the 'fw ctl affinity -l' command in VSX Mode ... 1646
Running the 'fw ctl affinity -s' command in Gateway Mode ... 1649
Running the 'fw ctl affinity -s' command in VSX Mode ... 1652
fw -i ... 1656
fwboot bootconf ... 1657
fwboot corexl ... 1661
fwboot cpuid ... 1668
fwboot ht ... 1670
fwboot multik_reg ... 1671
fwboot post_drv ... 1673
taskset_us_all ... 1674

Multi-Queue Commands ... *1679*
mq_mng ... *1680*
Multi-Queue Configuration in the Expert mode ... *1680*
Multi-Queue Configuration in Gaia Clish / Gaia gClish ... *1686*
Identity Awareness Commands ... *1689*
adlog ... *1690*
adlog control ... *1692*
adlog dc ... *1694*
adlog debug ... *1695*
adlog query ... *1696*
adlog statistics ... *1697*
pdp ... *1698*
pdp ad ... *1701*
General Syntax ... *1701*
The 'pdp ad associate' command ... *1701*
The 'pdp ad disassociate' command ... *1702*
pdp auth ... *1703*
pdp broker ... *1707*
pdp conciliation ... *1712*
pdp connections ... *1714*
pdp control ... *1715*
pdp debug ... *1716*
pdp idc ... *1719*
pdp idp ... *1723*
pdp monitor ... *1724*
pdp muh ... *1726*
pdp nested_groups ... *1727*
pdp network ... *1731*
pdp radius ... *1732*
pdp roles ... *1735*

General Syntax ... 1735
The 'pdp roles extract' command ... 1735
The 'pdp roles fetch' command ... 1735
pdp status ... 1738
pdp tasks_manager ... 1739
pdp timers ... 1740
pdp topology_map ... 1741
pdp tracker ... 1742
pdp update ... 1743
pdp vpn ... 1744
pep ... 1745
pep control ... 1746
pep debug ... 1748
pep show ... 1750
pep tracker ... 1753
test_ad_connectivity ... 1754
VPN Commands ... **1758**
ike debug ... 1759
vpn ... 1771
vpn check_ttm ... 1774
vpn compreset ... 1775
vpn compstat ... 1776
vpn crl_zap ... 1777
vpn crlview ... 1778
vpn debug ... 1780
vpn dll ... 1792
vpn drv ... 1793
vpn dump_psk ... 1794
vpn ipafile_check ... 1795
vpn ipafile_users_capacity ... 1796

vpn macutil ... 1797
vpn mep_refresh ... 1798
vpn neo_proto ... 1799
vpn nssm_toplogy ... 1800
vpn overlap_encdom ... 1801
vpn rim_cleanup ... 1803
vpn rll ... 1804
vpn set_slim_server ... 1805
vpn set_snx_encdom_groups ... 1806
vpn set_trac ... 1807
vpn shell ... 1808
vpn show_tcpt ... 1815
vpn tu ... 1816
vpn tu conn ... 1818
vpn tu del ... 1820
vpn tu list ... 1823
vpn tu mstats ... 1825
vpn tu tlist ... 1826
vpn ver ... 1837
mcc ... 1838
mcc add ... 1840
mcc add2main ... 1841
mcc del ... 1842
mcc lca ... 1843
mcc main2add ... 1844
mcc show ... 1845
Mobile Access Commands ... **1847**
admin_wizard ... 1848
cvpnd_admin ... 1852
cvpnd_settings ... 1855

cvpn_ver 1858
cvpnrestart 1859
cvpnstart 1860
cvpnstop 1861
deleteUserSettings 1862
fwpush 1863
ics_updates_script 1867
listusers 1868
rehash_ca_bundle 1869
UserSettingsUtil 1870
Data Loss Prevention Commands 1872
dlpcmd 1873
VSX Commands 1876
cpconfig 1877
vsenv 1881
vsx 1882
vsx fetch 1886
vsx fetch_all_cluster_policies 1888
vsx fetchvs 1889
vsx get 1890
vsx mstat 1891
vsx showncs 1895
vsx sicreset 1896
vsx stat 1897
vsx unloadall 1900
vsx vspurge 1901
vsx_util 1902
vsx_util add_member 1907
vsx_util change_interfaces 1909
vsx_util change_mgmt_ip 1913

vsx_util change_mgmt_subnet ... 1914
vsx_util change_private_net ... 1916
vsx_util convert_cluster ... 1918
vsx_util downgrade ... 1920
vsx_util reconfigure ... 1921
vsx_util remove_member ... 1927
vsx_util show_interfaces ... 1928
vsx_util upgrade ... 1932
vsx_util view_vs_conf ... 1933
vsx_util vsls ... 1937
vsx_provisioning_tool ... 1939
Transactions ... 1942
vsx_provisioning_tool Commands ... 1943
Explicit Transaction Commands ... 1944
Adding a VSX Gateway ... 1945
Adding a VSX Cluster ... 1948
Adding a Virtual Device ... 1951
Deleting a Virtual Device ... 1954
Modifying Settings of a Virtual Device ... 1955
Adding an Interface to a Virtual Device ... 1958
Adding a Bridge Interface to a Virtual System ... 1962
Adding a VPN Tunnel Interface to a Virtual Device ... 1964
Removing an Interface from a Virtual Device ... 1966
Modifying Settings of an Interface ... 1968
Configuring a Physical Interface as VLAN Trunk ... 1972
Adding a Route ... 1973
Removing a Route ... 1975
Showing Virtual Device Data ... 1977
Script Examples ... 1978
Example 1 ... 1978

Example 2 ... 1979
Example 3 ... 1980
QoS Commands ... **1981**
etmstart ... 1982
etmstop ... 1983
fgate ... 1984
IPS Commands ... **1992**
ips ... 1993
ips bypass ... 1995
ips debug ... 1997
ips off ... 1998
ips on ... 1999
ips refreshcap ... 2000
ips stat ... 2001
ips stats ... 2002
Monitoring Commands ... **2004**
rtm ... 2005
rtm debug ... 2006
rtm drv ... 2007
rtm rtmd ... 2008
rtm monitor ... 2009
rtm stat ... 2015
rtm ver ... 2018
rtmstart ... 2019
rtmstop ... 2020
Working with Kernel Parameters ... **2021**
Running Check Point Commands in Shell Scripts ... **2022**
On a Security Management Server / Log Server / SmartEvent Server ... 2022
On a Multi-Domain Server / Multi-Domain Log Server ... 2023
On a Security Gateway / Cluster Members (non-VSX) ... 2023

On a VSX Gateway / VSX Cluster Members *2024*

Glossary ***2025***

Introduction

The CLI Reference Guide provides CLI commands to configure and monitor Check Point Software Blades.

Syntax Legend

Whenever possible, this guide lists commands, parameters and options in the alphabetical order.

This guide uses this convention in the Command Line Interface (CLI) syntax:

Character	Description

TAB	Shows the available nested subcommands:
	`main command`
	`→ nested subcommand 1`
	`→ → nested subsubcommand 1-1`
	`→ → nested subsubcommand 1-2`
	`→ nested subcommand 2`
	Example:
	`cpwd_admin`
	`config`
	`-a <options>`
	`-d <options>`
	`-p`
	`-r`
	`del <options>`
	Meaning, you can run only **one** of these commands:
	■ This command: `cpwd_admin config -a <options>`
	■ Or this command: `cpwd_admin config -d <options>`
	■ Or this command: `cpwd_admin config -p`
	■ Or this command: `cpwd_admin config -r`
	■ Or this command: `cpwd_admin del <options>`

Curly brackets or braces **{ }**	Enclose a list of available commands or parameters, separated by the vertical bar **|**. User can enter only one of the available commands or parameters.

Character	Description
Angle brackets **< >**	Enclose a variable. User must explicitly specify a supported value.
Square brackets or brackets **[ ]**	Enclose an optional command or parameter, which user can also enter.

Gaia Commands

See:

- *R81.20 Gaia Administration Guide*
- *R81.20 Gaia Advanced Routing Administration Guide*

Common Commands

cpinfo

Description

A utility that collects diagnostics data on your Check Point computer at the time of execution.

It is mandatory to collect these data when you contact *Check Point Support* about an issue on your Check Point server.

For more information, see sk92739.

cpview

Overview of CPView

Description

CPView is a text based built-in utility on a Check Point computer.

CPView Utility shows statistical data that contain both general system information (CPU, Memory, Disk space) and information for different Software Blades (only on a Security Gateway / ClusterXL / Scalable Platform Security Group).

The CPView continuously updates the data in easy to access views.

On a Security Gateway / ClusterXL / Scalable Platform Security Group, you can use this statistical data to monitor the performance.

For more information, see sk101878.

Syntax

```
cpview --help
```

CPView User Interface

The CPView user interface has three sections:

Section	Description
Header	This view shows the time the statistics in the third view are collected. It updates when you refresh the statistics.
Navigation	This menu bar is interactive. Move between menus with the arrow keys and mouse. A menu can have sub-menus and they show under the menu bar.
View	This view shows the statistics collected in that view. These statistics update at the refresh rate.

Using CPView

Use these keys to navigate the CPView:

Key	Description
Arrow keys	Moves between menus and views. Scrolls in a view.
Home	Returns to the **Overview** view.
Enter	Changes to the **View Mode**. On a menu with sub-menus, the **Enter** key moves you to the lowest level sub-menu.
Esc	Returns to the **Menu Mode**.
Q	Quits CPView.

Use these keys to change CPView interface options:

Key	Description
R	Opens a window where you can change the refresh rate. The default refresh rate is 2 seconds.
W	Changes between wide and normal display modes. In wide mode, CPView fits the screen horizontally.
S	Manually sets the number of rows or columns.
M	Switches on/off the mouse.
P	Pauses and resumes the collection of statistics.

Use these keys to save statistics, show help, and refresh statistics:

Key	Description
C	Saves the current page to a file. The file name format is: `cpview_<ID of the cpview process>.cap<Number of the capture>`
H	Shows a tooltip with CPView options.
Space bar	Immediately refreshes the statistics.

hcp

Description

HealthCheck Point (HCP) is a self-updatable suite of tools for:

- **Tests:** Assesses the health of your system.
- **WTS (What's The Story):** Provides a timeline of critical and informative events occurred on the system.
- **Topology:** Visualize the Firewall topology.

For more information, see sk171436.

Security Management Server Commands

For more information about Security Management Server, see the *R81.20 Security Management Administration Guide*.

Managing Security through API

This section describes the API Server on a Management Server and the applicable API Tools.

API

You can configure and manage the Management Server through API Requests that you send to the API Server that runs on the Management Server.

The API Server can automate daily tasks and integrate Check Point solutions with third party systems, such as virtualization, ticketing, and change management systems.

To learn more about the management APIs, to see code samples, and to take advantage of user forums, see:

- The API Documentation:
  - Online - *Check Point Management API Reference* (at the top, select the correct version)
  - Local - `https://<Server IP Address>/api_docs/#introduction`

    By default, access to the local API Documentation is disabled. Follow the instructions in sk174606.

    Note - On a Standalone server (a server which runs both a Security Management Server and a Security Gateway), the API Documentation web portal (`https://<Server IP Address>/api_docs`) stops working when you open SmartView Web Application (`https://<Server IP Address>/smartview`).
- The **Developers Network** section of *Check Point CheckMates Community*.

API Tools

You can use these tools to work with the API Server on the Management Server:

- Standalone management tool, included with Gaia operating system:

  `mgmt_cli`
- Standalone management tool, included with SmartConsole:

  `mgmt_cli.exe`

  You can copy this tool from the SmartConsole installation folder to other computers that run Windows operating system.
- Web Services APIs that allow communication and data exchange between the clients and the Management Server over the HTTP protocol.

These APIs also let other Check Point processes communicate with the Management Server over the HTTPS protocol.

`https://<IP Address of Management Server>/web_api/<command>`

Configuring the API Server

To configure the API Server:

1. Connect with SmartConsole to the Security Management Server or applicable Domain Management Server.
2. From the left navigation panel, click **Manage & Settings**.
3. In the upper left section, click **Blades**.
4. In the **Management API** section, click **Advanced Settings**.

   The **Management API Settings** window opens.
5. Configure the **Startup Settings** and the **Access Settings**.

   Configuring Startup Settings

   Select **Automatic start** to automatically start the API server when you start or reboot the Management Server.

   Notes:
   - If the Management Server has more than 4GB of RAM installed, the **Automatic start** option is activated by default during Management Server installation.
   - If the Management Server has less than 4GB of RAM, the **Automatic Start** option is deactivated.

Configuring Access Settings

Select one of these options to configure which clients can connect to the API Server:

- **Management server only** - Only the Management Server itself can connect to the API Server. This option only lets you use the `mgmt_cli` utility on the Management Server to send API requests. You cannot use SmartConsole or Web services to send API requests.
- **All IP addresses that can be used for GUI clients** - You can send API requests from all IP addresses that are defined as **Trusted Clients** in SmartConsole. This includes requests from SmartConsole, Web services, and the `mgmt_cli` utility on the Management Server.
- **All IP addresses** - You can send API requests from all IP addresses. This includes requests from SmartConsole, Web services, and the `mgmt_cli` utility on the Management Server.

6. Click **OK**.
7. In the upper left section, click **Permissions & Administrators**.
8. In the object of each applicable Administrator, make sure the assigned Permission Profile allows access to Management API.

   Instructions

   a. Edit the Administrator object.
   b. In the left panel, click **General**.
   c. In the **Permissions** section, on the right side of the selected Permission Profile, click the eye icon.

      The Permission Profile object opens in the read-only view.
   d. In the left panel, click **Management**.
   e. The permission **Management API Login** has to be selected.

      If it is not selected, then close this window and edit this Permission Profile object.
   f. Click **Close**.

9. Publish the SmartConsole session.
10. Restart the API Server on the Management Server with this command:

```
api restart
```

Notes:

- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

- The output of this command must show:

```
API started successfully
```

11. Examine the status of the API server on the Management Server with this command:

```
api status
```

Notes:

- The output of this command must show:

```
------------------------------------------
Overall API Status: Started
------------------------------------------

API readiness test SUCCESSFUL. The server is up and ready
to receive connections
```

- The output of this command may show the state of the "**API**" process as "**Stopped**" when the API access is set to "**All IP addresses that can be used for GUI clients**", and more than 200 Trusted Clients are configured:

```
Processes:

Name      State     PID       More Information
------------------------------------------------
API       Stopped   ...
```

Discarding API Sessions with Locks or Pending Changes

Open SmartConsole and API sessions that contain locks or unpublished changes are not automatically discarded. As a result, some sessions can remain open for extended periods.

The `ENABLE_DISCARD_WORKSESSIONS_OLDER_THAN_DAYS` environment variable controls whether stale open sessions are automatically discarded. By default, this variable is disabled, and open sessions with locks or unpublished changes remain available until they are manually discarded.

When enabled, the Security Management Server periodically evaluates open sessions and discards sessions that exceed the configured age threshold.

To configure automatic discard of stale sessions:

1. Connect to the Security Management Server or Multi-Domain Server using SSH.
2. Switch to Expert mode.
3. To enable automatic discard of open sessions that contain locks or unpublished changes, set `ENABLE_DISCARD_WORKSESSIONS_OLDER_THAN_DAYS` to "`true`".

   Run:

   ```
   MDS_FWDIR/scripts/reload_env_vars.sh -e "ENABLE_DISCARD_
   WORKSESSIONS_OLDER_THAN_DAYS=true"
   ```

   ```
   $MDS_FWDIR/scripts/override_server_setting.sh -e ENABLE_DISCARD_
   WORKSESSIONS_OLDER_THAN_DAYS true
   ```

4. By default, only sessions which are open for more than 60 days are automatically discarded. To configure the number of days after which sessions are discarded, run:

   ```
   $MDS_FWDIR/scripts/reload_env_vars.sh -e "DISCARD_WORKSESSIONS_
   OLDER_THAN_DAYS=<Number_of_Days>" $MDS_FWDIR/scripts/override_
   server_setting.sh -e DISCARD_WORKSESSIONS_OLDER_THAN_DAYS
   <Number_of_Days>
   ```

   For example, to set the threshold to 30 days, run:

   ```
   $MDS_FWDIR/scripts/reload_env_vars.sh -e "DISCARD_WORKSESSIONS_
   OLDER_THAN_DAYS=30"
   $MDS_FWDIR/scripts/override_server_setting.sh -e DISCARD_
   WORKSESSIONS_OLDER_THAN_DAYS 30
   ```

Result:

When `ENABLE_DISCARD_WORKSESSIONS_OLDER_THAN_DAYS` is set to "`true`":

- The Security Management Server checks all open SmartConsole and API sessions one time per day.
- If a session remains open longer than the number of days configured in `DISCARD_WORKSESSIONS_OLDER_THAN_DAYS`, the session is automatically discarded.

contract_util

Description

Works with the Check Point Service Contracts.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util [-d]
    check <options>
    cpmacro <options>
    download <options>
    mgmt
    print <options>
    summary <options>
    update <options>
    verify
```

Parameters

Parameter	Description
`check <options>`	Checks whether the Security Gateway is eligible for an upgrade. See *"contract_util check" on page 52*.
`cpmacro <options>`	Overwrites the current `cp.macro` file with the specified `cp.macro` file. See *"contract_util cpmacro" on page 53*.
`download <options>`	Downloads all associated Check Point Service Contracts from the User Center, or from a local file. See *"contract_util download" on page 54*.
`mgmt`	Delivers the Service Contract information from the Management Server to the managed Security Gateways. See *"contract_util mgmt" on page 56*.
`print <options>`	Shows all the installed licenses and whether the Service Contract covers these license, which entitles them for upgrade or not. See *"contract_util print" on page 57*.

Parameter	Description
`summary <options>`	Shows post-installation summary. See *"contract_util summary" on page 58*.
`update <options>`	Updates Check Point Service Contracts from your User Center account. See *"contract_util update" on page 59*.
`verify`	Checks whether the Security Gateway is eligible for an upgrade. This command also interprets the return values and shows a meaningful message. See *"contract_util verify" on page 60*.

contract_util check

Description

Checks whether the Security Gateway is eligible for an upgrade.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util check
    {-h | -help}
    hfa
    maj_upgrade
    min_upgrade
    upgrade
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`hfa`	Checks whether the Security Gateway is eligible for an upgrade to a higher Hotfix Accumulator.
`maj_upgrade`	Checks whether the Security Gateway is eligible for an upgrade to a higher Major version.
`min_upgrade`	Checks whether the Security Gateway is eligible for an upgrade to a higher Minor version.
`upgrade`	Checks whether the Security Gateway is eligible for an upgrade.

contract_util cpmacro

Description

Overwrites the current `cp.macro` file with the specified `cp.macro` file, if the specified is newer than the current file.

For more information about the `cp.macro` file, see sk96217: What is a cp.macro file?

Syntax

```
contract_util cpmacro /<path_to>/cp.macro
```

This command shows one of these messages:

Message	Description
`CntrctUtils_ Write_cp_macro returned -1`	The `contract_util cpmacro` command failed: ■ Failed to create a temporary file. ■ Failed to write to a temporary file. ■ Failed to replace the current file.
`CntrctUtils_ Write_cp_macro returned 0`	The `contract_util cpmacro` command was able to overwrite the current file with the specified file, because the specified file is newer.
`CntrctUtils_ Write_cp_macro returned 1`	The `contract_util cpmacro` command did not overwrite the current file, because it is newer than the specified file.

contract_util download

Description

Downloads all associated Check Point Service Contracts from User Center, or from a local file.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util download
      {-h | -help}
      local
            {-h | -help}
            [{hfa | maj_upgrade | min_upgrade | upgrade}] <Service
Contract File>
      uc
            {-h | -help}
            [-i] [{hfa | maj_upgrade | min_upgrade | upgrade}]
<Username> <Password> [<Proxy Server> [<Proxy Username>:<Proxy
Password>]]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-i`	Interactive mode - prompts the user for the User Center credentials and proxy server settings.
`local`	Specifies to download the Service Contract from the local file. This is equivalent to the "`cplic contract put`" command (see *"cplic contract" on page 142*).
`uc`	Specifies to download the Service Contract from the User Center.
`hfa`	Downloads the information about a Hotfix Accumulator.
`maj_upgrade`	Downloads the information about a Major version.
`min_upgrade`	Downloads the information about a Minor version.
`upgrade`	Downloads the information about an upgrade.
<Username>	Your User Center account e-mail address.
<Password>	Your User Center account password.
<Proxy Server> [*<Proxy Username>*:*<Proxy Password>*]	Specifies that the connection to the User Center goes through the proxy server. ■ *<Proxy Server>* - IP address of resolvable hostname of the proxy server ■ *<Proxy Username>* - Username for the proxy server. ■ *<Proxy Password>* - Password for the proxy server. Note - If you do not specify the proxy server explicitly, the command uses the proxy server configured in the management database.
<Service Contract File>	Path to and the name of the Service Contract file. First, you must download the Service Contract file from your User Center account.

contract_util mgmt

Description

Delivers the Service Contract information from the Management Server to the managed Security Gateways.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util mgmt
```

contract_util print

Description

Shows all the installed licenses and whether the Service Contract covers these license, which entitles them for upgrade or not.

This command can show which licenses are not recognized by the Service Contract file.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util [-d] print
      {-h | -help}
      hfa
      maj_upgrade
      min_upgrade
      upgrade
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Shows a formatted table header and more information.
`hfa`	Shows the information about Hotfix Accumulator.
`maj_upgrade`	Shows the information about Major version.
`min_upgrade`	Shows the information about Minor version.
`upgrade`	Shows the information about an upgrade.

contract_util summary

Description

Shows post-installation summary and whether this Check Point server is eligible for upgrades.

Syntax

```
contract_util summary
      hfa
      maj_upgrade
      min_upgrade
      upgrade
```

Parameters

Parameter	Description
`hfa`	Shows the information about Hotfix Accumulator.
`maj_upgrade`	Shows the information about Major version.
`min_upgrade`	Shows the information about Minor version.
`upgrade`	Shows the information about an upgrade.

contract_util update

Description

Updates the Check Point Service Contracts from your User Center account.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util update
      [-proxy <Proxy Server>:<Proxy Port>]
      [-ca_path <Path to ca-bundle.crt File>]
```

Parameters

Parameter	Description
`update`	Updates Check Point Service Contracts (attached to pre-installed licenses) from your User Center account.
`-proxy <Proxy Server>:<Proxy Port>`	Specifies that the connection to the User Center goes through the proxy server: ■ `<Proxy Server>` - IP address of resolvable hostname of the proxy server. ■ `<Proxy Port>` - The applicable port on the proxy server. Note - If you do not specify the proxy explicitly, the command uses the proxy configured in the management database.
`-ca_path <Path to ca-bundle.crt File>`	Specifies the path to the Certificate Authority Bundle file (`ca-bundle.crt`). **Note** - If you do not specify the path explicitly, the command uses the default path.

contract_util verify

Description

Checks whether the Security Gateway is eligible for an upgrade.

This command is the same as the *"contract_util check" on page 52* command, but it also interprets the return values and shows a meaningful message.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util verify
```

cp_conf

Description

Configures or reconfigures a Check Point product installation.

Note - The available options for each Check Point server depend on the configuration and installed products.

Syntax on a Management Server

```
cp_conf
      -h
      admin <options>
      auto <options>
      ca <options>
      client <options>
      finger <options>
      lic <options>
      snmp <options>
```

Syntax on a Security Gateway / each Cluster Member in Gaia Clish or the Expert mode

```
cp_conf
      -h
      adv_routing <options>
      auto <options>
      corexl <options>
      fullha <options>
      ha <options>
      intfs <options>
      lic <options>
      sic <options>
      snmp <options>
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cp_conf
      -h
      adv_routing <options>
      auto <options>
      corexl <options>
      fullha <options>
      ha <options>
      intfs <options>
      lic <options>
      sic <options>
      snmp <options>
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cp_conf
      -h
      adv_routing <options>
      auto <options>
      corexl <options>
      fullha <options>
      ha <options>
      intfs <options>
      lic <options>
      sic <options>
      snmp <options>
```

Parameters

Parameter	Description
`-h`	Shows the entire built-in usage.
`admin <options>`	Configures Check Point system administrators for the Security Management Server. See *"cp_conf admin" on page 65*.
`adv_routing <options>`	Enables or disables the Advanced Routing feature on this Security Gateway. **Important** - Do **not** use these outdated commands. To configure Advanced Routing, see the *R81.20 Gaia Advanced Routing Administration Guide*.

Parameter	Description
`auto <options>`	Shows and configures the automatic start of Check Point products during boot. See *"cp_conf auto" on page 68*.
`ca <options>`	▪ Configures the Certificate Authority's (CA) Fully Qualified Domain Name (FQDN). ▪ Initializes the Internal Certificate Authority (ICA). See *"cp_conf ca" on page 70*.
`client <options>`	Configures the GUI clients that can use SmartConsole to connect to the Security Management Server. See *"cp_conf client" on page 72*.
`corexl <options>`	Enables or disables CoreXL on this Security Gateway / Cluster Member / Security Group. See *"cp_conf corexl" on page 983*.
`finger <options>`	Shows the ICA's Fingerprint. See *"cp_conf finger" on page 76*.
`fullha <options>`	Manages Full High Availability Cluster. See *"cp_conf fullha" on page 986*. **Note** - This command does **not** apply to Scalable Platforms (Maestro and Chassis).
`ha <options>`	Enables or disables cluster membership on this Security Gateway / Cluster Member. See *"cp_conf ha" on page 987*. **Note** - This command does **not** apply to Scalable Platforms (Maestro and Chassis).
`intfs <options>`	Sets the topology of interfaces on a Security Gateway / Cluster Member, which you manage with SmartProvisioning. See *"cp_conf intfs" on page 989*. **Note** - This command does **not** apply to Scalable Platforms (Maestro and Chassis).
`lic <options>`	Manages Check Point licenses. See *"cp_conf lic" on page 78*.
`sic <options>`	Manages SIC on this Security Gateway / Cluster Member / Security Group. See *"cp_conf sic" on page 994*.

Parameter	Description
`snmp <options>`	Do **not** use these outdated commands. To configure SNMP, see the *R81.20 Gaia Administration Guide* - Chapter *System Management* - Section *SNMP*.

cp_conf admin

Description

Configures Check Point system administrators for the Security Management Server.

Notes:

- Multi-Domain Server does not support this command.
- Only one administrator can be defined in the *"cpconfig" on page 134* menu. To define additional administrators, use SmartConsole.
- This command corresponds to the option **Administrator** in the *"cpconfig" on page 134* menu.

Syntax

```
cp_conf admin
      -h
      add [<UserName> <Password> {a | w | r}]
      add -gaia [{a | w | r}]
      del <UserName1> <UserName2> ...
      get
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`add [<UserName> <Password> {a | w | r}]`	Adds a Check Point system administrator: ■ *<UserName>* - Specifies the administrator's username ■ *<Password>* - Specifies the administrator's password ■ `a` - Assigns all permissions - read settings, write settings, and manage administrators ■ `w` - Assigns permissions to read and write settings only (cannot manage administrators) ■ `r` - Assigns permissions to only read settings
`add -gaia [{a | w | r}]`	Adds the Gaia administrator user `admin`: ■ `a` - Assigns all permissions - read settings, write settings, and manage administrators ■ `w` - Assigns permissions to read and write settings only (cannot manage administrators) ■ `r` - Assigns permissions to only read settings
`del <UserName1> <UserName2> ...`	Deletes the specified system administrators.
`get`	Shows the list of the configured system administrators.
`get -gaia`	Shows the management permissions assigned to the Gaia administrator user `admin`.

Example 1 - Adding a Check Point system administrator

```
[Expert@MGMT:0]# cp_conf admin add
Administrator name: admin
Administrator admin already exists.
Do you want to change Administrator's Permissions (y/n) [n] ? y

Permissions for all products (Read/[W]rite All, [R]ead Only All, [C]ustomized) c
        Permission for SmartUpdate (Read/[W]rite, [R]ead Only, [N]one) w
        Permission for Monitoring (Read/[W]rite, [R]ead Only, [N]one) w

Administrator admin was modified successfully and has
Read/Write Permission for SmartUpdate
Read/Write Permission for Monitoring
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin get

The following Administrators
are defined for this Security Management Server:

admin (Read/Write Permission for all products; )
[Expert@MGMT:0]#
```

Example 2 - Adding the Gaia administrator user

```
[Expert@MGMT:0]# cp_conf admin add -gaia
Permissions for all products (Read/[W]rite All, [R]ead Only All, [C]ustomized) c
        Permission for SmartUpdate (Read/[W]rite, [R]ead Only, [N]one) w
        Permission for Monitoring (Read/[W]rite, [R]ead Only, [N]one) w
Administrator admin was added successfully and has
Read/Write Permission for SmartUpdate
Read/Write Permission for Monitoring
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin get -gaia

The following Administrators
are defined for this Security Management Server:

admin (Read/Write Permission for all products; ) - Gaia admin
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin add -gaia a
Administrator admin already exists.

Administrator admin was modified successfully and has
Read/Write Permission for all products with Permission to Manage Administrators
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin add -gaia w
Administrator admin already exists.

Administrator admin was modified successfully and has
Read/Write Permission for all products without Permission to Manage Administrators
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin add -gaia r
Administrator admin already exists.

Administrator admin was modified successfully and has
Read Only Permission for all products
[Expert@MGMT:0]#
```

cp_conf auto

Description

Shows and controls which of Check Point products start automatically during boot.

Note - This command corresponds to the option **Automatic start of Check Point Products** in the *"cpconfig" on page 134* menu.

Note - On a Multi-Domain Server, use the option **Automatic Start of Multi-Domain Server** in the *"mdsconfig" on page 762*menu.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cp_conf auto
      -h
      {enable | disable} <Product1> <Product2> ...
      get all
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cp_conf auto
      -h
      {enable | disable} <Product1> <Product2> ...
      get all
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cp_conf auto
      -h
      {enable | disable} <Product1> <Product2> ...
      get all
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cp_conf auto
      -h
      {enable | disable} <Product1> <Product2> ...
      get all
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`{enable | disable} <Product1> <Product2> ...`	Controls whether the installed Check Point products start automatically during boot. This command is for Check Point use only.
`get all`	Shows which of these Check Point products start automatically during boot: ■ Check Point Security Gateway ■ QoS (former FloodGate-1) ■ SmartEvent Suite

Example from a Security Management Server

```
[Expert@MGMT:0]# cp_conf auto get all
Check Point Security Gateway is not installed

QoS is not installed

The SmartEvent Suite will start automatically at boot time.

[Expert@MGMT:0]#
```

Example from a Security Gateway

```
[Expert@GW:0] cp_conf auto get all
The Check Point Security Gateway will start automatically at boot time.

QoS will start automatically at boot time.

SmartEvent Suite is not installed.

[Expert@GW:0]#
```

cp_conf ca

Description

This command changes the settings of the Internal Certificate Authority (ICA).

Note - On a Security Management Server, this command corresponds to the option **Certificate Authority** in the *"cpconfig" on page 134* menu.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cp_conf ca
       -h
       fqdn <FQDN Name>
       init
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`fqdn <FQDN Name>`	Configures the Fully Qualified Domain Name (FQDN) for the Internal Certificate Authority (ICA). The "`<FQDN Name>`" is the text string in this format: *hostname.domainname* **Notes:** ■ The existing certificates for configured objects are **not** revoked. ■ The existing ICA certificate is **not** changed. ■ The Management Server uses the specified "`<FQDN Name>`" to configure the Certificate Revocation List Distribution Point (CRL DP) property in all certificates that the ICA generates. Refer to this command: *"cpca_client get_crldp" on page 109*
`init`	Initializes the Internal Certificate Authority (ICA).

Example

```
[Expert@MyMGMT:0]# hostname
MyMGMT
[Expert@MyMGMT:0]#

[Expert@MyMGMT:0]# domainname
checkpoint.com
[Expert@MyMGMT:0]#

[Expert@MyMGMT:0]# cp_conf ca fqdn MyMGMT.checkpoint.com
Trying to contact Certificate Authority. It might take a while...
Certificate was created successfully
MyMGMT.checkpoint.com was successfully set to the Internal CA
[Expert@MyMGMT:0]#
```

cp_conf client

Description

Configures the GUI clients that are allowed to connect with SmartConsoles to the Security Management Server.

Notes:

- Multi-Domain Server does not support this command.
- This command corresponds to the option **GUI Clients** in the *"cpconfig" on page 134* menu.

Syntax

```
cp_conf client
      add <GUI Client>
      createlist <GUI Client 1> <GUI Client 2> ...
      del <GUI Client 1> <GUI Client 2> ...
      get
```

Parameters

Parameter	Description
`-h`	Shows the built-in usage.
<GUI Client>	*<GUI Client>* can be one of these: ■ One IPv4 address (for example, 192.168.10.20), or one IPv6 address (for example, 3731:54:65fe:2::a7) ■ One hostname (for example, MyComputer) ■ "Any" - To denote all IPv4 and IPv6 addresses without restriction ■ A range of IPv4 addresses (for example, 192.168.10.0/255.255.255.0), or a range of IPv6 addresses (for example, 2001::1/128) ■ IPv4 address wildcard (for example, 192.168.10.*)
`add` *<GUI Client>*	Adds a GUI client.
`createlist` *<GUI Client 1> <GUI Client 2> ...*	Deletes the current allowed GUI clients and creates a new list of allowed GUI clients.
`del` *<GUI Client 1> <GUI Client 2> ...*	Deletes the specified the GUI clients.
`get`	Shows the allowed GUI clients.

Examples

Example 1 - Configure one IPv4 address

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add 172.20.168.15
172.20.168.15 was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
172.20.168.15
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del 172.20.168.15
172.20.168.15 was deleted successfully
[Expert@MGMT:0]#
```

Example 2 - Configure one hostname

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add MySmartConsoleHost
MySmartConsoleHost was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
MySmartConsoleHost
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del MySmartConsoleHost
MySmartConsoleHost was deleted successfully
[Expert@MGMT:0]#
```

Example 3 - Configure "Any"

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add "Any"
Any was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
Any
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del "Any"
Any was deleted successfully
[Expert@MGMT:0]#
```

Example 4 - Configure a range of IPv4 addresses

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add 172.20.168.0/255.255.255.0
172.20.168.0/255.255.255.0 was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
172.20.168.0/255.255.255.0
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del 172.20.168.0/255.255.255.0
172.20.168.0/255.255.255.0 was deleted successfully
[Expert@MGMT:0]#
```

Example 5 - Configure IPv4 address wildcard

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add 172.20.168.*
172.20.168.* was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
172.20.168.*
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del 172.20.168.*
172.20.168.* was deleted successfully
[Expert@MGMT:0]#
```

Example 6 - Delete the current list and create a new list of allowed GUI clients

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add 172.20.168.0/255.255.255.0
172.20.168.0/255.255.255.0 was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
172.20.168.0/255.255.255.0
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client createlist 192.168.40.0/255.255.255.0 172.30.40.55
New list was created successfully
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
192.168.40.0/255.255.255.0
172.30.40.55
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client createlist "Any"
New list was created successfully
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
Any
[Expert@MGMT:0]#
```

cp_conf finger

Description

Shows the Internal Certificate Authority's Fingerprint.

This fingerprint is a text string derived from the ICA certificate on the Security Management Server, Multi-Domain Server, or Domain Management Server.

This fingerprint verifies the identity of the Security Management Server, Multi-Domain Server, or Domain Management Server when you connect to it with SmartConsole.

Note - This command corresponds to the option **Certificate's Fingerprint** in the *"cpconfig" on page 134* menu.

Note - On a Multi-Domain Server:

- To see the fingerprint of the Multi-Domain Server, this command corresponds to the option **Certificate's Fingerprint** in the *"mdsconfig" on page 762* menu.
- You can run this command in these contexts:
  - To see the fingerprint of the Multi-Domain Server, run it in the context of the Multi-Domain Server:

    ```
    mdsenv
    ```

  - To see the fingerprint of a Domain Management Server, run it in the context of the applicable Domain Management Server:

    ```
    mdsenv <IP Address or Name of Domain Management Server>
    ```

Syntax

```
cp_conf finger
      -h
      get
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`get`	Shows the ICA's Fingerprint.

Example

```
[Expert@MGMT:0]# cp_conf finger get
EDNA COCO MOLE ATOM ASH MOT SAGE NINE ILL TINT HI CUBE
[Expert@MGMT:0]#
```

cp_conf lic

Description

Shows, adds and deletes Check Point licenses.

Note - This command corresponds to the option **Licenses and contracts** in the *"cpconfig" on page 134* menu.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cp_conf lic
      -h
      add -f <Full Path to License File>
      add -m <Host> <Date> <Signature Key> <SKU/Features>
      del <Signature Key>
      get [-x]
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cp_conf lic
      -h
      add -f <Full Path to License File>
      add -m <Host> <Date> <Signature Key> <SKU/Features>
      del <Signature Key>
      get [-x]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cp_conf lic
      -h
      add -f <Full Path to License File>
      add -m <Host> <Date> <Signature Key> <SKU/Features>
      del <Signature Key>
      get [-x]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cp_conf lic
      -h
      add -f <Full Path to License File>
      add -m <Host> <Date> <Signature Key> <SKU/Features>
      del <Signature Key>
      get [-x]
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`add -f <Full Path to License File>`	Adds a license from the specified Check Point license file. You get this license file in the *Check Point User Center*. This is the same command as the *"cplic db_add" on page 144*.
`add -m <Host> <Date> <Signature Key> <SKU/Features>`	Adds the license manually. You get these license details in the *Check Point User Center*. This is the same command as the *"cplic db_add" on page 144*.
`del <Signature Key>`	Delete the license based on its signature. This is the same command as the *"cplic del" on page 149*.
`get [-x]`	Shows the local installed licenses. If you specify the "`-x`" parameter, output also shows the signature key for every installed license. This is the same command as the *"cplic print" on page 153*.

Example 1 - Adding the license from the file

```
[Expert@HostName:0]# cp_conf lic add -f ~/License.lic
License was installed successfully.
[Expert@HostName:0]#

[Expert@HostName:0]# cp_conf lic get
Host            Expiration   Signature                                  Features
192.168.3.28    25Aug2019    xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx   CPMP-XXX
[Expert@HostName:0]#
```

Example 2 - Adding the license manually

```
[Expert@MyHostName:0]# cp_conf lic add -m MyHostName 25Aug2019
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx CPMP-XXX
License was successfully installed
[Expert@MyHostName:0]#

[Expert@MyHostName:0]# cp_conf lic get
Host             Expiration   Signature                                 Features
192.168.3.28     25Aug2019    xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx   CPMP-XXX
[Expert@MyHostName:0]#
```

cp_log_export

Description

Exports Check Point logs over syslog.

For more information, see sk122323 and *R81.20 Logging and Monitoring Administration Guide*.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cp_log_export
```

```
cp_log_export <command-name> help
```

Parameters

Parameter	Description
No Parameters	Shows the built-in general help.
`<command-name> help`	Shows the built help for the specified internal command.

Internal Commands

Name	Description
`add`	Configures a new Check Point Log Exporter. `cp_log_export add name <Name> target-server <Target-Server> target-port <Target-Server-Port> protocol {udp | tcp} [Optional Arguments]`
`delete`	Removes an existing Log Exporter. `cp_log_export delete name <Name>`

`reexport`	Resets the current log position and exports all logs again based on the configuration.
	`cp_log_export reexport name <Name> --apply-now`
	`cp_log_export reexport name <Name> start-position <Position of Last Exported Log> --apply-now`
	`cp_log_export reexport name <Name> start-position <Position of Gap Start> end-position <Position of Gap End> --apply-now`

`restart`	Restarts a Log Exporter process. `cp_log_export restart name <Name>`
`set`	Updates an existing Log Exporter configuration. `cp_log_export set name <Name> [<Optional Arguments>]`
`show`	Shows the current Log Exporter configuration. `cp_log_export show [<Optional Arguments>]`
`start`	Starts an existing Log Exporter process. `cp_log_export start name <Name>`
`status`	Shows a Log Exporter overview status. `cp_log_export status [<Optional Arguments>]`
`stop`	Stops an existing Log Exporter process. `cp_log_export stop name <Name>`

Internal Command Arguments

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`--apply-now`	Applies immediately any change that was done with the "`add`", "`set`", "`delete`", or "`reexport`" command.	Optional	Optional	**Mandatory**	N / A	N / A	**Mandatory**
`ca-cert <Path>`	Specifies the full path to the CA certificate file `*.pem`. **Important** - Applicable only when the value of the "`encrypted`" argument is "`true`".	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`client-cert <Path>`	Specifies the full path to the client certificate `*.p12`. **Important** - Applicable only when the value of the "`encrypted`" argument is "`true`".	Optional	Optional	N / A	N / A	N / A	N / A
`client-secret <Phrase>`	Specifies the challenge phrase used to create the client certificate `*.p12`. **Important** - Applicable only when the value of the "`encrypted`" argument is "`true`".	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`domain-server {mds | all}`	On a Multi-Domain Server, specifies the applicable Domain Management Server context. On a Multi-Domain Log Server, specifies the applicable Domain Log Server context. **Important:** ■ "`mds`" (in small letters) - Exports all logs from only the main **MDS** level. ■ "`all`" (in small letters) - Exports all logs from **all** Domains.	**Mandatory**	**Mandatory**	**Mandatory**	N / A	Optional	**Mandatory**

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`enabled {true | false}`	Specifies whether to allow the Log Exporter to start when you run the *"cpstart" on page 208* or *"mdsstart" on page 770* command. Default: `true`	Optional	Optional	N / A	N / A	N / A	N / A
`encrypted {true | false}`	Specifies whether to use TSL (SSL) encryption to send the logs. Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A
`end-position <Position>`	Specifies the end position, up to which to export the logs.	N / A	N / A	N / A	N / A	N / A	Optional
`export-attachment-ids {true | false}`	Specifies whether to add a field to the exported logs that represents the ID of log's attachment (if exists). Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`export-attachment-link {true | false}`	Specifies whether to add a field to the exported logs that represents a link to SmartView that shows the log card and automatically opens the attachment. Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A
`export-link {true | false}`	Specifies whether to add a field to the exported logs that represents a link to SmartView that shows the log card. Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`export-link-ip {true | false}`	Specifies whether to make the links to SmartView use a custom IP address (for example, for a Log Server behind NAT). **Important** - Applicable only when the value of the "`export-link`" argument is "`true`", or the value of the "`export-attachment-link`" argument is "`true`". Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A
`export-log-position {true | false}`	Specifies whether to export the log's position. Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`filter-action-in {"Action1","Action2",... | false}`	Specifies whether to export all logs that contain a specific value in the "**Action**" field. Each value must be surrounded by double quotes (""). Multiple values are supported and must be separated by a comma without spaces. To see all valid values: 1. In SmartConsole, go to the **Logs & Monitor** view and open the **Logs** tab. 2. In the top query field, enter **action:** and a letter. Examples of values:	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	▪ **Accept** ▪ **Block** ▪ **Bypass** ▪ **Detect** ▪ **Drop** ▪ **HTTPS Bypass** ▪ **HTTPS Inspect** ▪ **Prevent** ▪ **Reject** **Important** - This parameter replaces any other filter configuration that was declared earlier on this field directly in the filtering XML file. Other field filters are not overwritten.						

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`filter-blade-in {"Blade1","Blade2",... | false}`	Specifies whether to export all logs that contain a specific value in the "**Blade**" field (the object name of the Software Blade that generated these logs). Each value must be surrounded by double quotes (""). Multiple values are supported and must be separated by a comma without spaces. To see all valid values: 1. In SmartConsole, go to the **Logs & Monitor** view and open the **Logs** tab.	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	2. In the top query field, enter **blade:** and a letter. Examples of values: ■ **Anti-Bot** ■ **Firewall** ■ **HTTPS Inspection** ■ **Identity Awareness** ■ **IPS** Valid Software Blade families: ■ **Access** ■ **TP** ■ **Endpoint** ■ **Mobile**						

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	Important - This parameter replaces any other filter configuration that was declared earlier on this field directly in the filtering XML file. Other field filters are not overwritten.						

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`filter-origin-in {"Origin1","Origin2",... | false}`	Specifies whether to export all logs that contain a specific value in the "**Origin**" field (the object name of the Security Gateway / Cluster Member that generated these logs). Each origin value must be surrounded by double quotes (""). Multiple values are supported and must be separated by a comma without spaces.	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	Important - This parameter replaces any other filter configuration that was declared earlier on this field directly in the filtering XML file. Other field filters are not overwritten.						
`format {generic | cef | json | leef | logrhythm | rsa | splunk | syslog}`	Specifies the format, in which the logs are exported. Default: `syslog`	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`name "<Name>"`	Specifies the unique name of the Log Exporter configuration.	**Mandatory**	**Mandatory**	**Mandatory**	Optional. By default, applies to all.	Optional. By default, applies to all.	**Mandatory**

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	Notes: ■ Allowed characters are: Latin letters, digits ("`0-9`"), minus ("`-`"), underscore ("`_`"), and period ("`.`"). ■ Must start with a letter. ■ The minimum length is two characters. ■ The "`add`" command creates a new target directory with the specified unique name in the `$EXPORTERDIR/targets/` directory.						

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`protocol {tcp | udp}`	Specifies the Layer 4 Transport protocol to use (TCP or UDP). There is no default value.	**Mandatory**	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`read-mode {raw | semi-unified}`	Specifies the mode, in which to read the log files. ■ `raw` - Specifies to export log records without any unification. ■ `semi-unified` - Specifies to export log records with step-by-step unification. That is, for each log record, export a record that unifies this record with all previously-encountered records with the same ID.	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	Default: `semi-unified` Default: `raw`						
`reconnect-interval {<Number> | default}`	Specifies the interval (in minutes) after which the Log Exporter must connect again to the target server after the connection is lost. To disable, enter the value "`default`". There is no default value.	Optional	Optional	N / A	N / A	N / A	N / A
`start-position <Position>`	Specifies the start position, from which to export the logs.	N / A	N / A	N / A	N / A	N / A	Optional
`target-port <Target-Server-Port>`	Specifies the listening port on the target server, to which you export the logs.	**Mandatory**	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`target-server <Target-Server>`	Specifies the IP address or FQDN of the target server, to which you export the logs.	**Mandatory**	Optional	N / A	N / A	N / A	N / A
`time-in-milli {true | false}`	Specifies whether to export logs with the time resolution in milliseconds. Requires Security Gateways R81 and higher. Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A

cpca_client

Description

Execute operations on the Internal Certificate Authority (ICA).

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d]
      create_cert <options>
      double_sign <options>
      get_crldp <options>
      get_pubkey <options>
      init_certs <options>
      lscert <options>
      revoke_cert <options>
      revoke_non_exist_cert <options>
      search <options>
      set_ca_services <options>
      set_cert_validity <options>
      set_mgmt_tool <options>
      set_sign_hash <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`create_cert <options>`	Issues a SIC certificate for the Security Management Server or Domain Management Server. See *"cpca_client create_cert" on page 105*.

Parameter	Description
`double_sign <options>`	Creates a second signature for a certificate. See *"cpca_client double_sign" on page 107*.
`get_crldp <options>`	Shows how to access a CRL file from a CRL Distribution Point. See *"cpca_client get_crldp" on page 109*.
`get_pubkey <options>`	Saves the encoding of the public key of the ICA's certificate to a file. See *"cpca_client get_pubkey" on page 111*.
`init_certs <options>`	Imports a list of DNs for users and creates a file with registration keys for each user. See *"cpca_client init_certs" on page 112*.
`lscert <options>`	Shows all certificates issued by the ICA. See *"cpca_client lscert" on page 113*.
`revoke_cert <options>`	Revokes a certificate issued by the ICA. See *"cpca_client revoke_cert" on page 116*.
`revoke_non_exist_ cert <options>`	Revokes a non-existent certificate issued by the ICA. See *"cpca_client revoke_non_exist_cert" on page 119*.
`search <options>`	Searches for certificates in the ICA. See *"cpca_client search" on page 120*.
`set_ca_services <options>`	Controls the Certificate Authority Services Portal. See *"cpca_client set_ca_services" on page 123*.
`set_cert_validity <options>`	Configures the default certificate validity period for new certificates. See *"cpca_client set_cert_validity" on page 125*.
`set_mgmt_tool <options>`	Controls the ICA Management Tool. See *"cpca_client set_mgmt_tool" on page 126*.
`set_sign_hash <options>`	Sets the hash algorithm that the CA uses to sign the file hash. See *"cpca_client set_sign_hash" on page 131*.

cpca_client create_cert

Description

Issues a SIC certificate for the Security Management Server or Domain Management Server.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] create_cert [-p <CA port number>] -n "CN=<Common
Name>" -f <Full Path to PKCS12 file> [-w <Password>] [-k {SIC |
USER | IKE | ADMIN_PKG}] [-c "<Comment for Certificate>"]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <CA port number>`	Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18209.
`-n "CN=<Common Name>"`	Sets the CN to the specified `<Common Name>`.
`-f <Full Path to PKCS12 file>`	Specifies the PKCS12 file, which stores the certificate and keys.
`-w <Password>`	Optional. Specifies the certificate password.
`-k {SIC | USER | IKE | ADMIN_PKG}`	Optional. Specifies the certificate kind.
`-c "<Comment for Certificate>"`	Optional. Specifies the certificate comment (must enclose in double quotes).

Example

```
[Expert@MGMT:0]# cpca_client create_cert -n "cn=cp_mgmt" -f $CPDIR/conf/sic_cert.p12
```

cpca_client double_sign

Description

Creates a second signature for a certificate.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] double_sign [-p <CA port number>] -i <Certificate File in PEM format> [-o <Full Path to Output File>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <CA port number>`	Optional. Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18209.
`-i <Certificate File in PEM format>`	Imports the specified certificate (only in PEM format).
`-o <Full Path to Output File>`	Optional. Saves the certificate into the specified file.

Example

```
[Expert@MGMT:0]# cpca_client double_sign -i certificate.pem

 Requesting Double Signature for the following Certificate:
        refCount: 1
        Subject: Email=example@example.com,CN=http://www.example.com/,OU=ValiCert Class 2 Policy
Validation Authority,O=exampleO\, Inc.,L=ExampleL Validation Network

 Double Sign of Cert:
 ====================
 (
        : (
                :dn ("Email=example@example.com,CN=http://www.example.com/,OU=exampleOU Class 2
Policy Validation Authority,O=exampleO\, Inc.,L=exampleL Validation Network")
                :doubleSignCert (52016390... ... ...ebb67e96)
                :return_code (0)
        )
)

[Expert@MGMT:0]#
```

cpca_client get_crldp

Description

Shows the Fully Qualified Domain Name (FQDN) configured for the Internal Certificate Authority (ICA) with the "*"cp_conf ca" on page 70*" command.

The Management Server uses this FQDN:

1. To configure the Certificate Revocation List Distribution Point (CRL DP) property in all certificates that the ICA generates.
2. To create the URL for accessing the CRL.

   Example: `http://MyMGMT.checkpoint.com:18264/ICA_CRL1.crl`

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] get_crldp [-p <ICA port number>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <ICA port number>`	Optional. Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18264.

Example

```
[Expert@MyMGMT:0]# hostname
MyMGMT
[Expert@MyMGMT:0]#

[Expert@MyMGMT:0]# domainname
checkpoint.com
[Expert@MyMGMT:0]#

[Expert@MyMGMT:0]# cpca_client get_crldp
MyMGMT.checkpoint.com
[Expert@MyMGMT:0]
```

cpca_client get_pubkey

Description

Saves the encoding of the public key of the ICA's certificate to a file.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] get_pubkey [-p <CA port number>] <Full Path to Output File>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <CA port number>`	Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18209.
<Full Path to Output File>	Saves the encoding of the public key of the ICA's certificate to the specified file.

Example

```
[Expert@MGMT:0]# cpca_client get_pubkey /tmp/key.txt[Expert@MGMT:0]#
[Expert@MGMT:0]# cat /tmp/key.txt
3082010a... ... ...f98b8910
[Expert@MGMT:0]#
```

cpca_client init_certs

Description

Imports a list of Distinguished Names (DN) for users and creates a file with registration keys for each user.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] init_certs [-p <CA port number>] -i <Full Path to Input File> -o <Full Path to Output File>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <CA port number>`	Optional. Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18209.

`-i <Full Path to Input File>`	Imports the specified file.
	Make sure to use the full path.
	Make sure that there is an empty line between each DN in the specified file.
	Example:
	`...CN=test1,OU=users...`
	`<Empty Line>`
	`...CN=test2,OU=users...`

`-o <Full Path to Output File>`	Saves the registration keys to the specified file. This command saves the error messages in the `<Name of Output File>.failures` file in the same directory.

cpca_client lscert

Description

Shows all certificates issued by the ICA.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] lscert [-dn <SubString>] [-stat {Pending | Valid
| Revoked | Expired | Renewed}] [-kind {SIC | IKE | User | LDAP}]
[-ser <Certificate Serial Number>] [-dp <Certificate Distribution
Point>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-dn <SubString>`	Optional. Filters the search results to those with a DN that matches the specified `<SubString>`. This command does not support multiple values.
`-stat {Pending | Valid | Revoked | Expired | Renewed}`	Optional. Filters the search results to those with certificate status that matches the specified status. This command does not support multiple values.
`-kind {SIC | IKE | User | LDAP}`	Optional. Filters the search results to those with certificate kind that matches the specified kind. This command does not support multiple values.
`-ser <Certificate Serial Number>`	Optional. Filters the search results to those with certificate serial number that matches the specified serial number. This command does not support multiple values.
`-dp <Certificate Distribution Point>`	Optional. Filters the search results to the specified Certificate Distribution Point (CDP). This command does not support multiple values.

Example

```
[Expert@MGMT:0]# cpca_client lscert -stat Revoked
Operation succeeded. rc=0.
5 certs found.

Subject = CN=VSX2,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Revoked   Kind = SIC   Serial = 5521   DP = 0
Not_Before: Sun Apr  8 14:10:01 2018   Not_After: Sat Apr  8 14:10:01 2023

Subject = CN=VSX1,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Revoked   Kind = SIC   Serial = 9113   DP = 0
Not_Before: Sun Apr  8 14:09:02 2018   Not_After: Sat Apr  8 14:09:02 2023

Subject = CN=VSX1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Revoked   Kind = IKE   Serial = 82434   DP = 2
Not_Before: Mon May 14 19:15:05 2018   Not_After: Sun May 14 19:15:05 2023
[Expert@MGMT:0]#


[Expert@MGMT:0]# cpca_client lscert -kind IKE
Operation succeeded. rc=0.
3 certs found.

Subject = CN=VS1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Valid   Kind = IKE   Serial = 27214   DP = 1
Not_Before: Wed Apr 11 17:26:02 2018   Not_After: Tue Apr 11 17:26:02 2023

Subject = CN=VSX_Cluster VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Valid   Kind = IKE   Serial = 64655   DP = 1
Not_Before: Mon Apr  9 19:36:31 2018   Not_After: Sun Apr  9 19:36:31 2023

Subject = CN=VSX1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Revoked   Kind = IKE   Serial = 82434   DP = 2
Not_Before: Mon May 14 19:15:05 2018   Not_After: Sun May 14 19:15:05 2023
[Expert@MGMT:0]#
```

cpca_client revoke_cert

Description

Revokes a certificate issued by the ICA.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] revoke_cert [-p <CA port number>] -n "CN=<Common Name>" -s <Certificate Serial Number>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <CA port number>`	Optional. Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18209.

`-n "CN=<Common Name>"`	Specifies the certificate CN.
	To get the CN, run the *"cpca_client lscert" on page 113* command and examine the text that you see between the "`Subject =`" and the "`,O=...`".
	Example
	From this output:
	`Subject = CN=VS1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x`
	`Status = Valid Kind = IKE Serial = 27214 DP = 1`
	`Not_Before: Wed Apr 11 17:26:02 2018 Not_After: Tue Apr 11 17:26:02 2023`
	you get this syntax:
	`-n "CN=VS1 VPN Certificate`
	Note - You can use the parameter '`-n`' only, or together with the parameter "`-s`".

`-s <Certificate Serial Number>`	Specifies the certificate serial number. To see the serial number, run the *"cpca_client lscert" on page 113* command. **Note** - You can use the parameter "`-s`" only, or together with the parameter "`-n`".

Example 1 - Revoking a certificate specified by its CN

```
[Expert@MGMT:0]# cpca_client lscert
Subject = CN=VS1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Valid Kind = IKE Serial = 27214 DP = 1
Not_Before: Wed Apr 11 17:26:02 2018 Not_After: Tue Apr 11 17:26:02 2023
[Expert@MGMT:0]#
[Expert@MGMT:0]# cpca_client -d revoke_cert -n "CN=VS1 VPN Certificate"
 Certificate was revoked successfully
[Expert@MGMT:0]#
```

Example 2 - Revoking a certificate specified by its serial number.

```
[Expert@MGMT:0]# cpca_client lscert
Subject = CN=VS1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Valid Kind = IKE Serial = 27214 DP = 1
Not_Before: Wed Apr 11 17:26:02 2018 Not_After: Tue Apr 11 17:26:02 2023
[Expert@MGMT:0]#
[Expert@MGMT:0]# cpca_client -d revoke_cert -s 27214
 Certificate was revoked successfully
[Expert@MGMT:0]#
```

cpca_client revoke_non_exist_cert

Description

Revokes a non-existent certificate issued by the ICA.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] revoke_non_exist_cert -i <Full Path to Input File>
```

Parameters

Parameter	Description
`-d`	Runs the `cpca_client` command under debug.

`-i <Full Path to Input File>`	Specifies the file that contains the list of the certificate to revoke.
	You must create this file in the same format as the *"cpca_client lscert" on page 113* command prints its output.
	Example
	`Subject = CN=cp_mgmt,O=MGMT.5p72vp`
	`Status = Valid  Kind = SIC  Serial = 30287  DP = 0`
	`Not_Before: Sat Apr  7 19:40:12 2018  Not_After: Fri Apr  7 19:40:12 2023`
	`<Empty Line>`
	`Subject = CN=cp_mgmt,O=MGMT.5p72vp`
	`Status = Valid  Kind = SIC  Serial = 60870  DP = 0`
	`Not_Before: Sat Apr  7 19:40:13 2018  Not_After: Fri Apr  7 19:40:13 2023`

Note - This command saves the error messages in the `<Name of Input File>.failures` file.

cpca_client search

Description

Searches for certificates in the ICA.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] search <String> [-where {dn | comment | serial |
device_type | device_id | device_name}] [-kind {SIC | IKE | User |
LDAP}] [-stat {Pending | Valid | Revoked | Expired | Renewed}] [-
max <Maximal Number of Results>] [-showfp {y | n}]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
<String>	Specifies the text to search in the certificates. You can enter only one text string that does not contain spaces.

Parameter	Description
`-where {dn | comment | serial | device_type | device_id | device_name}`	Optional. Specifies the certificate's field, in which to search for the string: ■ `dn` - Certificate DN ■ `comment` - Certificate comment ■ `serial` - Certificate serial number ■ `device_type` - Device type ■ `device_id` - Device ID ■ `device_name` - Device Name The default is to search in all fields.
`-kind {SIC | IKE | User | LDAP}`	Optional. Specifies the certificate kind to search. You can enter multiple values in this format: `-kind <Kind1> <Kind2> <Kind3>` The default is to search for all kinds.
`-stat {Pending | Valid | Revoked | Expired | Renewed}`	Optional. Specifies the certificate status to search. You can enter multiple values in this format: `-stat <Status1> <Status2> <Status3>` The default is to search for all statuses.
`-max <Maximal Number of Results>`	Optional. Specifies the maximal number of results to show. ■ Range: 1 and greater ■ Default: 200
`-showfp {y | n}`	Optional. Specifies whether to show the certificate's fingerprint and thumbprint: ■ `y` - Shows the fingerprint and thumbprint (this is the default) ■ `n` - Does not show the fingerprint and thumbprint

Example 1

```
[Expert@MGMT:0]# cpca_client search samplecompany -where comment -kind SIC LDAP -stat Pending
Valid Renewed
```

Example 2

```
[Expert@MGMT:0]# cpca_client search 192.168.3.51 -where dnOperation succeeded. rc=0.
1 certs found.

Subject = CN=192.168.3.51,O=MGMT.5p72vp
Status = Valid Kind = SIC Serial = 73455 DP = 0
Not_Before: Sat Apr 7 19:40:12 2018 Not_After: Fri Apr 7 19:40:12 2023
Fingerprint = XXX XXX XXX XXX XXX XXX XXX XXX XXX XXX XXX XXX
Thumbprint = xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
[Expert@MGMT:0]#
```

Example 3

```
[Expert@MGMT:0]# cpca_client search 192.168.3.51 -where dn -showfp nOperation succeeded. rc=0.
1 certs found.

Subject = CN=192.168.3.51,O=MGMT.5p72vp
Status = Valid Kind = SIC Serial = 73455 DP = 0
Not_Before: Sat Apr 7 19:40:12 2018 Not_After: Fri Apr 7 19:40:12 2023
[Expert@MGMT:0]#
```

cpca_client set_ca_services

Description

This command enables and disables the Certificate Authority Services Portal on the Management Server on the TCP port 18268.

From this portal, you can download the applicable Internal Certificate Authority certificates.

For trust purposes, you can install this certificate on the applicable Security Gateways, externally managed Site to Site VPN peer gateways, Remote Access VPN clients, clients that use Clientless VPN, and so on.

Note - In R81.20, the TCP port 18264 on the Management Server is available only for the retrieval of the CRL (Certificate Revocation List).

Syntax

```
cpca_client set_ca_services {on | off}
```

Parameters

Parameter	Description
`on`	Enables the Certificate Authority Services Portal
`off`	Disables the Certificate Authority Services Portal

Procedure for a Security Management Server

Enabling the Certificate Authority Services Portal

1. Connect to the command line on the Security Management Server.
2. Log in to the Expert mode.
3. Enable the Certificate Authority Services Portal:

   ```
   cpca_client set_ca_services on
   ```

4. With a web browser, connect to:

   ```
   http://<IP Address of Security Management Server>:18268
   ```

5. Download the required certificate.
6. Install this certificate on the applicable computers.

Disabling the Certificate Authority Services Portal

1. Connect to the command line on the Security Management Server.
2. Log in to the Expert mode.
3. Disable the Certificate Authority Services Portal:

```
cpca_client set_ca_services off
```

Procedure for a Domain Management Server

Enabling the Certificate Authority Services Portal

1. Connect to the command line on the Multi-Domain Server.
2. Log in to the Expert mode.
3. Go to the context of the Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

4. Enable the Certificate Authority Services Portal:

```
cpca_client set_ca_services on
```

5. With a web browser, connect to:

```
http://<IP Address of Domain Management Server>:18268
```

6. Download the required certificate.
7. Install this certificate on the applicable computers.

Disabling the Certificate Authority Services Portal

1. Connect to the command line on the Multi-Domain Server.
2. Log in to the Expert mode.
3. Go to the context of the Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

4. Disable the Certificate Authority Services Portal:

```
cpca_client set_ca_services off
```

cpca_client set_cert_validity

Description

This command configures the default certificate validity period for new certificates.

Notes:

- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- The new certificate validity period applies only to certificate you create after this change.

Syntax

```
cpca_client set_cert_validity -k {SIC | IKE | USER} [-y <Number of Years>] [-d <Number of Days>] [-h <Number of Hours>] [-s <Number of Seconds>]
```

Parameters

Parameter	Description
`-k {SIC | IKE | USER}`	Specifies the certificate type.
`-y <Number of Years>`	Specifies the validity period in years.
`-d <Number of Days>`	Specifies the validity period in days.
`-h <Number of Hours>`	Specifies the validity period in hours.
`-s <Number of Seconds>`	Specifies the validity period in seconds.

Example

```
[Expert@MGMT:0]# cpca_client set_cert_validity -k IKE -y 3
 cert validity period was changed successfully.
[Expert@MGMT:0]#
```

cpca_client set_mgmt_tool

Description

Controls the ICA Management Tool.

This tool is disabled by default.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

See sk102837: Best Practices - ICA Management Tool configuration

Syntax

```
cpca_client [-d] set_mgmt_tool {on | off | add | remove | clean |
print} [-p <CA port number>] [{-a <Administrator DN> | -u <User
DN> | -c <Custom User DN>}]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`on`	Starts the ICA Management Tool.
`off`	Stops the ICA Management Tool.
`add`	Adds the specified administrator, user, or custom user that is permitted to use the ICA Management Tool.
`remove`	Removes the specified administrator, user, or custom user that is permitted to use the ICA Management Tool.
`clean`	Removes all administrators, users, or custom users that are permitted to use the ICA Management Tool.
`print`	Shows the configured administrators, users, or custom users that are permitted to use the ICA Management Tool.

Parameter	Description
`-p <CA port number>`	Optional. Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18265.
`-a <Administrator DN>`	Optional. Specifies the DN of the administrator that is permitted to use the ICA Management Tool. Must specify the full DN as appears in SmartConsole **Procedure** 1. Open **Object Explorer** > **Users** 2. Open the Administrator object or a User object properties 3. Click the **Certificates** pane 4. Select the certificate and click the pencil icon 5. Click **View certificate details** 6. In the **Certificate Info** window, click the **Details** tab 7. Click the **Subject** field 8. Concatenate all fields Example: `-a "CN=ICA_Tool_Admin,OU=users,O=MGMT.s6t98x"`
`-u <User DN>`	Optional. Specifies the DN of the user that is permitted to use the ICA Management Tool. Must specify the full DN as appears in SmartConsole: **Procedure** 1. Open **Object Explorer** > **Users** 2. Open the Administrator object or a User object properties 3. Click the **Certificates** pane 4. Select the certificate and click the pencil icon 5. Click **View certificate details** 6. In the **Certificate Info** window, click the **Details** tab 7. Click the **Subject** field 8. Concatenate all fields Example: `-u "CN=ICA_Tool_User,OU=users,O=MGMT.s6t98x"`

Parameter	Description
`-c <Custom User DN>`	Optional. Specifies the DN for the custom user that is permitted to use the ICA Management Tool. Must specify the full DN as appears in SmartConsole. **Procedure** 1. Open **Object Explorer** > **Users** 2. Open the Administrator object or a User object properties 3. Click the **Certificates** pane 4. Select the certificate and click the pencil icon 5. Click **View certificate details** 6. In the **Certificate Info** window, click the **Details** tab 7. Click the **Subject** field 8. Concatenate all fields Example: `-c "CN=ICA_Tool_User,OU=users,O=MGMT.s6t98x"`

Note - If you run the "`cpca_client set_mgmt_tool`" command without the parameter "`-a`" or "`-u`", the list of the permitted administrators and users is not changed. The previously defined permitted administrators and users can start and stop the ICA Management Tool.

To connect to the ICA Management Tool

1. In SmartConsole, configure the required administrator and user objects.

   You must create a certificate for these administrators and users.

   You use this certificate to configure the permitted users in the ICA Management Tool and in the client web browsers.

2. In the command line on the Management Server, add the required administrators and users that are permitted to use the ICA Management Tool.

   ```
   cpca_client set_mgmt_tool add ...
   ```

3. In the command line on the Management Server, start the ICA Management Tool.

   ```
   cpca_client set_mgmt_tool on
   ```

4. Check the status of the ICA Management Tool:

   ```
   cpca_client set_mgmt_tool print
   ```

5. Import the administrator's / user's certificate into the Windows Certificate Store:.

   a. Right-click the *.p12 file you saved when you created the required administrator / user, and click **Install PFX**.

      The **Certificate Import Wizard** opens.

   b. In the **Store Location** section, select the applicable option:

      - **Current User** (this is the default)
      - **Local Machine**

   c. Click **Next**.

   d. Enter the same certificate password you used when you created the required administrator / user certificate.

   e. Clear **Enable strong private key protection**.

   f. Select **Mark this key as exportable**.

   g. Click **Next**.

   h. Select **Place all certificates in the following store** > click **Browse** > select **Personal** > click **OK**.

   i. Click **Next**.

   j. Click **Finish**.

6. In a web browser, connect to the ICA Management Tool:

   ```
   https://<IP Address of the Management Server>:18265
   ```

   Important - The fact that the TCP port 18265 is open is not a vulnerability. The ICA Management Tool Portal is secured and protected by SSL. In addition, only authorized administrators and users are allowed to access it using a certificate.

7. A dialog box with this message appears:

   ```
   Client Authentication

   Identification

   The Web site you want to view requests identification.

   Select the certificate to use when connecting.
   ```

8. Select the appropriate certificate for authenticating to the ICA Management Tool.
9. Click **OK**.
10. In the **Security Alert** dialog box, click **Yes**.

cpca_client set_sign_hash

Description

Sets the hash algorithm that the CA uses to sign the file hash. Also, see sk103840.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] set_sign_hash {sha1 | sha256 | sha384 | sha512}
```

Important - After this change, you must restart the Check Point services with these commands:

- On Security Management Server, run:
  1. `cpstop`
  2. `cpstart`
- On a Multi-Domain Server, run:
  1. `mdsstop_customer <Name or IP Address of Domain Management Server>`
  2. `mdsstart_customer <Name or IP Address of Domain Management Server>`

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{sha1 | sha256 | sha384 | sha512}`	The hash algorithms that the CA uses to sign the file hash. The default algorithm is SHA-256.

Example

```
[Expert@MGMT:0]# cpca_client set_sign_hash sha256

You have selected the signature hash function SHA-256
WARNING: This hash algorithm is not supported in Check Point gateways prior to R71.
WARNING: It is also not supported on older clients and SG80 R71.

Are you sure? (y/n)
y
Internal CA signature hash changed successfully.
Note that the signature on the Internal CA certificate has not changed, but this has no security
implications.
[Expert@MGMT:0]#
[Expert@MGMT:0]# cpstop ; cpstart
```

cpca_create

Description

Creates new Check Point Internal Certificate Authority database.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_create [-d] -dn <CA DN>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-dn <CA DN>`	Specifies the Certificate Authority Distinguished Name (DN).

cpconfig

Description

This command starts the Check Point Configuration Tool.

This utility configures specific settings for the installed Check Point products.

Syntax

```
cpconfig
```

Note - On a Multi-Domain Server, run the *"mdsconfig" on page 762* command.

Menu Options

Note - The options shown depend on the configuration and installed products.

Menu Option	Description
Licenses and contracts	Manages Check Point licenses and contracts on this server.
Administrator	Configures Check Point system administrators for this server.
GUI Clients	Configures the GUI clients that can use SmartConsole to connect to this server.
SNMP Extension	Obsolete. Do **not** use this option anymore. To configure SNMP, see the *R81.20 Gaia Administration Guide* - Chapter *System Management* - Section *SNMP*.
Random Pool	Configures the RSA keys, to be used by Gaia Operating System.
Certificate Authority	Initializes the Internal Certificate Authority (ICA) and configures the Certificate Authority's (CA) Fully Qualified Domain Name (FQDN).
Certificate's Fingerprint	Shows the ICA's Fingerprint. This fingerprint is a text string derived from the server's ICA certificate. This fingerprint verifies the identity of the server when you connect to it with SmartConsole.
Automatic start of Check Point Products	Shows and controls which of the installed Check Point products start automatically during boot.
Exit	Exits from the Check Point Configuration Tool.

Example - Menu on a Security Management Server

```
[Expert@MyMGMT:0]# cpconfig
This program will let you re-configure
your Check Point Security Management Server configuration.


Configuration Options:
----------------------
(1) Licenses and contracts
(2) Administrator
(3) GUI Clients
(4) SNMP Extension
(5) Random Pool
(6) Certificate Authority
(7) Certificate's Fingerprint
(8) Automatic start of Check Point Products

(9) Exit

Enter your choice (1-9) :
```

cplic

Description

The `cplic` command manages Check Point licenses.

You can run this command in Gaia Clish or in the Expert mode.

License Management is divided into three types of commands:

Licensing Commands	Applies To	Description
Local licensing commands	Management Servers, Security Gateways and Cluster Members	You execute these commands locally on the Check Point servers.
Remote licensing commands	Management Servers only	You execute these commands on the Security Management Server or Domain Management Server. These changes affect the managed Security Gateways and Cluster Members.
License Repository commands	Management Servers only	You execute these commands on the Security Management Server or Domain Management Server. These changes affect the licenses stored in the local license repository.

For more about managing licenses, see the *R81.20 Security Management Administration Guide*.

Syntax for Local Licensing on a Management Server itself

```
cplic [-d]
      {-h | -help}
      check <options>
      contract <options>
      del <options>
      print <options>
      put <options>
```

Syntax for Remote Licensing on managed Security Gateways and Cluster Members

```
cplic [-d]
      {-h | -help}
      del <options>
      get <options>
      put <options>
      upgrade <options>
```

Syntax for License Database Operations on a Management Server

```
cplic [-d]
      {-h | -help}
      db_add <options>
      db_print <options>
      db_rm <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{-h | -help}`	Shows the applicable built-in usage.
`check <options>`	Confirms that the license includes the feature on the local Security Gateway or Management Server. See *"cplic check" on page 140*.
`contract <options>`	Manages (deletes and installs) the Check Point Service Contract on the local Check Point server. See *"cplic contract" on page 142*.
`db_add <options>`	Applies only to a Management Server. Adds licenses to the license repository on the Management Server. See *"cplic db_add" on page 144*.

Parameter	Description
`db_print <options>`	Applies only to a Management Server. Shows the details of Check Point licenses stored in the license repository on the Management Server. See *"cplic db_print" on page 146*.
`db_rm <options>`	Applies only to a Management Server. Removes a license from the license repository on the Management Server. See *"cplic db_rm" on page 148*.
`del <options>`	Deletes a Check Point license on a host, including unwanted evaluation, expired, and other licenses. See *"cplic del" on page 149*.
`del <Object Name> <options>`	Detaches a Central license from a remote managed Security Gateway or Cluster Member. See *"cplic del <object name>" on page 150*.
`get <options>`	Applies only to a Management Server. Retrieves all licenses from managed Security Gateways and Cluster Members into the license repository on the Management Server. See *"cplic get" on page 151*.
`print <options>`	Prints details of the installed Check Point licenses on the local Check Point server. See *"cplic print" on page 153*.
`put <options>`	Installs and attaches licenses on a Check Point server. See *"cplic put" on page 155*.
`put <Object Name> <options>`	Attaches one or more Central or Local licenses to a remote managed Security Gateways and Cluster Members. See *"cplic put <object name>" on page 158*.
`upgrade <options>`	Applies only to a Management Server. Upgrades licenses in the license repository with licenses in the specified license file. See *"cplic upgrade" on page 161*.

cplic check

Description

Confirms that the license includes the feature on the local Security Gateway or Management Server. See sk66245.

Syntax

```
cplic check {-h | -help}
```

```
cplic [-d] check [-p <Product>] [-v <Version>] [{-c | -count}] [-t <Date>] [{-r | -routers}] [{-S | -SRusers}] <Feature>
```

You can run this command:

- On a Management Server / Security Gateway / Cluster Member in Gaia Clish or the Expert mode
- On a Scalable Platform Security Group in Gaia gClish or the Expert mode

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <Product>`	Product, for which license information is requested. Some examples of products: ■ `fw1` - FireWall-1 infrastructure on Security Gateway / Cluster Member / Security Group (all Software Blades), or Management Server (all Software Blades) ■ `mgmt` - Multi-Domain Server infrastructure ■ `services` - Entitlement for various services ■ `cvpn` - Mobile Access ■ `etm` - QoS (FloodGate-1) ■ `eps` - Endpoint Software Blades on Management Server
`-v <Version>`	Product version, for which license information is requested.

Parameter	Description
{-c | -count}	Outputs the number of licenses connected to this feature.
-t <*Date*>	Checks license status on future date. Use the format **ddmmyyyy**. A feature can be valid on a given date on one license, but invalid on another.
{-r | -routers}	Checks how many routers are allowed. The <*Feature*> option is not needed.
{-S | -SRusers}	Checks how many SecuRemote users are allowed.
<*Feature*>	Feature, for which license information is requested.

Example from a Management Server

```
[Expert@MGMT]# cplic print -p
Host Expiration Primitive-Features
W.X.Y.Z 24Mar2016 ::CK-XXXXXXXXXXX fw1:6.0:swb fw1:6.0:comp fw1:6.0:compunlimited fw1:6.0:cluster-1 fw1:6.0:cpxmgmt_qos_u_sites
fw1:6.0:sprounl fw1:6.0:nxunlimit fw1:6.0:swp evnt:6.0:smrt_evnt fw1:6.0:fwc fw1:6.0:ca fw1:6.0:rtmui fw1:6.0:sstui fw1:6.0:fwlv
fw1:6.0:cmd evnt:6.0:alzd5 evnt:6.0:alzc1 evnt:6.0:alzs1 fw1:6.0:sstui fw1:6.0:fwlv fw1:6.0:sme10 etm:6.0:rtm_u fw1:6.0:cep1 fw1:6.0:rt
fw1:6.0:cemid fw1:6.0:web_sec_u fw1:6.0:workflow fw1:6.0:ram1 fw1:6.0:routers fw1:6.0:supmgmt fw1:6.0:supunlimit fw1:6.0:prov
fw1:6.0:atlas-unlimit fw1:6.0:filter fw1:6.0:ui psmp:6.0:psmsunlimited fw1:6.0:vpe_unlimit fw1:6.0:cluster-u fw1:6.0:remote1 fw1:6.0:aes
fw1:6.0:strong fw1:6.0:rdp fw1:6.0:des fw1:6.0:isakmp fw1:6.0:dbvr_unlimit fw1:6.0:cmpmgmt fw1:6.0:rtmmgmt fw1:6.0:fgmgmt fw1:6.0:blades
fw1:6.0:cpipv6 fw1:6.0:mgmtha fw1:6.0:remote
[Expert@MGMT]#
```

Example from a Management Server in High Availability

```
[Expert@MGMT]# cplic check -p fw1 -v 6.0 -c mgmtha
cplic check 'mgmtha': 1 licenses
[Expert@MGMT]#
```

Example from a Security Gateway

```
[Expert@GW]# cplic print -p
Host Expiration Primitive-Features
W.X.Y.Z 23Mar2016 ::CK-XXXXXXXXXXX fw1:6.0:swb fw1:6.0:abot fw1:6.0:ips fw1:6.0:appi fw1:6.0:aspm fw1:6.0:av1000 fw1:6.0:urlf fw1:6.0:av
fw1:6.0:vsx5 fw1:6.0:cpls fw1:6.0:cluster-u fw1:6.0:mpu fw1:6.0:sxl_vpn fw1:6.0:sxl_fw fw1:6.0:sxl_ppk fw1:6.0:connect fw1:6.0:pam
etm:6.0:fgcountunl etm:6.0:fg etm:6.0:tclog etm:6.0:fgvpn fw1:6.0:identity cvpn:6.0:ccvunl cvpn:6.0:cvpnunlimited fw1:6.0:des
fw1:6.0:strong fw1:6.0:encryption cvpn:6.0:cvpn fw1:6.0:dlp evnt:6.0:smrt_evnt fw1:6.0:ipsa fw1:6.0:spcps fw1:6.0:pam
fw1:6.0:enchostsunlimit fw1:6.0:aes fw1:6.0:rdp fw1:6.0:isakmp fw1:6.0:xlate fw1:6.0:auth fw1:6.0:content fw1:6.0:sync fw1:6.0:fm
fw1:6.0:blades fw1:6.0:sr5000 fw1:6.0:hostsunlimit fw1:6.0:mc_all_8 fw1:6.0:multicore
[Expert@GW]#
```

Example from a Cluster Member

```
[Expert@GW]# cplic check cluster-u
cplic check 'cluster-u': license valid
[Expert@GW]#
[Expert@GW]# cplic check -c cluster-u
cplic check 'cluster-u': 9 licenses
[Expert@GW]#
```

cplic contract

Description

Deletes the Check Point Service Contract on the local Check Point server.

Installs the Check Point Service Contract on the local Check Point server.

Note

- For more information about Service Contract files, see sk33089: What is a Service Contract File?
- If you install a Service Contract on a managed Security Gateway / Cluster Member / Scalable Platform Security Group, you must update the license repository on the applicable Management Server - either with the *"cplic get" on page 151* command, or in SmartUpdate.

Syntax

```
cplic contract -h
```

```
cplic [-d] contract
      del
            -h
            <Service Contract ID>
      put
            -h
            [{-o | -overwrite}] <Service Contract File>
```

You can run this command:

- On a Management Server / Security Gateway / Cluster Member in Gaia Clish or the Expert mode
- On a Scalable Platform Security Group in Gaia gClish or the Expert mode

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`del`	Deletes the Service Contract from the `$CPDIR/conf/cp.contract` file on the local Check Point server.
`put`	Merges the Service Contract to the `$CPDIR/conf/cp.contract` file on the local Check Point server.
<Service Contract ID>	ID of the Service Contract.
`{-o | -overwrite}`	Specifies to overwrite the current Service Contract.
<Service Contract File>	Path to and the name of the Service Contract file. First, you must download the Service Contract file from your *Check Point User Center* account.

cplic db_add

Description

Adds licenses to the license repository on the Management Server.

When you add Local licenses to the license repository, Management Server automatically attaches them to the managed Security Gateway / Cluster Member with the matching IP address.

When you add Central licenses, you must manually attach them.

Note - You get the license details in the *Check Point User Center*.

Syntax

```
cplic db_add {-h | -help}
```

```
cplic [-d] db_add -l <License File> [<Host>] [<Expiration Date>]
[<Signature>] [<SKU/Features>]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-l <License File>`	Name of the file that contains the license.
<Host>	Hostname or IP address of the Security Management Server / Domain Management Server.
<Expiration Date>	The license expiration date.
<Signature>	The license signature string. For example: `aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m` Case sensitive. Hyphens are optional.

Parameter	Description
<SKU/Features>	The SKU of the license summarizes the features included in the license. For example, `CPSUITE-EVAL-3DES-vNG`

Example

If the file `192.0.2.11.lic` contains one or more licenses, the command "`cplic db_add -l 192.0.2.11.lic`" produces output similar to:

```
[Expert@MGMT]# cplic db_add -l 192.0.2.11.lic
Adding license to database ...
Operation Done
[Expert@MGMT]#
```

cplic db_print

Description

Shows the details of Check Point licenses stored in the license repository on the Management Server.

Syntax

```
cplic db_print {-h | -help}
```

```
cplic [-d] db_print {<Object Name> | -all} [{-n | -noheader}] [-x]
[{-t | -type}] [{-a | -attached}]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
<Object Name>	Prints only the licenses attached to *<Object Name>*. *<Object Name>* is the name of the Security Gateway / Cluster Member object as defined in SmartConsole.
`-all`	Prints all the licenses in the license repository.
`{-n | -noheader}`	Prints licenses with no header.
`-x`	Prints licenses with their signatures.
`{-t | -type}`	Prints licenses with their type: Central or Local.
`{-a | -attached}`	Shows to which object the license is attached. Useful, if the parameter "`-all`" is specified.

Example

```
[Expert@MGMT:0]# cplic db_print -all
 Retrieving license information from database ...

The following licenses appear in the database:
==============================================
Host             Expiration Features
192.168.3.28     25Aug2019  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx CPMP-XXX  CK-XXXXXXXXXXX
[Expert@MGMT:0]#

[Expert@MGMT:0]# cplic db_print -all -x -a
 Retrieving license information from database ...

The following licenses appear in the database:
==============================================
Host             Expiration Features
192.168.3.28     25Aug2019  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx CPMP-XXX  CK-XXXXXXXXXXX  MGMT
[Expert@MGMT:0]#
```

cplic db_rm

Description

Removes a license from the license repository on the Management Server.

After you remove the license from the repository, it can no longer use it.

Warning - You can run this command ONLY after you detach the license with the *"cplic del" on page 149* command.

Syntax

```
cplic db_rm {-h | -help}
cplic [-d] db_rm <Signature>
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
<Signature>	The signature string within the license. To see the license signature string, run the *"cplic print" on page 153* command.

Example

```
[Expert@MGMT:0]# cplic db_rm 2f540abb-d3bcb001-7e54513e-kfyigpwn
```

cplic del

Description

Deletes a Check Point license on a host, including unwanted evaluation, expired, and other licenses.

This command can delete a license on both local server, and on remote managed servers.

Syntax

```
cplic del {-h | -help}
cplic [-d] del [-F <Output File>] <Signature> <Object Name>
```

You can run this command:

- On a Management Server / Security Gateway / Cluster Member in Gaia Clish or the Expert mode
- On a Scalable Platform Security Group in Gaia gClish or the Expert mode

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-F <Output File>`	Saves the command output to the specified file.
`<Signature>`	The signature string within the license. To see the license signature string, run the *"cplic print" on page 153* command.
`<Object Name>`	The name of the Security Gateway / Cluster Member object as configured in SmartConsole.

cplic del <object name>

Description

Detaches a Central license from a remote managed Security Gateway or Cluster Member.

When you run this command, it automatically updates the license repository.

The Central license remains in the license repository as an unattached license.

Syntax

```
cplic del {-h | -help}
```

```
cplic [-d] del <Object Name> [-F <Output File>] [-ip <Dynamic IP Address>] <Signature>
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
<Object Name>	The name of the Security Gateway / Cluster Member object as defined in SmartConsole.
`-F` *<Output File>*	Saves the command output to the specified file.
`-ip` *<Dynamic IP Address>*	Deletes the license on the DAIP Security Gateway with the specified IP address. **Note** - If this parameter is used, then object name must be a DAIP Security Gateway.
<Signature>	The signature string within the license. To see the license signature string, run the *"cplic print" on page 153* command.

cplic get

Description

Retrieves all licenses from managed Security Gateways and Cluster Members into the license repository on the Management Server.

This command helps synchronize the license repository with the managed Security Gateways and Cluster Members.

When you run this command, it updates the license repository with all local changes.

Syntax

```
cplic get {-h | -help}
```

```
cplic [-d] get
      -all
      <IP Address>
      <Host Name>
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-all`	Retrieves licenses from all Security Gateways and Cluster Members in the managed network.
<IP Address>	The IP address of the Security Gateway / Cluster Member, from which licenses are to be retrieved.
<Host Name>	The name of the Security Gateway / Cluster Member object as defined in SmartConsole, from which licenses are to be retrieved.

Example

If the Security Gateway with the object name `MyGW` contains four Local licenses, and the license repository contains two other Local licenses, the command "`cplic get MyGW`" produces output similar to this:

```
[Expert@MGMT:0]# cplic get MyGW
Get retrieved 4 licenses.
Get removed 2 licenses.
[Expert@MGMT:0]#
```

cplic print

Description

Prints details of the installed Check Point licenses on the local Check Point server.

Note - On a Security Gateway / Cluster Member / Scalable Platform Security Group, this command prints all installed licenses (both Local and Central).

Syntax

```
cplic print {-h | -help}
```

```
cplic [-d] print[{-n | -noheader}] [-x] [{-t | -type}] [-F <Output File>] [{-p | -preatures}] [-D]
```

You can run this command:

- On a Management Server / Security Gateway / Cluster Member in Gaia Clish or the Expert mode
- On a Scalable Platform Security Group in Gaia gClish or the Expert mode

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{-n | -noheader}`	Prints licenses with no header.
`-x`	Prints licenses with their signature.
`{-t | -type]`	Prints licenses showing their type: Central or Local.
`-F <Output File>`	Saves the command output to the specified file.
`{-p | -preatures}`	Prints licenses resolved to primitive features.
`-D`	On a Multi-Domain Server, prints only Domain licenses.

Example 1

```
[Expert@HostName:0]# cplic print
Host             Expiration   Features
192.168.3.28     25Aug2019    CPMP-XXX  CK-XXXXXXXXXXX
[Expert@HostName:0]#
```

Example 2

```
[Expert@HostName:0]# cplic print -x
Host             Expiration   Signature                          Features
192.168.3.28     25Aug2019    xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx   CPMP-XXX  CK-XXXXXXXXXXX
[Expert@HostName:0]#
```

cplic put

Description

Installs one or more Local licenses on a Check Point server.

Note - You get the license details in the *Check Point User Center*.

Syntax

```
cplic put {-h | -help}
```

```
cplic [-d] put [{-o | -overwrite}] [{-c | -check-only}] [{-s | -select}] [-F <Output File>] [{-P | -Pre-boot}] [{-k | -kernel-only}] -l <License File> [<Host>] [<Expiration Date>] [<Signature>] [<SKU/Features>]
```

You can run this command:

- On a Management Server / Security Gateway / Cluster Member in Gaia Clish or the Expert mode
- On a Scalable Platform Security Group in Gaia gClish or the Expert mode

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{-o | -overwrite}`	On a Security Gateway / Cluster Member / Scalable Platform Security Group, this command erases only the local licenses, but not central licenses that are installed remotely.
`{-c | -check-only}`	Verifies the license. Checks if the IP of the license matches the Check Point server and if the signature is valid.
`{-s | -select}`	Selects only the local license whose IP address matches the IP address of the Check Point server.

Parameter	Description
`-F <Output File>`	Saves the command output to the specified file.
`{-P | -Pre-boot}`	Use this option after you have upgraded and before you reboot the Check Point server. Use of this option will prevent certain error messages.
`{-K | -kernel-only}`	Pushes the current valid licenses to the kernel. For use by Check Point Support only.
`-l <License File>`	Name of the file that contains the license.
<Host>	Hostname or IP address of the Security Gateway / Cluster Member / Scalable Platform Security Group for a local license. Hostname or IP address of the Security Management Server / Domain Management Server for a central license.
<Expiration Date>	The license expiration date.
<Signature>	The signature string within the license. Case sensitive. The hyphens are optional.
<SKU/Features>	The SKU of the license summarizes the features included in the license. For example: `CPSUITE-EVAL-3DES-vNG`

Copy and paste the parameters from the license received from the User Center:

Parameter	Description
`host`	The IPv4 address of the external interface (in quad-dot notation).
`expiration date`	The license expiration date. It can be `never`.
`signature`	The license signature string. Case sensitive. The hyphens are optional.
`SKU/features`	A string listing the SKU and the Certificate Key of the license. The SKU of the license summarizes the features included in the license. For example: `CPSB-SWB CPSB-ADNC-M CK0123456789ab`

Example

```
[Expert@HostName:0]# cplic put -l License.lic
Host Expiration SKU
192.168.2.3 14Jan2016  CPSB-SWB CPSB-ADNC-M CK0123456789ab
[Expert@HostName:0]#
```

cplic put <object name>

Description

Attaches one or more Central or Local licenses to a remote managed Security Gateways and Cluster Members.

When you run this command, it automatically updates the license repository.

Note

- You get the license details in the *Check Point User Center*.
- You can attach more than one license.

Syntax

```
cplic put {-h | -help}
```

```
cplic [-d] put <Object Name> [-ip<Dynamic IP Address> ] [-F
<Output File>] -l <License File> [<Host>] [<Expiration Date>]
[<Signature>] [<SKU/Feature>]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
<Object Name>	The name of the Security Gateway / Cluster Member object, as defined in SmartConsole.
`-ip` *<Dynamic IP Address>*	Installs the license on the Security Gateway with the specified IP address. This parameter is used to install a license on a Security Gateway with dynamically assigned IP address (DAIP). **Note** - If you use this parameter, then the object name must be that of a DAIP Security Gateway.
`-F` *<Output File>*	Saves the command output to the specified file.
`-l` *<License File>*	Installs the licenses from the *<License file>*.
<Host>	Hostname or IP address of the Security Management Server / Domain Management Server.
<Expiration Date>	The license expiration date.
<Signature>	The license signature string. Case sensitive. The hyphens are optional.
<SKU/Features>	The SKU of the license summarizes the features included in the license. For example: `CPSUITE-EVAL-3DES-vNG`

Copy and paste the parameters from the license received from the User Center:

Parameter	Description
`host`	The IP address of the external interface (in quad-dot notation). The last part cannot be 0 or 255.
`expiration date`	The license expiration date. It can be `never`.
`signature`	The license signature string. Case sensitive. The hyphens are optional.
`SKU/features`	A string listing the SKU and the Certificate Key of the license. The SKU of the license summarizes the features included in the license. For example: `CPSB-SWB CPSB-ADNC-M CK0123456789ab`

cplic upgrade

Description

Upgrades licenses in the license repository with licenses in the specified license file.

Note - You get this license file in the *Check Point User Center*.

Syntax

```
cplic upgrade {-h | -help}
cplic [-d] upgrade -l <Input File>
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-l <Input File>`	Upgrades the licenses in the license repository and Check Point Security Gateways / Cluster Members to match the licenses in the specified file.

Example

This example explains the procedure to upgrade the licenses in the license repository.

There are two Software Blade licenses in the input file:

- One license does not match any license on a remote managed Security Gateway.
- The other license matches an NGX-version license on a managed Security Gateway that has to be upgraded.

Workflow in this example:

1. Upgrade the Security Management Server to the latest version.

   Ensure that there is connectivity between the Security Management Server and the Security Gateways with the previous product versions.

2. Import all licenses into the license repository.

   You can also do this after you upgrade the products on the remote Security Gateways.

3. Run this command:

```
cplic get -all
```

Example:

```
[Expert@MyMGMT]# cplic get -all
Getting licenses from all modules ...
MyGW:
Retrieved 1 licenses
```

4. To see all the licenses in the repository, run this command:

```
cplic db_print -all -a
```

Example:

```
[Expert@MyMGMT]# cplic db_print -all -a
Retrieving license information from database ...

The following licenses appear in the database:
=================================================
Host Expiration Features
192.0.2.11 Never CPFW-FIG-25-53 CK49C3A3CC7121 MyGW1
192.0.2.11 26Nov2017 CPSB-SWB CPSB-ADNC-M CK0123456789ab MyGW2
```

5. In the *Check Point User Center*, view the licenses for the products that were upgraded from version NGX to a Software Blades license.

   You can also create new upgraded licenses.

6. Download a file containing the upgraded licenses.

   Only download licenses for the products that were upgraded from version NGX to Software Blades.

7. If you did not import the version NGX licenses into the repository, import the version NGX licenses now.

   Use this command:

```
cplic get -all
```

8. Run the license upgrade command:

```
cplic upgrade -l <Input File>
```

   - The licenses in the downloaded license file and in the license repository are compared.
   - If the certificate keys and features match, the old licenses in the repository and in the remote Security Gateways are updated with the new licenses.
   - A report of the results of the license upgrade is printed.

For more about managing licenses, see the *R81.20 Security Management Administration Guide*.

CPLogInvestigator

Description

This heuristic tool can analyze the specified logs files from managed Security Gateways and show:

- The estimated number of events per day.
- The number of logs from each Software Blade.
- The number of logs during each minute.

Important - You can run this command only in the Expert mode.

Syntax

```
CPLogInvestigator
      [-h]
      [-d]
      [-a]
      [{-i /<Path>/<Name of Log File> | -f <Path to Directory>}]
      [-l]
      [-m]
      [-p]
      [-u <Number of Users>]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
No Parameters	Analyzes the events in all the `$FWDIR/log/*.log` files (the active log and the rotated logs). The default analysis duration for each log file is 60 seconds.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. This option "`-d`" is not supported (ignored) when specified together with the option "`-p`".
`-a`	Analyzes the events in all the "`*.log`" files - the active log and the rotated logs. The default path is `$FWDIR/log/`. The default analysis duration is 60 seconds. If the number of log files is large, and the log files are large, then the analysis can take significant time.
`-f <Path to Directory>`	Analyzes the events in all the "`*.log`" files in the specified directory. This parameter must the last parameter in the syntax.
`-i /<Path>/<Name of Log File>`	Analyzes the events in the specified log file. This parameter must the last parameter in the syntax.
`-l`	Limits the duration of the analysis to 60 seconds.
`-m`	Saves the number of logs for each minute of analyzes log files in the output file called "`logPerMinute.txt`" in the current working directory.
`-p`	Shows the daily estimated number of logs from each Software Blade that generated these logs.
`-u <Number of Users>`	Specifies the number of required users to show estimations for events from the Application Control and the URL Filtering Software Blades.

Examples

Example 1 - "CPLogInvestigator" (command without parameters)

```
[Expert@Mgmt:0]# CPLogInvestigator

Thank you for using log investigator tool.

============================================================
Start reading log file: /opt/CPsuite-R81.20/fw1/log/fw.log

Start reading log file: /opt/CPsuite-R81.20/fw1/log/fw.log from log 0

..
Reading log file is DONE.

Start reading log file: /opt/CPsuite-R81.20/fw1/log/2025-04-11_000000.log

Start reading log file: /opt/CPsuite-R81.20/fw1/log/2025-04-11_000000.log from log 0

..
Reading log file is DONE.


Total scanned 10846112 logs out of 28070147 logs in file
Scanned logs dates are from 29-01-2025 00:00:00 to 11-04-2025 19:48:14
Observed blades:
     - Application Control
     - IPS
     - N/A
     - VPN-1 & FireWall-1

========================================

Summary - Estimations based on findings:

Log file size per day: 1.7815GB (149018 logs)

Estimated events per day:
- Estimated events per day based on active blades: 1

Storage required per day:
- SmartEvent: 0.0000GB
- Log Server: 1.7815GB
- Log Server + SmartLog: 3.5629GB

============================================================
[Expert@Mgmt:0]#
```

Example 2 - "CPLogInvestigator -p -i <log file>"

```
[Expert@Mgmt:0]# CPLogInvestigator -p -i $FWDIR/log/fw.log


Thank you for using log investigator tool.

============================================================
Start reading log file: /opt/CPsuite-R81.20/fw1/log/fw.log

Start reading log file: /opt/CPsuite-R81.20/fw1/log/fw.log from log 0

..
Reading log file is DONE.


Total scanned 10459 logs out of 10459 logs in file
Scanned logs dates are from 11-04-2025 00:00:01 to 11-04-2025 19:56:40

======================================
Product log statistics (Per Day):
Days of counting:       0.831007
Product name:   Application Control         Amount of logs:     1               Average:
  1
Product name:   N/A                         Amount of logs:     3               Average:
  3
Product name:   Security Gateway/Management Amount of logs:     20              Average:
  24
Product name:   SmartConsole                Amount of logs:     1               Average:
  1
Product name:   SmartEvent Client           Amount of logs:     2               Average:
  2
Product name:   System Monitor              Amount of logs:     6               Average:
  7
Product name:   VPN-1 & FireWall-1          Amount of logs:     10426           Average:
  12546


Total logs per day:

    Date     |   GB   |   Count

============================================================
[Expert@Mgmt:0]#
```

Example 3 - "CPLogInvestigator -a -p"

```
[Expert@Mgmt:0]# CPLogInvestigator -a -p

Thank you for using log investigator tool.

============================================================
Start reading log file: /opt/CPsuite-R81.20/fw1/log/fw.log

Start reading log file: /opt/CPsuite-R81.20/fw1/log/fw.log from log 0

..
Reading log file is DONE.


Total scanned 10530 logs out of 10530 logs in file
Scanned logs dates are from 11-04-2025 00:00:01 to 11-04-2025 19:57:28

======================================
Product log statistics (Per Day):
Days of counting:       0.831562
Product name:   Application Control         Amount of logs:     1               Average:
  1
Product name:   N/A                         Amount of logs:     3               Average:
  3
Product name:   Security Gateway/Management Amount of logs:     20              Average:
  24
Product name:   SmartConsole                Amount of logs:     1               Average:
  1
Product name:   SmartEvent Client           Amount of logs:     2               Average:
  2
Product name:   System Monitor              Amount of logs:     6               Average:
  7
Product name:   VPN-1 & FireWall-1          Amount of logs:     10497           Average:
  12623


Total logs per day:

    Date     |   GB   |   Count
  2025-01-14 | 0.0000 | 174
... (truncated for brevity) ...
  2025-01-23 | 0.3787 | 11959308
... (truncated for brevity) ...
  2025-04-11 | 0.0007 | 18448
  fw.log | 0.0009 | 21060

============================================================
[Expert@Mgmt:0]#
```

Example 4 - "CPLogInvestigator -m -a -p"

```
[Expert@Mgmt:0]# CPLogInvestigator -m -a -p

Thank you for using log investigator tool.

============================================================
Start reading log file: /opt/CPsuite-R81.20/fw1/log/fw.log

Start reading log file: /opt/CPsuite-R81.20/fw1/log/fw.log from log 0

..
Reading log file is DONE.


Total scanned 15098 logs out of 15098 logs in file
Scanned logs dates are from 11-04-2025 00:00:01 to 11-04-2025 20:59:41

======================================
Product log statistics (Per Day):
Days of counting:       0.874769
Product name:   Application Control         Amount of logs:     1               Average:
  1
Product name:   N/A                         Amount of logs:     3               Average:
  3
Product name:   Security Gateway/Management Amount of logs:     22              Average:
  25
Product name:   SmartConsole                Amount of logs:     1               Average:
  1
Product name:   SmartEvent Client           Amount of logs:     2               Average:
  2
Product name:   System Monitor              Amount of logs:     6               Average:
  6
Product name:   VPN-1 & FireWall-1          Amount of logs:     15063           Average:
  17219


Total logs per day:

    Date     |   GB   |   Count
  2025-04-10 | 0.0007 | 18368
  2025-04-11 | 0.0007 | 18448
  fw.log | 0.0014 | 30196

============================================================
Logs per minute table can be found at logPerMinute.txt

============================================================
[Expert@Mgmt:0]#
[Expert@Mgmt:0]# wc -l logPerMinute.txt
1253 logPerMinute.txt
[Expert@Mgmt:0]#
[Expert@Mgmt:0]# head -n 10 logPerMinute.txt
Rounded log time: 11-04-2025 20:59;     Log count: 48
Rounded log time: 11-04-2025 20:58;     Log count: 73
Rounded log time: 11-04-2025 20:57;     Log count: 70
Rounded log time: 11-04-2025 20:56;     Log count: 76
Rounded log time: 11-04-2025 20:55;     Log count: 70
Rounded log time: 11-04-2025 20:54;     Log count: 74
Rounded log time: 11-04-2025 20:53;     Log count: 76
Rounded log time: 11-04-2025 20:52;     Log count: 78
Rounded log time: 11-04-2025 20:51;     Log count: 70
Rounded log time: 11-04-2025 20:50;     Log count: 76
[Expert@Mgmt:0]#
```

Example 5 - "CPLogInvestigator -l -a -u 1000"

```
[Expert@Mgmt:0]# CPLogInvestigator -l -a -u 1000

Thank you for using log investigator tool.

============================================================
Start reading log file: /opt/CPsuite-R81.20/fw1/log/fw.log

Start reading log file: /opt/CPsuite-R81.20/fw1/log/fw.log from log 0

..
Reading log file is DONE.

Start reading log file: /opt/CPsuite-R81.20/fw1/log/2025-04-11_000000.log

Start reading log file: /opt/CPsuite-R81.20/fw1/log/2025-04-11_000000.log from log 0

..
Reading log file is DONE.

Start reading log file: /opt/CPsuite-R81.20/fw1/log/2025-04-10_000000.log

Start reading log file: /opt/CPsuite-R81.20/fw1/log/2025-04-10_000000.log from log 0

..
Reading log file is DONE.


Total scanned 36245 logs out of 36245 logs in file
Scanned logs dates are from 09-04-2025 00:00:02 to 11-04-2025 21:37:49
Observed blades:
     - Application Control
     - N/A
     - VPN-1 & FireWall-1

========================================

Summary - Estimations based on findings:

Log file size per day: 0.0032GB (12492 logs)

Estimated events per day:
- Estimated events per day based on active blades: 0
- Activated blades + Application Control and URL Filtering for 1000 users: 250000

Storage required per day:
- SmartEvent: 1GB
- Log Server: 0.0032GB
- Log Server + SmartLog: 0.0064GB


============================================================
[Expert@Mgmt:0]#
```

cppkg

Description

Manages the SmartUpdate software packages repository on the Security Management Server.

Important - Installing software packages with the SmartUpdate is not supported for Security Gateways running on Gaia OS.

Syntax

```
cppkg
      add <options>
      {del | delete} <options>
      get
      getroot
      print
      setroot <options>
```

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run `mdsenv`).

Parameters

Parameter	Description
`add <options>`	Adds a SmartUpdate software package to the repository. See *"cppkg add" on page 173*.
`{del | delete} <options>`	Deletes a SmartUpdate software package from the repository. See *"cppkg delete" on page 174*.
`get`	Updates the list of the SmartUpdate software packages in the repository. See *"cppkg get" on page 176*.
`getroot`	Shows the path to the root directory of the repository (the value of the environment variable `$SUROOT`). See *"cppkg getroot" on page 177*.
`print`	Prints the list of SmartUpdate software packages in the repository. See *"cppkg print" on page 178*.
`setroot <options>`	Configures the path to the root directory of the repository. See *"cppkg setroot" on page 179*.

cppkg add

Description

Adds a SmartUpdate software package to the SmartUpdate software packages repository.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).
- This command does not overwrite existing packages. To overwrite an existing package, you must first delete the existing package.
- You get the SmartUpdate software packages from the *Check Point Support Center*.

Syntax

```
cppkg add <Full Path to Package | DVD Drive [Product]>
```

Parameters

Parameter	Description
<Full Path to Package>	Specifies the full local path on the computer to the SmartUpdate software package.
DVD Drive `[Product]`	Specifies the DVD root path. Example: `/mnt/CPR80`

Example - Adding R77.20 HFA_75 (R77.20.75) firmware package for 1100 Appliances

```
[Expert@MGMT:0]# cppkg print
Vendor          Product              Version    OS                  Minor Version
-------------------------------------------------------------------------------
[Expert@MGMT:0]#

[Expert@MGMT:0]# cppkg add /var/log/CP1100_6.0_4_0_-.tgz
Adding package to the repository
Getting the package type...
Extracting the package files...
Copying package to the repository...
Package was successfully added to the repository
[Expert@MGMT:0]#

[Expert@MGMT:0]# cppkg print
Vendor          Product              Version    OS                  Minor Version
-------------------------------------------------------------------------------
Check Point     CP1100               R77.20     Gaia Embedded       R77.20
[Expert@MGMT:0]#
```

cppkg delete

Description

Deletes SmartUpdate software packages from the SmartUpdate software packages repository.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).

Syntax

```
cppkg del ["<Vendor>" "<Product>" "<Major Version>" "<OS>" "<Minor Version>"]
```

```
cppkg delete ["<Vendor>" "<Product>" "<Major Version>" "<OS>" "<Minor Version>"]
```

Parameters

Parameter	Description
`del | delete`	When you do not specify optional parameters, the command runs in the interactive mode. The command shows the menu with applicable options.
"*<Vendor>*"	Specifies the package vendor. Enclose in double quotes.
"*<Product>*"	Specifies the product name. Enclose in double quotes.
"*<Major Version>*"	Specifies the package Major Version. Enclose in double quotes.
"*<OS>*"	Specifies the package OS. Enclose in double quotes.
"*<Minor Version>*"	Specifies the package Minor Version. Enclose in double quotes.

Notes:

- To see the values for the optional parameters, run the *"cppkg print" on page 178* command.
- You must specify all optional parameters, or no parameters.

Example 1 - Interactive mode

```
[Expert@MGMT:0]# cppkg delete

Select package:
--------------------
(0) Delete all
(1) CP1100 Gaia Embedded Check Point R77.20 R77.20

(e) Exit

Enter your choice : 1

You chose to delete 'CP1100 Gaia Embedded Check Point R77.20 R77.20', Is this correct? [y/n] : y

Package was successfully removed from the repository
[Expert@MGMT:0]#
```

Example 2 - Manually deleting the specified package

```
Expert@MGMT:0]# cppkg print
Vendor          Product              Version    OS                  Minor Version
-------------------------------------------------------------------------------
Check Point     CP1100               R77.20     Gaia Embedded       R77.20
[Expert@MGMT:0]#

[Expert@MGMT:0]# cppkg delete "Check Point" "CP1100" "R77.20" "Gaia Embedded" "R77.20"
Package was successfully removed from the repository
[Expert@MGMT:0]#
```

cppkg get

Description

Updates the list of the SmartUpdate software packages in the SmartUpdate software packages repository based on the real content of the repository.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).

Syntax

```
cppkg get
```

Example

```
[Expert@MGMT:0]# cppkg get
Update successfully completed
[Expert@MGMT:0]#
```

cppkg getroot

Description

Shows the path to the root directory of the SmartUpdate software packages repository (the value of the environment variable `$SUROOT`)

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).

Syntax

```
cppkg getroot
```

Example

```
[Expert@MGMT:0]# cppkg getroot
[cppkg 7119 4128339728]@MGMT[29 May 19:16:06] Current repository root is set to :
/var/log/cpupgrade/suroot
[Expert@MGMT:0]#
```

cppkg print

Description

Prints the list of SmartUpdate software packages in the SmartUpdate software packages repository.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).

Syntax

```
cppkg print
```

Example - R77.20 HFA_75 (R77.20.75) firmware package for 1100 Appliances

```
[Expert@MGMT:0]# cppkg print
Vendor          Product              Version    OS                  Minor Version
-------------------------------------------------------------------------------
Check Point     CP1100               R77.20     Gaia Embedded       R77.20
[Expert@MGMT:0]#
```

cppkg setroot

Description

Configures the path to the root directory of the SmartUpdate software packages repository.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).
- The default path is: `/var/log/cpupgrade/suroot`
- When changing repository root directory:
  - This command copies the software packages from the old repository to the new repository. A package in the new location is overwritten by a package from the old location, if the packages have the same name.
  - This command updates the value of the environment variable `$SUROOT` in the Check Point Profile shell scripts (`$CPDIR/tmp/.CPprofile.sh` and `$CPDIR/tmp/.CPprofile.csh`).

Syntax

```
cppkg setroot <Full Path to Repository Root Directory>
```

Example

```
[Expert@MGMT:0]# cppkg setroot /var/log/my_directory

Repository root is set to : /var/log/cpupgrade/suroot

Note : When changing repository root directory :

       1. Old repository content will be copied into the new repository
       2. A package in the new location will be overwritten by a package in the old
          location, if the packages have the same name

Change the current repository root ? [y/n] : y

The new repository directory does not exist. Create it ? [y/n] : y

Repository root was set to : /var/log/my_directory

Notice : To complete the setting of your directory, reboot the machine!
[Expert@MGMT:0]#
```

cpprod_util

Description

This utility works with Check Point Registry (`$CPDIR/registry/HKLM_registry.data`) without manually opening it:

- Shows which Check Point products and features are enabled on this Check Point server.
- Enables and disables Check Point products and features on this Check Point server.

Syntax on a Management Server in Gaia Clish or the Expert mode

`cpprod_util CPPROD_GetValue "<Product>" "<Parameter>" {0|1}`
`cpprod_util CPPROD_SetValue "<Product>" "<Parameter>" {1|4} "<Value>" {0|1}`
`cpprod_util -dump`

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

`cpprod_util CPPROD_GetValue "<Product>" "<Parameter>" {0|1}`
`cpprod_util CPPROD_SetValue "<Product>" "<Parameter>" {1|4} "<Value>" {0|1}`
`cpprod_util -dump`

Syntax on a Scalable Platform Security Group in Gaia gClish

`cpprod_util CPPROD_GetValue "<Product>" "<Parameter>" {0|1}`
`cpprod_util CPPROD_SetValue "<Product>" "<Parameter>" {1|4} "<Value>" {0|1}`
`cpprod_util -dump`

Syntax on a Scalable Platform Security Group in the Expert mode

`g_all cpprod_util CPPROD_GetValue "<Product>" "<Parameter>" {0|1}`
`g_all cpprod_util CPPROD_SetValue "<Product>" "<Parameter>" {1|4} "<Value>" {0|1}`
`g_all cpprod_util -dump`

Parameters

Parameter	Description
`CPPROD_GetValue`	Gets the configuration status of the specified product or feature: ■ 0 - Disabled ■ 1 - Enabled
`CPPROD_SetValue`	Sets the configuration for the specified product or feature. **Important** - Do not run these commands unless explicitly instructed by Check Point Support or R&D to do so.
"<*Product*>"	Specifies the product or feature.
"<*Parameter*>"	Specifies the configuration parameter for the specified product or feature.
"<*Value*>"	Specifies the value of the configuration parameter for the specified product or feature: ■ One of these integers: 0, 1, 4 ■ A string
`dump`	Creates a dump file of the Check Point Registry (`$CPDIR/registry/HKLM_registry.data`) in the current working directory. The name of the output file is `RegDump`.

Notes

- On a Multi-Domain Server, you must run this command in the context of the relevant Domain Management Server.
- If you run the "`cpprod_util`" command without parameters, it prints:
  - The list of all available products and features (for example, "`FwIsFirewallMgmt`", "`FwIsLogServer`", "`FwIsStandAlone`")
  - The type of the expected argument when you configure a product or feature ("`no-parameter`", "`string-parameter`", or "`integer-parameter`")
  - The type of the returned output ("`status-output`", or "`no-output`")
- To redirect the output of the "`cpprod_util`" command, it is necessary to redirect the *stderr* to *stdout*:

  ```
  cpprod_util <options> > <output file> 2>&1
  ```

  Example:

  ```
  cpprod_util > /tmp/output_of_cpprod_util.txt 2>&1
  ```

Examples

Example - Showing a list of all installed Check Point Products Packages on a Management Server

```
[Expert@MGMT:0]# cpprod_util CPPROD_GetInstalledProducts
CPFC
IDA
MGMT
FW1
SecurePlatform
NGXCMP
EdgeCmp
SFWCMP
SFWR75CMP
SFWR77CMP
FLICMP
R75CMP
R7520CMP
R7540CMP
R76CMP
R77CMP
PROVIDER-1
Reporting Module
SmartLog
CPinfo
VSEC
DIAG
[Expert@MGMT:0]#
```

Example - Checking if this Check Point server is configured as a Management Server

```
[Expert@MGMT:0]# cpprod_util FwIsFirewallMgmt
1
[Expert@MGMT:0]#
```

Example - Checking if this Check Point server is configured as a Standalone

```
[Expert@MGMT:0]# cpprod_util FwIsStandAlone
0
[Expert@MGMT:0]#
```

Example - Checking if this Management Server is configured as a Primary in High Availability

```
[Expert@MGMT:0]# cpprod_util FwIsPrimary
1
[Expert@MGMT:0]#
```

Example - Checking if this Management Server is configured as Active in High Availability

```
[Expert@MGMT:0]# cpprod_util FwIsActiveManagement
1
[Expert@MGMT:0]#
```

Example - Checking if this Management Server is configured as Backup in High Availability

```
[Expert@MGMT:0]# cpprod_util FwIsSMCBackup
1
[Expert@MGMT:0]#
```

Example - Checking if this Check Point server is configured as a dedicated Log Server

```
[Expert@MGMT:0]# cpprod_util FwIsLogServer
1
[Expert@MGMT:0]#
```

Example - Checking if on this Management Server the SmartProvisioning blade is enabled

```
[Expert@MGMT:0]# cpprod_util FwIsAtlasManagement
1
[Expert@MGMT:0]#
```

Example - Checking if on this Management Server the SmartEvent Server blade is enabled

```
[Expert@MGMT:0]# cpprod_util RtIsAnalyzerServer
1
[Expert@MGMT:0]#
```

Example - Checking if on this Management Server the SmartEvent Correlation Unit blade is enabled

```
[Expert@MGMT:0]# cpprod_util RtIsAnalyzerCorrelationUnit
1
[Expert@MGMT:0]#
```

Example - Checking if on this Management Server the Endpoint Policy Management blade is enabled

```
[Expert@MGMT:0]# cpprod_util UepmIsInstalled
1
[Expert@MGMT:0]#
```

Example - Checking if this Management Server is configured as Endpoint Policy Server

```
[Expert@MGMT:0]# cpprod_util UepmIsPolicyServer
0
[Expert@MGMT:0]#
```

Example - Showing a list of all installed Check Point Products Packages on a Security Gateway

```
[Expert@MyGW:0]# cpprod_util CPPROD_GetInstalledProducts
CPFC
IDA
MGMT
FW1
SecurePlatform
CPinfo
DIAG
PPACK
CVPN
[Expert@MyGW:0]#
```

Example - Checking if this Security Gateway is configured as a VSX Gateway

```
[Expert@MyGW:0]# cpprod_util FwIsVSX
0
[Expert@MyGW:0]#
```

Example - Checking if on this Security Gateway the QoS blade is enabled

```
[Expert@MyGW:0]# cpprod_util FwIsFloodGate
1
[Expert@MyGW:0]#
```

Example - Checking if on this Security Gateway the SmartProvisioning is enabled

```
[Expert@MyGW:0]# cpprod_util FwIsAtlasModule
0
[Expert@MyGW:0]#
```

Example - Checking if this Security Gateway is configured in Bridge Mode

```
[Expert@MyGW:0]# cpprod_util FwIsBridge
0
[Expert@MyGW:0]#
```

Example - Checking if this Security Gateway is a member of Full HA cluster

```
[Expert@MyGW:0]# cpprod_util FwIsFullHA
0
[Expert@MyGW:0]#
```

Example - Checking if this Security Gateway is configured with Dynamically Assigned IP (DAIP)

```
[Expert@MyGW:0]# cpprod_util FwIsDAG
0
[Expert@MyGW:0]#
```

Example - Checking if this Security Gateway is configured with IPv6 addresses

```
[Expert@MyGW:0]# cpprod_util FwIsFireWallIPv6
1
[Expert@MyGW:0]#
```

cprid

Description

Manages the Check Point Remote Installation Daemon (`cprid`).

This daemon is used for remote upgrade and installation of Check Point products on the managed Security Gateways.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run these commands in the context of the MDS (run `mdsenv`).

Commands

Syntax	Description
`cpridstart`	Starts the Check Point Remote Installation Daemon (`cprid`).
`cpridstop`	Stops the Check Point Remote Installation Daemon (`cprid`).
`run_cprid_restart`	Stops and then starts the Check Point Remote Installation Daemon (`cprid`).

cprinstall

Description

Performs installation of Check Point product packages and associated operations on remote managed Security Gateways.

Important - Installing software packages with this command is not supported for Security Gateways that run on Gaia OS.

Notes:

- This command requires a license for SmartUpdate.
- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- On the remote Security Gateways these are required:
  - SIC Trust must be established between the Security Management Server and the Security Gateway.
  - The `cpd` daemon must run.
  - The `cprid` daemon must run.

Syntax

```
cprinstall
      boot <options>
      cprestart <options>
      cpstart <options>
      cpstop <options>
      delete <options>
      get <options>
      install <options>
      revert <options>
      show <options>
      snapshot <options>
      transfer <options>
      uninstall <options>
      verify <options>
```

Parameters

Parameter	Description
`boot <options>`	Reboots the managed Security Gateway. See *"cprinstall boot" on page 190*.
`cprestart <options>`	Runs the `cprestart` command on the managed Security Gateway. See *"cprinstall cprestart" on page 191*.
`cpstart <options>`	Runs the `cpstart` command on the managed Security Gateway. See *"cprinstall cpstart" on page 192*.
`cpstop <options>`	Runs the `cpstop` command on the managed Security Gateway. See *"cprinstall cpstop" on page 193*.
`delete <options>`	Deletes a snapshot (backup) file on the managed Security Gateway. See *"cprinstall delete" on page 194*.
`get <options>`	■ Gets details of the products and the operating system installed on the managed Security Gateway. ■ Updates the management database on the Security Management Server. See *"cprinstall get" on page 195*.
`install <options>`	Installs Check Point products on the managed Security Gateway. See *"cprinstall install" on page 196*.
`revert <options>`	Restores the managed Security Gateway that runs on SecurePlatform OS from a snapshot saved on that Security Gateway. See *"cprinstall revert" on page 199*.
`show <options>`	Displays all snapshot (backup) files on the managed Security Gateway that runs on SecurePlatform OS. See *"cprinstall show" on page 200*.
`snapshot <options>`	Creates a snapshot on the managed Security Gateway that runs on SecurePlatform OS and saves it on that Security Gateway. See *"cprinstall snapshot" on page 201*.
`transfer <options>`	Transfers a software package from the repository to the managed Security Gateway without installing the package. See *"cprinstall transfer" on page 202*.
`uninstall <options>`	Uninstalls Check Point products on the managed Security Gateway. See *"cprinstall uninstall" on page 204*.

Parameter	Description
`verify <options>`	Confirms these operations were successful: ■ If a specific product can be installed on the managed Security Gateway. ■ That the operating system and currently installed products the managed Security Gateway are appropriate for the software package. ■ That there is enough disk space to install the product the managed Security Gateway. ■ That there is a CPRID connection with the managed Security Gateway. See *"cprinstall verify" on page 206*.

cprinstall boot

Description

Reboots the managed Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall boot <Object Name>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example

```
[Expert@MGMT]# cprinstall boot MyGW
```

cprinstall cprestart

Description

Runs the `cprestart` command on the managed Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- All Check Point products on the managed Security Gateway must be of the same version.

Syntax

```
cprinstall cprestart <Object Name>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example

```
[Expert@MGMT:0]# cprinstall cprestart MyGW
```

cprinstall cpstart

Description

Runs the `cpstart` command on the managed Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- All Check Point products on the managed Security Gateway must be of the same version.

Syntax

```
cprinstall cpstart <Object Name>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example

```
[Expert@MGMT]# cprinstall cpstart MyGW
```

cprinstall cpstop

Description

Runs the `cpstop` command on the managed Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- All Check Point products on the managed Security Gateway must be of the same version.

Syntax

```
cprinstall cpstop {-proc | -nopolicy} <Object Name>
```

Parameters

Parameter	Description
`-proc`	Kills the Check Point daemons and Security Servers, while it maintains the active Security Policy running in the Check Point kernel. Rules with generic *Allow*, *Drop* or *Reject* action based on services, continue to work.
`-nopolicy`	Kills the Check Point daemons and Security Servers and unloads the Security Policy from the Check Point kernel.
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example

```
[Expert@MGMT]# cprinstall cpstop -proc MyGW
```

cprinstall delete

Description

Deletes a snapshot (backup) file on the managed Security Gateway that runs on SecurePlatform OS.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall delete <Object Name> <Snapshot File>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
<Snapshot File>	Specifies the name of the snapshot (backup) on SecurePlatform OS.

Example

```
[Expert@MGMT]# cprinstall delete MyGW Snapshot25Apr2017
```

cprinstall get

Description

- Gets details of the products and the operating system installed on the managed Security Gateway.
- Updates the management database on the Security Management Server.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall get <Object Name>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example:

```
[Expert@MGMT]# cprinstall get MyGW
Checking cprid connection...
Verified
Operation completed successfully
Updating machine information...
Update successfully completed
'Get Gateway Data' completed successfully
Operating system   Major Version      Minor Version
-------------------------------------------------------------------
SecurePlatform     R75.20             R75.20

Vendor             Product            Major Version       Minor Version
-------------------------------------------------------------------
Check Point        VPN-1 Power/UTM    R75.20              R75.20
Check Point        SecurePlatform     R75.20              R75.20
Check Point        SmartPortal        R75.20              R75.20
[Expert@MGMT]#
```

cprinstall install

Description

Installs Check Point products on the managed Security Gateway.

Important - Installing software packages with this command is not supported for Security Gateways that run Gaia OS.

Notes:

- Before transferring the software package, this command runs the *"cprinstall verify" on page 206* command.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- To see the values for the package attributes, run the *"cppkg print" on page 178* command.

Syntax

```
cprinstall install [-boot] [-backup] [-skip_transfer] <Object
Name> "<Vendor>" "<Product>" "<Major Version>" "<Minor Version>"
```

Parameters

Parameter	Description
`-boot`	Reboots the managed Security Gateway after installing the package. **Note** - Only reboot after ALL products have the same version. Reboot is canceled in certain scenarios.
`-backup`	Creates a snapshot on the managed Security Gateway before installing the package. **Note** - Only on Security Gateways that runs on SecurePlatform OS.
`-skip_ transfer`	Skip the transfer of the package.
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
"*<Vendor>*"	Specifies the package vendor. Enclose in double quotes. Example: ■ `checkpoint` ■ `Check Point`
"*<Product>*"	Specifies the product name. Enclose in double quotes. Examples: ■ `SVNfoundation` ■ `firewall` ■ `floodgate` ■ `CP1100` ■ `VPN-1 Power/UTM` ■ `SmartPortal`
"*<Major Version>*"	Specifies the package Major Version. Enclose in double quotes.
"*<Minor Version>*"	Specifies the package Minor Version. Enclose in double quotes.

Example

```
[Expert@MGMT]# cprinstall install -boot MyGW "checkpoint" "firewall" "R75" "R75.20"

Installing firewall R75.20 on MyGW...
Info : Testing Check Point Gateway
Info : Test completed successfully.
Info : Transferring Package to Check Point Gateway
Info : Extracting package on Check Point Gateway
Info : Installing package on Check Point Gateway
Info : Product was successfully applied.
Info : Rebooting the Check Point Gateway
Info : Checking boot status
Info : Reboot completed successfully.
Info : Checking Check Point Gateway
Info : Operation completed successfully.
[Expert@MGMT]#
```

cprinstall revert

Description

Restores the managed Security Gateway that runs on SecurePlatform OS from a snapshot saved on that Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall revert <Object Name> <Snapshot File>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
<Snapshot File>	Name of the SecurePlatform snapshot file. To see the names of the saved snapshot files, run the *"cprinstall show" on page 200* command.

cprinstall show

Description

Displays all snapshot (backup) files on the managed Security Gateway that runs on SecurePlatform OS.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall show <Object Name>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example

```
[Expert@MGMT]# cprinstall show GW1
SU_backup.tzg
[Expert@MGMT]#
```

cprinstall snapshot

Description

Creates a snapshot on the managed Security Gateway that runs on SecurePlatform OS and saves it on that Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall snapshot <Object Name> <Snapshot File>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
<Snapshot File>	Name of the SecurePlatform snapshot file. To see the names of the saved snapshot files, run the *"cprinstall show" on page 200* command.

cprinstall transfer

Description

Transfers a software package from the repository to the managed Security Gateway without installing the package.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- To see the values for the package attributes, run the *"cppkg print" on page 178* command.

Syntax

```
cprinstall transfer <Object Name> "<Vendor>" "<Product>" "<Major Version>" "<Minor Version>"
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
"*<Vendor>*"	Specifies the package vendor. Enclose in double quotes. Example: ■ `checkpoint` ■ `Check Point`
"*<Product>*"	Specifies the product name. Enclose in double quotes. Examples: ■ `SVNfoundation` ■ `firewall` ■ `floodgate` ■ `CP1100`
"*<Major Version>*"	Specifies the package major version. Enclose in double quotes.
"*<Minor Version>*"	Specifies the package minor version. Enclose in double quotes.

cprinstall uninstall

Description

Uninstalls Check Point products on the managed Security Gateway.

Important - Uninstalling software packages with this command is not supported for Security Gateways running on Gaia OS.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- Before uninstalling product packages, this command runs the *"cprinstall verify" on page 206* command.
- After uninstalling a product package, you must run the *"cprinstall get" on page 195* command.
- To see the values for the package attributes, run the *"cppkg print" on page 178* command.

Syntax

```
cprinstall uninstall [-boot] <Object Name> "<Vendor>" "<Product>"
"<Major Version>" "<Minor Version>"
```

Parameters

Parameter	Description
`-boot`	Reboots the managed Security Gateway after uninstalling the package. **Note** - Reboot is canceled in certain scenarios.
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
"*<Vendor>*"	Specifies the package vendor. Enclose in double quotes. Example: ■ `checkpoint` ■ `Check Point`
"*<Product>*"	Specifies the product name. Enclose in double quotes. Examples: ■ `SVNfoundation` ■ `firewall` ■ `floodgate` ■ `CP1100`
"*<Major Version>*"	Specifies the package major version. Enclose in double quotes.
"*<Minor Version>*"	Specifies the package minor version. Enclose in double quotes.

Example

```
[Expert@MGMT]# cprinstall uninstall MyGW "checkpoint" "firewall" "R75.20" "R75.20"
Uninstalling firewall R75.20 from MyGW...
Info : Removing package from Check Point Gateway
Info : Product was successfully applied.
Operation Success. Please get network object data to complete the operation.
[Expert@MGMT]#
[Expert@MGMT]# cprinstall get
```

cprinstall verify

Description

Confirms these operations were successful:

- If a specific product can be installed on the managed Security Gateway.
- That the operating system and currently installed products the managed Security Gateway are appropriate for the software package.
- That there is enough disk space to install the product the managed Security Gateway.
- That there is a CPRID connection with the managed Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```
- To see the values for the package attributes, run the *"cppkg print" on page 178* command.

Syntax

```
cprinstall verify <Object Name> "<Vendor>" "<Product>" "<Major
Version>" ["<Minor Version>"]
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
"*<Vendor>*"	Specifies the package vendor. Enclose in double quotes. Example: ■ `checkpoint` ■ `Check Point`
"*<Product>*"	Specifies the product name. Enclose in double quotes. Examples: ■ `SVNfoundation` ■ `firewall` ■ `floodgate` ■ `CP1100` ■ `VPN-1 Power/UTM` ■ `SmartPortal`
"*<Major Version>*"	Specifies the package major version. Enclose in double quotes.
"*<Minor Version>*"	Specifies the package minor version. Enclose in double quotes. This parameter is optional.

Example 1 - Verification succeeds

```
[Expert@MGMT]# cprinstall verify MyGW "checkpoint" "SVNfoundation" "R75.20"
Verifying installation of SVNfoundation R75.20 on MyGW...
Info : Testing Check Point Gateway.
Info : Test completed successfully.
Info : Installation Verified, The product can be installed.
```

Example 2 - Verification fails

```
[Expert@MGMT]# cprinstall verify MyGW "checkpoint" "SVNfoundation" "R75.20"
Verifying installation of SVNfoundation R75.20 on MyGW...
Info : Testing Check Point Gateway
Info : SVN Foundation R75 is already installed on 192.0.2.134
Operation Success. Product cannot be installed, did not pass dependency check.
```

cpstart

Description

Manually starts all Check Point processes and applications.

Notes:

- For the `cprid` daemon, use the *"cprid" on page 186* command.
- For manually starting specific Check Point processes, see sk97638.

Syntax

```
cpstart
```

cpstat

Description

Shows the status and statistics information for Check Point applications.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpstat [-d] [-h <Host>] [-p <Port>] [-s <SICname>] [-f <Flavor>]
[-o <Polling Interval> [-c <Count>] [-e <Period>]] <Application
Flag>
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpstat [-d] [-h <Host>] [-p <Port>] [-s <SICname>] [-f <Flavor>]
[-o <Polling Interval> [-c <Count>] [-e <Period>]] <Application
Flag>
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpstat [-d] [-h <Host>] [-p <Port>] [-s <SICname>] [-f <Flavor>]
[-o <Polling Interval> [-c <Count>] [-e <Period>]] <Application
Flag>
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpstat [-d] [-h <Host>] [-p <Port>] [-s <SICname>] [-f
<Flavor>] [-o <Polling Interval> [-c <Count>] [-e <Period>]]
<Application Flag>
```

Note - You can write the parameters in the syntax in any order.

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. The output shows the SNMP queries and SNMP responses for the applicable SNMP OIDs.
`-h <Host>`	Optional. When you run this command on a Management Server, this parameter specifies the managed Security Gateway / ClusterXL object. *<Host>* is an IPv4 address, a resolvable hostname, or a DAIP object name. The default is `localhost`. **Note** - On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:`mdsenv <IP Address or Name of Domain Management Server>`.
`-p <Port>`	Optional. Port number of the Application Monitoring (AMON) server. The default port is 18192.
`-s <SICname>`	Optional. Secure Internal Communication (SIC) name of the Application Monitoring (AMON) server.
`-f <Flavor>`	Optional. Specifies the type of the information to collect. If you do not specify a flavor explicitly, the command uses the first flavor in the *<Application Flag>*. To see all flavors, run the `cpstat` command without any parameters.

Parameter	Description
`-o <Polling Interval>`	Optional. Specifies the polling interval (in seconds) - how frequently the command collects and shows the information. Examples: ■ 0 - The command shows the results only once and the stops (this is the default value). ■ 5 - The command shows the results every 5 seconds in the loop. ■ 30 - The command shows the results every 30 seconds in the loop. ■ N - The command shows the results every N seconds in the loop. Use this parameter together with the "`-c <Count>`" parameter and the "`-e <Period>`" parameter. Example: `cpstat os -f perf -o 2`
`-c <Count>`	Optional. Specifies how many times the command runs and shows the results before it stops. You must use this parameter together with the "`-o <Polling Interval>`" parameter. Examples: ■ 0 - The command shows the results repeatedly every <*Polling Interval*> (this is the default value). ■ 10 - The command shows the results 10 times every <*Polling Interval*> and then stops. ■ 20 - The command shows the results 20 times every <*Polling Interval*> and then stops. ■ N - The command shows the results N times every <*Polling Interval*> and then stops. Example: `cpstat os -f perf -o 2 -c 2`

Parameter	Description
`-e <Period>`	Optional. Specifies the time (in seconds), over which the command calculates the statistics. You must use this parameter together with the "`-o <Polling Interval>`" parameter. You can use this parameter together with the "`-c <Count>`" parameter. Example: `cpstat os -f perf -o 2 -c 2 -e 60`
`<Application Flag>`	Mandatory. See the table below with flavors for the application flags.

These flavors are available for the application flags

Note - The available flags depend on the enabled Software Blades. Some flags are supported only by a Security Gateway / ClusterXL, and some flags are supported only by a Management Server.

Feature or Software Blade	Flag	Flavors
List of enabled Software Blades	`blades`	`fw, ips, av, urlf, vpn, cvpn, aspm, dlp, appi, anti_bot, default, content_awareness, threat-emulation, default`
Operating System	`os`	`default, ifconfig, routing, routing6, memory, old_memory, cpu, disk, perf, multi_cpu, multi_disk, raidInfo, sensors, power_supply, hw_info, all, average_cpu, average_memory, statistics, updates, licensing, connectivity, vsx`
Firewall	`fw`	`default, interfaces, policy, perf, hmem, kmem, inspect, cookies, chains, fragments, totals, totals64, ufp, http, ftp, telnet, rlogin, smtp, pop3, sync, log_connection, all`

Feature or Software Blade	Flag	Flavors
HTTPS Inspection	`https_inspection`	`default, hsm_status, all`
Identity Awareness	`identityServer`	`default, authentication, logins, ldap, components, adquery, idc, muh`
Application Control	`appi`	`default, subscription_status, update_status, RAD_status, top_last_hour, top_last_day, top_last_week, top_last_month`
URL Filtering	`urlf`	`default, subscription_status, update_status, RAD_status, top_last_hour, top_last_day, top_last_week, top_last_month`
IPS	`ips`	`default, statistics, all`
Anti-Virus	`ci`	`default`
Threat Prevention	`antimalware`	`default, scanned_hosts, scanned_mails, subscription_status, update_status, ab_prm_contracts, av_prm_contracts, ab_prm_contracts, av_prm_contracts`

Feature or Software Blade	Flag	Flavors
Threat Emulation	`threat-emulation`	`default, general_statuses, update_status, scanned_files, malware_detected, scanned_on_cloud, malware_on_cloud, average_process_time, emulated_file_size, queue_size, peak_size, file_type_stat_file_scanned, file_type_stat_malware_detected, file_type_stat_cloud_scanned, file_type_stat_cloud_malware_scanned, file_type_stat_filter_by_analysis, file_type_stat_cache_hit_rate, file_type_stat_error_count, file_type_stat_no_resource_count, contract, downloads_information_current, downloading_file_information, queue_table, history_te_incidents, history_te_comp_hosts`
Threat Extraction	`scrub`	`default, subscription_status, threat_extraction_statistics`
Mobile Access	`cvpn`	`cvpnd, sysinfo, products, overall`
VSX	`vsx`	`default, stat, traffic, conns, cpu, all, memory, cpu_usage_per_core`
IPSec VPN	`vpn`	`default, product, IKE, ipsec, traffic, compression, accelerator, nic, statistics, watermarks, all`
Data Loss Prevention	`dlp`	`default, dlp, exchange_agents, fingerprint`
Content Awareness	`ctnt`	`default`
QoS	`fg`	`all`
High Availability	`ha`	`default, all`
Policy Server for Remote Access VPN clients	`polsrv`	`default, all`

Feature or Software Blade	Flag	Flavors
Desktop Policy Server for Remote Access VPN clients	`dtps`	`default, all`
LTE / GX	`gx`	`default, contxt_create_info, contxt_delete_info, contxt_update_info, contxt_path_mng_info, GXSA_GPDU_info, contxt_initiate_info, gtpv2_create_info, gtpv2_delete_info, gtpv2_update_info, gtpv2_path_mng_info, gtpv2_cmd_info, all`
Management Server	`mg`	`default, log_server, indexer`
Certificate Authority	`ca`	`default, crl, cert, user, all`
SmartEvent	`cpsemd`	`default`
SmartEvent Correlation Unit	`cpsead`	`default`
Log Server	`ls`	`default`
CloudGuard Controller	`vsec`	`default`
SmartReporter	`svr`	`default`
Provisioning Agent	`PA`	`default`
Thresholds configured with the "`threshold_config`" command	`thresholds`	`default, active_thresholds, destinations, error`
Historical status values	`persistency`	`product, TableConfig, SourceConfig`

Examples

Example - Interfaces on a Security Gateway

```
[Expert@MyGW:0]# cpstat -f interfaces fw

Network interfaces
-------------------------------------------------------------------------------------------------
-----------------------
|Name|IP           |Netmask      |Flags|Peer name|Remote IP|Topology|Proxy
name|Slaves|Ports|IPv6 Address|IPv6 Len|
-------------------------------------------------------------------------------------------------
-----------------------
|eth0|192.168.30.40|255.255.255.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
|eth1| 172.30.60.80|255.255.255.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
|eth2|      0.0.0.0|      0.0.0.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
|eth3|      0.0.0.0|      0.0.0.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
|eth4|      0.0.0.0|      0.0.0.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
|eth5|      0.0.0.0|      0.0.0.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
|eth6|      0.0.0.0|      0.0.0.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
|eth7|      0.0.0.0|      0.0.0.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
-------------------------------------------------------------------------------------------------
-----------------------

[Expert@MyGW:0]#
```

Example - Policy on a Security Gateway

```
[Expert@MyGW:0]# cpstat -f default fw

Policy name:  MyGW_Policy
Install time: Wed May 23 18:14:32 2018


Interface table
----------------------------------------
|Name|Dir|Total   |Accept|Deny    |Log|
----------------------------------------
|eth0|in | 2393126| 32589| 2360537| 52|
|eth0|out|   33016| 33016|       0|  0|
|eth1|in | 2360350|     0| 2360350|  0|
|eth1|out|       0|     0|       0|  0|
|eth2|in | 2360350|     0| 2360350|  0|
|eth2|out|       0|     0|       0|  0|
|eth3|in | 2348704|     0| 2348704|  1|
|eth3|out|       0|     0|       0|  0|
|eth4|in | 2360350|     0| 2360350|  0|
|eth4|out|       0|     0|       0|  0|
----------------------------------------
|    |   |11855896| 65605|11790291| 53|
----------------------------------------

... ... [truncated for brevity] ... ...

[Expert@MyGW:0]#
```

Example - CPU utilization

```
[Expert@HostName:0]# cpstat -f cpu os
CPU User Time (%):   1
CPU System Time (%): 0
CPU Idle Time (%):   99
CPU Usage (%):       1
CPU Queue Length:    -
CPU Interrupts/Sec:  172
CPUs Number:         8

[Expert@HostName:0]#
```

Example - Performance

```
[Expert@HostName:0]# cpstat os -f perf -o 2 -c 2 -e 60

Total Virtual Memory (Bytes):            12417720320
Active Virtual Memory (Bytes):           3741331456
Total Real Memory (Bytes):               8231063552
Active Real Memory (Bytes):              3741331456
Free Real Memory (Bytes):                4489732096
Memory Swaps/Sec:                        -
Memory To Disk Transfers/Sec:            -
CPU User Time (%):                       0
CPU System Time (%):                     0
CPU Idle Time (%):                       100
CPU Usage (%):                           0
CPU Queue Length:                        -
CPU Interrupts/Sec:                      135
CPUs Number:                             8
Disk Servicing Read\Write Requests Time: -
Disk Requests Queue:                     -
Disk Free Space (%):                     61
Disk Total Free Space (Bytes):           12659716096
Disk Available Free Space (Bytes):       11606188032
Disk Total Space (Bytes):                20477751296


Total Virtual Memory (Bytes):            12417720320
Active Virtual Memory (Bytes):           3741556736
Total Real Memory (Bytes):               8231063552
Active Real Memory (Bytes):              3741556736
Free Real Memory (Bytes):                4489506816
Memory Swaps/Sec:                        -
Memory To Disk Transfers/Sec:            -
CPU User Time (%):                       3
CPU System Time (%):                     0
CPU Idle Time (%):                       97
CPU Usage (%):                           3
CPU Queue Length:                        -
CPU Interrupts/Sec:                      140
CPUs Number:                             8
Disk Servicing Read\Write Requests Time: -
Disk Requests Queue:                     -
Disk Free Space (%):                     61
Disk Total Free Space (Bytes):           12659716096
Disk Available Free Space (Bytes):       11606188032
Disk Total Space (Bytes):                20477751296

[Expert@HostName:0]#
```

Example - List of current connected sessions on a Management Server

```
[Expert@MGMT:0]# cpstat -f default mg

Product Name:  Check Point Security Management Server
Major version: 6
Minor version: 0
Build number:  994000031
Is started:    1
Active status: active
Status:        OK

Connected clients
-----------------------------------------------------
|Client type |Administrator|Host        |Database lock|
-----------------------------------------------------
|SmartConsole|admin        |JOHNDOE-PC  |false        |
-----------------------------------------------------

[Expert@MGMT:0]#
```

cpstop

Description

Manually stops all Check Point processes and applications.

Notes:

- For the `cprid` daemon, use the *"cprid" on page 186* command.
- For manually stopping specific Check Point processes, see sk97638.

Syntax

```
cpstop
```

cpwd_admin

Description

The Check Point WatchDog (`cpwd`) is a process that invokes and monitors critical processes such as Check Point daemons on the local server, and attempts to restart them if they fail.

Among the processes monitored by Watchdog are `fwm`, `fwd`, `cpd`, `DAService`, and others.

The list of monitored processes depends on the installed and configured Check Point products and Software Blades.

The Check Point WatchDog writes monitoring information to the `$CPDIR/log/cpwd.elg` log file.

The `cpwd_admin` utility shows the status of the monitored processes, and configures the Check Point WatchDog.

There are two types of Check Point WatchDog monitoring

Monitoring	Description
Passive	WatchDog restarts the process only when the process terminates abnormally. In the output of the `cpwd_admin list` command, the `MON` column shows `N` for passively monitored processes.
Active	WatchDog checks the process status every predefined interval. WatchDog makes sure the process is alive, as well as properly functioning (not stuck on deadlocks, frozen, and so on). In the output of the `cpwd_admin list` command, the `MON` column shows `Y` for actively monitored processes. The list of actively monitored processes is predefined by Check Point. Users cannot change or configure it.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin
      config <options>
      del <options>
      detach <options>
      exist
      flist <options>
      getpid <options>
      kill
      list <options>
      monitor_list
      start <options>
      start_monitor
      stop <options>
      stop_monitor
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin
      config <options>
      del <options>
      detach <options>
      exist
      flist <options>
      getpid <options>
      kill
      list <options>
      monitor_list
      start <options>
      start_monitor
      stop <options>
      stop_monitor
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin
      config <options>
      del <options>
      detach <options>
      exist
      flist <options>
      getpid <options>
      kill
      list <options>
      monitor_list
      start <options>
      start_monitor
      stop <options>
      stop_monitor
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin
      config <options>
      del <options>
      detach <options>
      exist
      flist <options>
      getpid <options>
      kill
      list <options>
      monitor_list
      start <options>
      start_monitor
      stop <options>
      stop_monitor
```

Parameters

Parameter	Description
`config <options>`	Configures the Check Point WatchDog. See *"cpwd_admin config" on page 224*.

Parameter	Description
`del <options>`	Temporarily deletes a monitored process from the WatchDog database of monitored processes. See *"cpwd_admin del" on page 229*.
`detach <options>`	Temporarily detaches a monitored process from the WatchDog monitoring. See *"cpwd_admin detach" on page 231*.
`exist`	Checks whether the WatchDog process `cpwd` is alive. See *"cpwd_admin exist" on page 233*.
`flist <options>`	Saves the status of all monitored processes to a `$CPDIR/tmp/cpwd_list_<Epoch Timestamp>.lst` file. See *"cpwd_admin flist" on page 234*.
`getpid <options>`	Shows the PID of a monitored process. See *"cpwd_admin getpid" on page 236*.
`kill <options>`	Terminates the WatchDog process `cpwd`. See *"cpwd_admin kill" on page 237*. **Important** - Do **not** run this command unless explicitly instructed by Check Point Support or R&D to do so.
`list`	Prints the status of all monitored processes on the screen. See *"cpwd_admin list" on page 238*.
`monitor_list`	Prints the status of actively monitored processes on the screen. See *"cpwd_admin monitor_list" on page 243*.
`start <options>`	Starts a process as monitored by the WatchDog. See *"cpwd_admin start" on page 244*.
`start_monitor`	Starts the active WatchDog monitoring - WatchDog monitors the predefined processes actively. See *"cpwd_admin start_monitor" on page 247*.
`stop <options>`	Stops a monitored process. See *"cpwd_admin stop" on page 248*.
`stop_monitor`	Stops the active WatchDog monitoring - WatchDog monitors all processes only passively. See *"cpwd_admin stop_monitor" on page 250*.

cpwd_admin config

Description

Configures the Check Point WatchDog.

Important - After changing the WatchDog configuration parameters, you must restart the WatchDog process with the "`cpstop`" and "`cpstart`" commands (which restart *all* Check Point processes).

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin config
      -h
      -a <options>
      -d <options
      -p
      -r
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin config
      -h
      -a <options>
      -d <options
      -p
      -r
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin config
      -h
      -a <options>
      -d <options
      -p
      -r
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin config
      -h
      -a <options>
      -d <options
      -p
      -r
```

Parameters

Parameter	Description
`-h`	Shows built-in usage.
`-a <Configuration_Parameter_1>=<Value_1> <Configuration_Parameter_2>=<Value_2> ... <Configuration_Parameter_N>=<Value_N>`	Adds the WatchDog configuration parameters. **Note** - Spaces are not allowed between the name of the configuration parameter, the equal sign, and the value.
`-d <Configuration_Parameter_1> <Configuration_Parameter_2> ... <Configuration_Parameter_N>`	Deletes the WatchDog configuration parameters that user added with the "`cpwd_admin config -a`" command.
`-p`	Shows the WatchDog configuration parameters that user added with the "`cpwd_admin config -a`" command.
`-r`	Restores the default WatchDog configuration.

These are the available configuration parameters and the accepted values:

Configuration Parameter	Accepted Values	Description
`default_ctx`	Text string up to 128 characters	On a VSX Gateway, configures the CTX value that is assigned to monitored processes, for which no CTX is specified.
`display_ctx`	■ 0 (default) ■ 1	On a VSX Gateway, configures whether the WatchDog shows the `CTX` column in the output of the `cpwd_admin list` command (between the `APP` and the `PID` columns): ■ 0 - Does not show the `CTX` column ■ 1 - Shows the `CTX` column

Configuration Parameter	Accepted Values	Description
`no_limit`	■ Range: -1, 0, >0 ■ Default: 5	If `rerun_mode=1`, specifies the maximal number of times the WatchDog tries to restart a process. ■ -1 - Always tries to restart ■ 0 - Never tries to restart ■ >0 - Tries this number of times
`num_of_procs`	■ Range: 30 - 3000 ■ Default: 3000	Configures the maximal number of processes managed by the WatchDog.
`rerun_mode`	■ 0 ■ 1 (default)	Configures whether the WatchDog restarts processes after they fail: ■ 0 - Does not restart a failed process. Monitor and log only. ■ 1 - Restarts a failed process (this is the default).
`reset_ startups`	■ Range: > 0 ■ Default: 3600	Configures the time (in seconds) the WatchDog waits after the process starts and before the WatchDog resets the process's `startup_counter` to 0. To see the process's startup counter, in the output of the `cpwd_admin list` command, refer to the `#START` column.
`sleep_mode`	■ 0 ■ 1 (default)	Configures how the WatchDog restarts the process: ■ 0 - Ignores timeout and restarts the process immediately ■ 1 - Waits for the duration of `sleep_timeout`
`sleep_ timeout`	■ Range: 0 - 3600 ■ Default: 60	If `rerun_mode=1`, specifies how much time (in seconds) passes from a process failure until WatchDog tries to restart it.
`stop_timeout`	■ Range: > 0 ■ Default: 60	Configures the time (in seconds) the WatchDog waits for a process stop command to complete.

Configuration Parameter	Accepted Values	Description
`zero_timeout`	■ Range: > 0 ■ Default: 7200	After failing `no_limit` times to restart a process, the WatchDog waits `zero_timeout` seconds before it tries again. The value of the `zero_timeout` must be greater than the value of the `timeout`.

The WatchDog saves the user defined configuration parameters in the `$CPDIR/registry/HKLM_registry.data` file in the "`: (Wd_Config`" section:

```
("CheckPoint Repository Set"
  : (SOFTWARE
    : (CheckPoint
      : (CPshared
        :CurrentVersion (6.0)
        : (6.0
        ... ...
          : (reserved
          ... ...
            : (Wd
                : (Wd_Config
                    :Configuration_Parameter_1 ("[4]Value_1")
                    :Configuration_Parameter_2 ("[4]Value_2")
                )
            )
          ... ...
```

Example

```
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -a sleep_timeout=120 no_limit=12
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog Configuration parameters are:
sleep_timeout : 120
no_limit : 12
[Expert@HostName:0]#
[Expert@HostName:0]# cpstop ; cpstart
[Expert@HostName:0]#

[Expert@HostName:0]# cpwd_admin config -r
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
[Expert@HostName:0]# cpstop ; cpstart
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
```

cpwd_admin del

Description

Temporarily deletes a monitored process from the WatchDog database of monitored processes.

Notes:

- WatchDog stops monitoring the detached process, but the process stays alive.
- The *"cpwd_admin list" on page 238* command does not show the deleted process anymore.
- This change applies until all Check Point services restart during boot, or with the *"cpstart" on page 208* command.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin del -name <Application Name>
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin del -name <Application Name> [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin del -name <Application Name> [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin del -name <Application Name> [-ctx <VSID>]
```

Parameters

Parameter	Description
<Application Name>	Name of the monitored Check Point process as you see in the output of the *"cpwd_admin list" on page 238* command in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`
`-ctx <VSID>`	On a VSX Gateway, specifies the context of the applicable Virtual System.

Example

```
[Expert@HostName:0]# cpwd_admin del -name FWD
cpwd_admin:
successful Del operation
[Expert@HostName:0]#
```

cpwd_admin detach

Description

Temporarily detaches a monitored process from the WatchDog monitoring.

Notes:

- WatchDog stops monitoring the detached process, but the process stays alive.
- The *"cpwd_admin list" on page 238* command does not show the detached process anymore.
- This change applies until all Check Point services restart during boot, or with the *"cpstart" on page 208* command.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin detach -name <Application Name>
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin detach -name <Application Name> [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin detach -name <Application Name> [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin detach -name <Application Name> [-ctx <VSID>]
```

Parameters

Parameter	Description
<Application Name>	Name of the monitored Check Point process as you see in the output of the *"cpwd_admin list" on page 238* command in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`
`-ctx <VSID>`	On a VSX Gateway, specifies the context of the applicable Virtual System.

Example

```
[Expert@HostName:0]# cpwd_admin detach -name FWD
cpwd_admin:
successful Detach operation
[Expert@HostName:0]#
```

cpwd_admin exist

Description

Checks whether the WatchDog process `cpwd` is alive.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin exist
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin exist
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin exist
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin exist
```

Example

```
[Expert@HostName:0]# cpwd_admin exist
 cpwd_admin: cpWatchDog is running
[Expert@HostName:0]#
```

cpwd_admin flist

Description

Saves the status of all WatchDog monitored processes to a file.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin flist [-full]
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin flist [-full] [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin flist [-full] [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin flist [-full] [-ctx <VSID>]
```

Parameters

Parameter	Description
`-full`	Shows the verbose output.
`-ctx <VSID>`	On a VSX Gateway, specifies the context of the applicable Virtual System.

Output

Column	Description
APP	Shows the WatchDog name of the monitored process.
CTX	On a VSX Gateway, shows the VSID, in which the monitored process runs.
PID	Shows the PID of the monitored process.
STAT	Shows the status of the monitored process: ■ E - executing ■ T - terminated
#START	Shows how many times the WatchDog started the monitored process.
START_TIME	Shows the time when the WatchDog started the monitored process for the last time.
SLP/LIMIT	In verbose output, shows the values of the sleep_timeout and no_limit configuration parameters (see *"cpwd_admin config" on page 224*).
MON	Shows how the WatchDog monitors this process (see the explanation for the *"cpwd_admin" on page 220*): ■ Y - Active monitoring ■ N - Passive monitoring
COMMAND	Shows the command the WatchDog run to start this process.

Example

```
[Expert@HostName:0]# cpwd_admin flist
/opt/CPshrd-R81.20/tmp/cpwd_list_1564617600.lst
[Expert@HostName:0]#
```

cpwd_admin getpid

Description

Shows the PID of a WatchDog monitored process.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin getpid -name <Application Name>
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin getpid -name <Application Name> [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin getpid -name <Application Name> [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin getpid -name <Application Name> [-ctx <VSID>]
```

Parameters

Parameter	Description
<Application Name>	Name of the monitored Check Point process as you see in the output of the *"cpwd_admin list" on page 238* command in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`
`-ctx <VSID>`	On VSX Gateway, specifies the context of the applicable Virtual System.

Example

```
[Expert@HostName:0]# cpwd_admin getpid -name FWD
5640
[Expert@HostName:0]#
```

cpwd_admin kill

Description

Terminates the WatchDog process `cpwd`.

Important - Do **not** run this command unless explicitly instructed by Check Point Support or R&D to do so.
To restart the WatchDog process, you must restart all Check Point services with the *"cpstop" on page 219* and *"cpstart" on page 208* commands.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin kill
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin kill
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin kill
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin kill
```

cpwd_admin list

Description

Prints the status of all WatchDog monitored processes on the screen.

Note - By default, WatchDog monitors a maximum of 3000 processes.
To increase this threshold, use the command "`cpwd_admin config -a num_of_procs=<value>`".
See *"cpwd_admin config" on page 224*.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin list [-full]
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin list [-full] [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin list [-full] [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin list [-full] [-ctx <VSID>]
```

Parameters

Parameter	Description
`-full`	Shows the verbose output.
`-ctx <VSID>`	On a VSX Gateway, specifies the context of the applicable Virtual System.

Output

Column	Description
APP	Shows the WatchDog name of the monitored process.
CTX	On a VSX Gateway, shows the VSID, in which the monitored process runs.
PID	Shows the PID of the monitored process.
STAT	Shows the status of the monitored process: ■ E - executing ■ T - terminated
#START	Shows how many times the WatchDog started the monitored process.
START_TIME	Shows the time when the WatchDog started the monitored process for the last time.
SLP/LIMIT	In verbose output, shows the values of the sleep_timeout and no_limit configuration parameters (see *"cpwd_admin config" on page 224*).
MON	Shows how the WatchDog monitors this process (see the explanation for the *"cpwd_admin" on page 220*): ■ Y - Active monitoring ■ N - Passive monitoring
COMMAND	Shows the command the WatchDog run to start this process.

Examples

Example - Default output on a Management Server

```
[Expert@HostName:0]# cpwd_admin list
APP          PID    STAT  #START  START_TIME             MON  COMMAND
CPVIEWD      19738  E     1       [17:50:44] 31/5/2019   N    cpviewd
HISTORYD     0      T     0       [17:54:44] 31/5/2019   N    cpview_historyd
CPD          19730  E     1       [17:54:45] 31/5/2019   Y    cpd
SOLR         19935  E     1       [17:50:55] 31/5/2019   N    java_solr /opt/CPrt-
R81.20/conf/jetty.xml
RFL          19951  E     1       [17:50:55] 31/5/2019   N    LogCore
SMARTVIEW    19979  E     1       [17:50:55] 31/5/2019   N    SmartView
INDEXER      20032  E     1       [17:50:55] 31/5/2019   N    /opt/CPrt-R81.20/log_indexer/log_
indexer
SMARTLOG_SERVER 20100  E     1       [17:50:55] 31/5/2019   N    /opt/CPSmartLog-
R81.20/smartlog_server
CP3DLOGD     20237  E     1       [17:50:55] 31/5/2019   N    cp3dlogd
EPM          20251  E     1       [17:50:56] 31/5/2019   N    startEngine
DASERVICE    20404  E     1       [17:50:59] 31/5/2019   N    DAService_script
[Expert@HostName:0]#
```

Example - Default output on a Security Gateway

```
[Expert@HostName:0]# cpwd_admin list
APP         CTX         PID    STAT  #START  START_TIME             MON  COMMAND
FWK_FORKER  0           4180   E     1       [18:14:04] 23/5/2019   N    fwk_forker
FWK_WD      0           4182   E     1       [18:14:04] 23/5/2019   N    fwk_wd -i 1 -i6 0
CPSICDEMUX  0           5383   E     1       [18:14:14] 23/5/2019   N    cpsicdemux
CPVIEWD     0           5407   E     1       [18:14:15] 23/5/2019   N    cpviewd
HISTORYD    0           5410   E     1       [18:14:15] 23/5/2019   N    cpview_historyd
SXL_STATD   0           5413   E     1       [18:14:15] 23/5/2019   N    sxl_statd
CPD         0           5420   E     1       [18:14:15] 23/5/2019   Y    cpd
MPDAEMON    0           5436   E     1       [18:14:16] 23/5/2019   N    mpdaemon /opt/CPshrd-
R81.20/log/mpdaemon.elg /opt/CPshrd-R81.20/conf/mpdaemon.conf
CI_CLEANUP  0           5626   E     1       [18:14:26] 23/5/2019   N    avi_del_tmp_files
CIHS        0           5628   E     1       [18:14:26] 23/5/2019   N    ci_http_server -j -f
/opt/CPsuite-R81.20/fw1/conf/cihs.conf
FWD         0           5640   E     1       [18:14:26] 23/5/2019   N    fwd
RAD         0           6330   E     1       [18:14:28] 23/5/2019   N    rad
DASERVICE   0           8604   E     1       [18:14:43] 23/5/2019   N    DAService_script
[Expert@HostName:0]#
```

Example - Verbose output on a Management Server

```
[Expert@HostName:0]# cpwd_admin list -full
APP        PID    STAT  #START  START_TIME             SLP/LIMIT  MON
-------------------------------------------------------------------------------
CPVIEWD    19738  E     1       [17:50:44] 31/5/2019   60/5       N
           PATH = /opt/CPshrd-R81.20/bin/cpviewd
           COMMAND = cpviewd
-------------------------------------------------------------------------------
HISTORYD   0      T     0       [17:54:44] 31/5/2019   60/5       N
           PATH = /opt/CPshrd-R81.20/bin/cpview_historyd
           COMMAND = cpview_historyd
-------------------------------------------------------------------------------
CPD        19730  E     1       [17:54:45] 31/5/2019   60/5       Y
           PATH = /opt/CPshrd-R81.20/bin/cpd
           COMMAND = cpd
-------------------------------------------------------------------------------
SOLR       19935  E     1       [17:50:55] 31/5/2019   60/5       N
           PATH = /opt/CPrt-R81.20/bin/java_solr
           COMMAND = java_solr /opt/CPrt-R81.20/conf/jetty.xml
-------------------------------------------------------------------------------
RFL        19951  E     1       [17:50:55] 31/5/2019   60/5       N
           PATH = /opt/CPrt-R81.20/bin/LogCore
           COMMAND = LogCore
-------------------------------------------------------------------------------
SMARTVIEW  19979  E     1       [17:50:55] 31/5/2019   60/5       N
           PATH = /opt/CPrt-R81.20/bin/SmartView
           COMMAND = SmartView
-------------------------------------------------------------------------------
INDEXER    20032  E     1       [17:50:55] 31/5/2019   60/5       N
           PATH = /opt/CPrt-R81.20/log_indexer/log_indexer
           COMMAND = /opt/CPrt-R81.20/log_indexer/log_indexer
-------------------------------------------------------------------------------
SMARTLOG_SERVER 20100  E     1       [17:50:55] 31/5/2019   60/5       N
           PATH = /opt/CPSmartLog-R81.20/smartlog_server
           COMMAND = /opt/CPSmartLog-R81.20/smartlog_server
           ENV = LANG=C
-------------------------------------------------------------------------------
CP3DLOGD   20237  E     1       [17:50:55] 31/5/2019   60/5       N
           PATH = /opt/CPuepm-R81.20/bin/cp3dlogd
           COMMAND = cp3dlogd
-------------------------------------------------------------------------------
EPM        20251  E     1       [17:50:56] 31/5/2019   60/5       N
           PATH = /opt/CPuepm-R81.20/bin/startEngine
           COMMAND = startEngine
-------------------------------------------------------------------------------
DASERVICE  20404  E     1       [17:50:59] 31/5/2019   60/5       N
           PATH = /opt/CPda/bin/DAService_script
           COMMAND = DAService_script
[Expert@HostName:0]#
```

Example - Verbose output on a Security Gateway

```
[Expert@HostName:0]# cpwd_admin list -full
APP         CTX        PID    STAT  #START  START_TIME             SLP/LIMIT  MON
-------------------------------------------------------------------------------
FWK_FORKER 0           4180   E     1       [18:14:04] 23/5/2019   60/5       N
                       PATH = /opt/CPsuite-R81.20/fw1/bin/fwk_forker
                       COMMAND = fwk_forker
-------------------------------------------------------------------------------
FWK_WD     0           4182   E     1       [18:14:04] 23/5/2019   3/u        N
                       PATH = /opt/CPsuite-R81.20/fw1/bin/fwk_wd
                       COMMAND = fwk_wd -i 1 -i6 0
-------------------------------------------------------------------------------
CPSICDEMUX 0           5383   E     1       [18:14:14] 23/5/2019   60/5       N
                       PATH = /opt/CPshrd-R81.20/bin/cpsicdemux
                       COMMAND = cpsicdemux
-------------------------------------------------------------------------------
CPVIEWD    0           5407   E     1       [18:14:15] 23/5/2019   60/5       N
                       PATH = /opt/CPshrd-R81.20/bin/cpviewd
                       COMMAND = cpviewd
-------------------------------------------------------------------------------
HISTORYD   0           5410   E     1       [18:14:15] 23/5/2019   60/5       N
                       PATH = /opt/CPshrd-R81.20/bin/cpview_historyd
                       COMMAND = cpview_historyd
-------------------------------------------------------------------------------
SXL_STATD  0           5413   E     1       [18:14:15] 23/5/2019   60/5       N
                       PATH = /opt/CPsuite-R81.20/fw1/bin/sxl_statd
                       COMMAND = sxl_statd
-------------------------------------------------------------------------------
CPD        0           5420   E     1       [18:14:15] 23/5/2019   60/5       Y
                       PATH = /opt/CPshrd-R81.20/bin/cpd
                       COMMAND = cpd
-------------------------------------------------------------------------------
MPDAEMON   0           5436   E     1       [18:14:16] 23/5/2019   60/5       N
                       PATH = /opt/CPshrd-R81.20/bin/mpdaemon
                       COMMAND = mpdaemon /opt/CPshrd-R81.20/log/mpdaemon.elg /opt/CPshrd-
R81.20/conf/mpdaemon.conf
-------------------------------------------------------------------------------
CI_CLEANUP 0           5626   E     1       [18:14:26] 23/5/2019   60/5       N
                       PATH = /opt/CPsuite-R81.20/fw1/bin/avi_del_tmp_files
                       COMMAND = avi_del_tmp_files
-------------------------------------------------------------------------------
CIHS       0           5628   E     1       [18:14:26] 23/5/2019   60/5       N
                       PATH = /opt/CPsuite-R81.20/fw1/bin/ci_http_server
                       COMMAND = ci_http_server -j -f /opt/CPsuite-R81.20/fw1/conf/cihs.conf
-------------------------------------------------------------------------------
FWD        0           5640   E     1       [18:14:26] 23/5/2019   60/5       N
                       PATH = /opt/CPsuite-R81.20/fw1/bin/fw
                       COMMAND = fwd
-------------------------------------------------------------------------------
RAD        0           6330   E     1       [18:14:28] 23/5/2019   60/5       N
                       PATH = /opt/CPsuite-R81.20/fw1///bin/rad
                       COMMAND = rad
-------------------------------------------------------------------------------
DASERVICE  0           8604   E     1       [18:14:43] 23/5/2019   60/5       N
                       PATH = /opt/CPda/bin/DAService_script
                       COMMAND = DAService_script
[Expert@HostName:0]#
```

cpwd_admin monitor_list

Description

Prints the status of actively monitored processes on the screen.

See the explanation about the active monitoring in *"cpwd_admin" on page 220*.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin monitor_list
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin monitor_list
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin monitor_list
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin monitor_list
```

Example

```
[Expert@HostName:0]# cpwd_admin monitor_list
cpwd_admin:
APP        FILE_NAME                      NO_MSG_TIMES   LAST_MSG_TIME
CPD        CPD_5420_4714.mntr             0/10           [19:00:33] 31/5/2019
[Expert@HostName:0]#
```

cpwd_admin start

Description

Starts a process as monitored by the WatchDog.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin start -name <Application Name> -path "<Full Path to
Executable>" -command "<Command Syntax>" [-env {inherit | <Env_
Var>=<Value>] [-slp_timeout <Timeout>] [-retry_limit {<Limit> |
u}]
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin start -name <Application Name> [-ctx <VSID>] -path
"<Full Path to Executable>" -command "<Command Syntax>" [-env
{inherit | <Env_Var>=<Value>] [-slp_timeout <Timeout>] [-retry_
limit {<Limit> | u}]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin start -name <Application Name> [-ctx <VSID>] -path
"<Full Path to Executable>" -command "<Command Syntax>" [-env
{inherit | <Env_Var>=<Value>] [-slp_timeout <Timeout>] [-retry_
limit {<Limit> | u}]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin start -name <Application Name> [-ctx <VSID>] -
path "<Full Path to Executable>" -command "<Command Syntax>" [-env
{inherit | <Env_Var>=<Value>] [-slp_timeout <Timeout>] [-retry_
limit {<Limit> | u}]
```

Parameters

Parameter	Description
`-name <Application Name>`	Name, under which the `cpwd_admin list` command shows the monitored process in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`
`-ctx <VSID>`	On a VSX Gateway, specifies the context of the applicable Virtual System.
`-path "<Full Path to Executable>"`	The full path (with or without Check Point environment variables) to the executable including the executable name. Must enclose in double quotes. Examples: ■ For FWM: "`$FWDIR/bin/fwm`" ■ For FWD: "`/opt/CPsuite-R81.20/fw1/bin/fw`" ■ For CPD: "`$CPDIR/bin/cpd`" ■ For CPM: "`/opt/CPsuite-R81.20/fw1/scripts/cpm.sh`" ■ For SICTUNNEL: "`/opt/CPshrd-R81.20/bin/cptnl`"
`-command "<Command Syntax>"`	The command and its arguments to run. Must enclose in double quotes. Examples: ■ For FWM: "`fwm`" ■ For FWM on Multi-Domain Server: "`fwm mds`" ■ For FWD: "`fwd`" ■ For CPD: "`cpd`" ■ For CPM: "`/opt/CPsuite-R81.20/fw1/scripts/cpm.sh -s`" ■ For SICTUNNEL: "`/opt/CPshrd-R81.20/bin/cptnl -c "/opt/CPuepm-R81.20/engine/conf/cptnl_srv.conf"`"

Parameter	Description
`-env {inherit | <Env_Var>=<Value>}`	Configures whether to inherit the environment variables from the shell. ■ `inherit` - Inherits all the environment variables (WatchDog supports up to 80 environment variables) ■ *<Env_Var>=<Value>* - Assigns the specified value to the specified environment variable
`-slp_timeout <Timeout>`	Configures the specified value of the "`sleep_timeout`" configuration parameter. See *"cpwd_admin config" on page 224*.
`-retry_limit {<Limit> | u}`	Configures the value of the "`retry_limit`" configuration parameter. See *"cpwd_admin config" on page 224*. ■ *<Limit>* - Tries to restart the process the specified number of times ■ `u` - Tries to restart the process unlimited number of times

Example

For the list of process and the applicable syntax, see sk97638.

cpwd_admin start_monitor

Description

Starts the active WatchDog monitoring. WatchDog monitors the predefined processes actively.

See the explanation for the *"cpwd_admin" on page 220* command.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin start_monitor
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin start_monitor
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin start_monitor
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin start_monitor
```

Example

```
[Expert@HostName:0]# cpwd_admin start_monitor
cpwd_admin:
CPWD has started to perform active monitoring on Check Point services/processes
[Expert@HostName:0]#
```

cpwd_admin stop

Description

Stops a WatchDog monitored process.

Important - This change does **not** survive reboot.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin stop -name <Application Name> [-path "<Full Path to
Executable>" -command "<Command Syntax>" [-env {inherit | <Env_
Var>=<Value>]
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin stop -name <Application Name> [-ctx <VSID>] [-path
"<Full Path to Executable>" -command "<Command Syntax>" [-env
{inherit | <Env_Var>=<Value>]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin stop -name <Application Name> [-ctx <VSID>] [-path
"<Full Path to Executable>" -command "<Command Syntax>" [-env
{inherit | <Env_Var>=<Value>]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin stop -name <Application Name> [-ctx <VSID>] [-
path "<Full Path to Executable>" -command "<Command Syntax>" [-env
{inherit | <Env_Var>=<Value>]
```

Parameters

Parameter	Description
`-name <Application Name>`	Name under which the `cpwd_admin list` command shows the monitored process in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`
`-ctx <VSID>`	On a VSX Gateway, specifies the context of the applicable Virtual System.
`-path "<Full Path to Executable>"`	The full path (with or without Check Point environment variables) to the executable including the executable name. Must enclose in double quotes. Examples: ■ For FWM: "`$FWDIR/bin/fwm`" ■ For FWD: "`/opt/CPsuite-R81.20/fw1/bin/fw`" ■ For CPD: "`$CPDIR/bin/cpd_admin`"
`-command "<Command Syntax>"`	The command and its arguments to run. Must enclose in double quotes. Examples: ■ For FWM: "`fw kill fwm`" ■ For FWD: "`fw kill fwd`" ■ For CPD: "`cpd_admin stop`"
`-env {inherit | <Env_Var>=<Value>}`	Configures whether to inherit the environment variables from the shell. ■ `inherit` - Inherits all the environment variables (WatchDog supports up to 80 environment variables) ■ `<Env_Var>=<Value>` - Assigns the specified value to the specified environment variable

Example

For the list of process and the applicable syntax, see sk97638.

cpwd_admin stop_monitor

Description

Stops the active WatchDog monitoring. WatchDog monitors all processes only passively.

See the explanation for the *"cpwd_admin" on page 220* command.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin stop_monitor
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin stop_monitor
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin stop_monitor
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin stop_monitor
```

Example

```
[Expert@HostName:0]# cpwd_admin stop_monitor
cpwd_admin:
CPWD has stopped performing active monitoring on Check Point services/processes
[Expert@HostName:0]#
```

dbedit

Description

Edits the management database - the `$FWDIR/conf/objects_5_0.C` file - on the Security Management Server or Domain Management Server. See sk13301.

Important - Do NOT run this command, unless explicitly instructed by Check Point Support or R&D to do so. Otherwise, you can corrupt settings in the management database.

Syntax

```
dbedit -help
```

```
dbedit [-globallock] [{-local | -s <Management_Server>}] [{-u
<Username> | -c <Certificate>}] [-p <Password>] [-f <File_Name>
[ignore_script_failure] [-continue_updating]] [-r "<Open_Reason_
Text>"] [-d <Database_Name>] [-listen] [-readonly] [-session]
```

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Parameters

Parameter	Description
`-help`	Prints the general help.
`-globallock`	When you work with the dbedit utility, it partially locks the management database. If a user configures objects in SmartConsole at the same time, it causes problems in the management database. This option does not let SmartConsole, or a dbedit user to make changes in the management database. When you specify this option, the dbedit commands run on a copy of the management database. After you make the changes with the `dbedit` commands and run the `savedb` command, the dbedit utility saves and commits your changes to the actual management database.
`-local`	Connects to the localhost (127.0.0.1) without using username/password. If you do not specify this parameter, the dbedit utility asks how to connect.

Parameter	Description
`-s <Management_Server>`	Specifies the Security Management Server - by IP address or HostName. If you do not specify this parameter, the dbedit utility asks how to connect.
`-u <Username>`	Specifies the username, with which the dbedit utility connects to the Security Management Server. Mandatory parameter when you specify the "`-s <Management_Server>`" parameter.
`-c <Certificate>`	Specifies the user's certificate file, with which the dbedit utility connects to the Security Management Server. Mandatory parameter when you specify the "`-s <Management_Server>`" parameter.
`-p <Password>`	Specifies the user's password, with which the dbedit utility connects to the Security Management Server. Mandatory parameter when you specify the "`-s <Management_Server>`" and "`-u <Username>`" parameters.
`-f <File_Name>`	Specifies the file that contains the applicable dbedit internal commands (see the section "*dbedit Internal Commands*" below): ■ `create <object_type> <object_name>` ■ `modify <table_name> <object_name> <field_name> <value>` ■ `update <table_name> <object_name>` ■ `delete <table_name> <object_name>` ■ `print <table_name> <object_name>` ■ `quit` **Note** - Each command is limited to 4096 characters.
`ignore_script_failure`	Continues to execute the dbedit internal commands in the file and ignores errors. You can use it when you specify the "`-f <File_Name>`" parameter.
`-continue_updating`	Continues to update the modified objects, even if the operation fails for some of the objects (ignores the errors and runs the `update_all` command at the end of the script). You can use it when you specify the "`-f <File_Name>`" parameter.
`-r "<Open_Reason_Text>"`	Specifies the reason for opening the database in read-write mode (default mode).

Parameter	Description
`-d <Database_Name>`	Specifies the name of the database, to which the dbedit utility should connect (for example, `mdsdb`).
`-listen`	The dbedit utility "listens" for changes (use this mode for advanced troubleshooting with the assistance of Check Point Support). The dbedit utility prints its internal messages when a change occurs in the management database.
`-readonly`	Specifies to open the management database in read-only mode.
`-session`	Session Connectivity.

`dbedit` Internal Commands

Note - To see the available tables, class names (object types), attributes and values, connect to Management Server with Database Tool (GuiDBEdit Tool) (see sk13009).

Command	Description, Syntax, Examples
`-h`	**Description:** Prints the general help. **Syntax:** `dbedit> -h`

`-q`
 	
`quit`
	Description:
	Quits from dbedit.
	Syntax:
	`dbedit> -q`
	`dbedit> quit [-update_all | -noupdate]`
	Examples:
	■ Exit the utility and commit the remaining modified objects (interactive mode):
	`dbedit> quit`
	■ Exit the utility and update all the remaining modified objects:
	`dbedit> quit -update_all`
	■ Exit the utility and discard all modifications:
	`dbedit> quit -no_update`

Command	Description, Syntax, Examples

`update`	**Description:**
	Saves the specified object in the specified table (for example, "`network_objects`", "`services`", "`users`").
	Syntax:
	`dbedit> update <table_name> <object_name>`
	Example:
	Save the object *My_Service* in the table *services*:
	`dbedit> update services My_Service`

`update_all`	**Description:** Saves all the modified objects. **Syntax:** `dbedit> update_all`

`_print_set`	**Description:**
	Prints the specified object from the specified table (for example, "`network_objects`", "`services`", "`users`") as it appears in the `$FWDIR/conf/objects_5_0.C` file (sets of attributes).
	Syntax:
	`dbedit> _print_set <table_name> <object_name>`
	Example:
	Print the object *My_Obj* from the table *network_objects*:
	`dbedit> print network_objects My_Obj`

`print`	**Description:**
	Prints the list of attributes of the specified object from the specified table (for example, "`network_objects`", "`properties`", "`services`", "`users`").
	Syntax:
	`dbedit> print <table_name> <object_name>`
	Examples:
	■ Print the object *My_Obj* from the table *network_objects* (in "Network Objects"):
	`dbedit> print network_objects my_obj`
	■ Print the object *firewall_properties* from the table *properties* (in "Global Properties"):
	`dbedit> print properties firewall_properties`

Command	Description, Syntax, Examples

`printxml`	**Description:**
	Prints in XML format the list of attributes of the specified object from the specified table (for example, "`network_objects`", "`properties`", "`services`", "`users`").
	You can export the settings from a Management Server to an XML file that you can use later with external automation systems.
	Syntax:
	`dbedit> printxml <table_name> [<object_name>]`
	Examples:
	■ Print the object *My_Obj* from the table *network_objects*:
	`dbedit> printxml network_objects my_obj`
	■ Print the object *firewall_properties* from the table *properties* (in "Global Properties"):
	`dbedit> printxml properties firewall_ properties`

`printbyuid`	**Description:**
	Prints the attributes of the object specified by its UID (appears in the `$FWDIR/conf/objects_5_0.C` file at the beginning of the object as "`chkpf_uid ({...})`").
	Syntax:
	`dbedit> printbyuid {object_id}`
	Example:
	Print the attributes of the object with the specified UID:
	`dbedit> printbyuid {D3833F1D-0A58-AA42-865F-39BFE3C126F1}`

Command	Description, Syntax, Examples

`query`	**Description:**
	Prints all the objects in the specified table.
	Optionally, you can query for objects with specific attribute and value - query is separated by a comma after "`query <table_name>`" (spaces are not allowed between the `<attribute>` and `'<value>'`).
	Syntax:
	`dbedit> query <table_name> [ , <attribute>='<value>' ]`
	Examples:
	■ Print all objects in the table *users*:
	`dbedit> query users`
	■ Print all objects in the table *network_objects* that are defined as Management Servers:
	`dbedit> query network_objects, management='true'`
	■ Print all objects in the table *services* with the name *ssh*:
	`command_sdbedit> query services, name='ssh'`
	■ Print all objects in the table *services* with the port *22*:
	`dbedit> query services, port='22'`
	■ Print all objects with the IP address *10.10.10.10*:
	`dbedit> query network_objects, ipaddr='10.10.10.10'`

`whereused`	**Description:**
	Checks where the specified object used in the database.
	Prints the number of places, where this object is used and relevant information about each such place.
	Syntax:
	`dbedit> whereused <table_name> <object_name>`
	Example:
	Check where the object *My_Obj* is used:
	`dbedit> whereused network_objects My_Obj`

Command	Description, Syntax, Examples

`create`	**Description:**
	Creates an object of specified type (with its default values) in the database.
	Restrictions apply to the object's name:
	■ Object names can have a maximum of 100 characters.
	■ Objects names can contain only ASCII letters, numbers, and dashes.
	■ Reserved words will be blocked by the Management Server (refer to sk40179).
	Syntax:
	`dbedit> create <object_type> <object_name>`
	Example:
	Create the service object *My_Service* of the type *tcp_service* (with its default values):
	`dbedit> create tcp_service my_service`

`delete`	**Description:**
	Deletes an object from the specified table.
	Syntax:
	`dbedit> delete <table_name> <object_name>`
	Example:
	Delete the service object *My_Service* from the table *services*:
	`dbedit> delete services my_service`

Command	Description, Syntax, Examples

`modify`	**Description:**
	Modifies the value of specified attribute in the specified object in the specified table (for example, "`network_objects`", "`services`", "`users`") in the management database.
	Syntax:
	`dbedit> modify <table_name> <object_name> <field_name> <value>`
	Examples:
	■ Modify the color to *red* in the object *My_Service* in the table *services*:
	`dbedit> modify services My_Service color red`
	■ Add a comment to the object *MyObj*:
	`dbedit> modify network_objects MyObj comments "Created by fwadmin with dbedit"`
	■ Set the value of the global property *ike_use_largest_possible_subnets* in the table *properties* to *false*:
	`dbedit> modify properties firewall_properties ike_use_largest_possible_subnets false`
	■ Create a new interface on the Security Gateway *My_FW* and modify its attributes - set the IP address / Mask and enable Anti-Spoofing on interface with *"Element Index"=3* (check the attributes of the object *My_FW* in Database Tool (GuiDBEdit Tool) (see sk13009)):

Command	Description, Syntax, Examples

```
dbedit> addelement network_objects My_FW
interfaces interface
dbedit> modify network_objects My_FW
interfaces:3:officialname NAME_OF_INTERFACE
dbedit> modify network_objects My_FW
interfaces:3:ipaddr IP_ADDRESS
dbedit> modify network_objects My_FW
interfaces:3:netmask NETWORK_MASK
dbedit> modify network_objects My_FW
interfaces:3:security:netaccess:access
specific
dbedit> modify network_objects My_FW
interfaces:3:security:netaccess:allowed
network_objects:group_name
dbedit> modify network_objects My_FW
interfaces:3:security:netaccess:perform_anti_
spoofing true
dbedit> modify network_objects MyObj FieldA
LINKSYS
```

- In the Owned Object *MyObj* change the value of *FieldB* to *NewVal*:

```
dbedit> modify network_objects MyObj
FieldA:FieldB NewVal
```

- In the Linked Object *MyObj* change the value of *FieldA* from *B* to *C*:

```
dbedit> modify network_objects MyObj FieldA
B:C
```

Command	Description, Syntax, Examples

`lock`	**Description:**
	Locks the specified object (by administrator) in the specified table (for example, "`network_objects`", "`services`", "`users`") from being modified by other users.
	For example, if you connect from a remote server to this Management Server with *admin1* and lock an object, you are be able to connect with *admin2*, but are not able to modify the locked object, until *admin1* releases the lock.
	Syntax:
	`dbedit> lock <table_name> <object_name>`
	Example:
	Lock the object *My_Service_Obj* in the table *services* in the database:
	`dbedit> lock services My_Service_Obj`

`addelement`	**Description:**
	Adds a specified multiple field / container (with specified value) to a specified object in specified table.
	Syntax:
	`dbedit> addelement <table_name> <object_name> <field_name> <value>`
	Examples:
	■ Add the element *BranchObjectClass* with the value *Organization* to a multiple field *Read* in the object *My_Obj* in the table *ldap*:
	`dbedit> addelement ldap My_Obj Read:BranchObjectClass Organization`
	■ Add the service *MyService* to the group of services *MyServicesGroup* in the table *services*:
	`dbedit> addelement services MyServicesGroup '' services:MyService`
	■ Add the network *MyNetwork* to the group of networks *MyNetworksGroup* in the table *network_objects*:
	`dbedit> addelement network_objects MyNetworksGroup '' network_objects:MyNetwork`

Command	Description, Syntax, Examples

`rmelement`	**Description:**
	Removes a specified multiple field / container (with specified value) from a specified object in specified table.
	Syntax:
	`dbedit> rmelement <table_name> <object_name> <field_name> <value>`
	Examples:
	■ Remove the service *MyService* from the group of services *MyServicesGroup* from the table *services*:
	`dbedit> rmelement services MyServicesGroup '' services:MyService`
	■ Remove the network *MyNetwork* from the group of networks *MyNetworksGroup* from the table *network_objects*:
	`dbedit> rmelement network_objects MyNetworksGroup '' network_objects:MyNetwork`
	■ Remove the element *BranchObjectClass* with the value *Organization* from the multiple field *Read* in the object *My_Obj* in the table *ldap*:
	`dbedit> rmelement ldap my_obj Read:BranchObjectClass Organization`

`rename`	**Description:**
	Renames the specified object in specified table.
	Syntax:
	`dbedit> rename <table_name> <object_name> <new_object_name>`
	Example:
	Rename the network object *london* to *chicago* in the table *network_objects*:
	`dbedit> rename network_objects london chicago`

Command	Description, Syntax, Examples

`rmbyindex`	**Description:**
	Removes an element from a container by element's index.
	Syntax:
	`dbedit> rmbyindex <table_name> <object_name> <field_name> <index_number>`
	Example:
	Remove the element *backup_log_servers* from the container *log_servers* by element index *1* in the table *network_objects*:
	`dbedit> rmbyindex network_objects g log_servers:backup_log_servers 1`

`add_owned_remove_name`	**Description:**
	Adds an owned object (and removes its name) to a specified owned object field (or container).
	Syntax:
	`dbedit> add_owned_remove_name <table_name> <object_name> <field_name> <value>`
	Example:
	Add the owned object *My_Gateway* (and remove its name) to the owned object field (or container) *my_external_products*:
	`dbedit> add_owned_remove_name network_objects My_Gateway additional_products owned:my_external_products`

`is_delete_allowed`	**Description:**
	Checks if the specified object can be deleted from the specified table (object cannot be deleted if it is used by other objects).
	Syntax:
	`dbedit> is_delete_allowed <table_name> <object_name>`
	Example:
	`dbedit> is_delete_allowed network_objects MyObj`
	Check if the object *MyObj* can be deleted from the table *network_objects*:

Command	Description, Syntax, Examples

`set_pass`	**Description:**
	Sets specified password for specified user.
	Notes:
	■ The password must contain at least 4 characters and no more than 50 characters.
	■ This command cannot change the administrator's password.
	Syntax:
	`dbedit> set_pass <Username> <Password>`
	Example:
	Set the password *1234* for the user *abcd*:
	`dbedit> set_pass abcd 1234`

`savedb`	**Description:** Saves the database. You can run this command only when the database is locked globally (when you start the dbedit utility with the "`dbedit -globallock`" command). **Syntax:** `dbedit> savedb`
`savesession`	**Description:** Saves the session. You can run this command only when you start the dbedit utility in session mode (with the "`dbedit -session`" command). **Syntax:** `dbedit> savesession`

evstart

Description

On a dedicated SmartEvent Server or on a Security Management Server with the enabled SmartEvent Server and SmartEvent Correlation Unit Software Blades, this command:

- Starts the SmartEvent Server and the SmartEvent Correlation Unit services, if you stopped them with the "`evstop`" command (see *"evstop" on page 265*).
- Starts only the SmartEvent Correlation Unit service, if you stopped it with the "`evstop`" command (see *"evstop" on page 265*).

Important:

- You can run this command only in the Expert mode.
- SmartEvent Server runs this command automatically:
  - During boot.
  - When you run the "`cpstart`" command (see *"cpstart" on page 208*).

Related command

"evstop" on page 265

Syntax

```
evstart [-analyzer]
```

Parameters

Parameter	Description
No Parameters	Starts the SmartEvent Server and the SmartEvent Correlation Unit services.
`-analyzer`	Starts only the SmartEvent Correlation Unit service.

evstop

Description

On a dedicated SmartEvent Server or on a Security Management Server with the enabled SmartEvent Server and SmartEvent Correlation Unit Software Blades, this command:

- Stops the SmartEvent Server and the SmartEvent Correlation Unit services.
- Stops only the SmartEvent Correlation Unit service.

Important:

- You can run this command only in the Expert mode.
- SmartEvent Server runs this command automatically:
  - When you run the "`cpstop`" command (see *"cpstop" on page 219*).
  - During reboot or shutdown.

Related command

"evstart" on page 264

Syntax

```
evstop [-analyzer]
```

Parameters

Parameter	Description
No Parameters	Stops the SmartEvent Server and the SmartEvent Correlation Unit services.
`-analyzer`	Stops only the SmartEvent Correlation Unit service.

fw

Description

- Performs various operations on Security or Audit log files.
- Kills the specified Check Point processes.
- Manages the Suspicious Activity Monitoring (SAM) rules.
- Manages the Suspicious Activity Policy editor.

Syntax

```
fw [-d]
      fetchlogs <options>
      hastat <options>
      kill <options>
      log <options>
      logswitch <options>
      lslogs <options>
      mergefiles <options>
      repairlog <options>
      sam <options>
      sam_policy <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`fetchlogs <options>`	Fetches the specified Check Point log files - Security (`$FWDIR/log/*.log*`) or Audit (`$FWDIR/log/*.adtlog*`), from the specified Check Point server. See *"fw fetchlogs" on page 268*.
`hastat <options>`	Shows information about Check Point servers in High Availability configuration and their states. See *"fw hastat" on page 272*.

Parameter	Description
`kill <options>`	Kills the specified Check Point process. See *"fw kill" on page 273*.
`log <options>`	Shows the content of Check Point log files - Security (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`). See *"fw log" on page 274*.
`logswitch <options>`	Switches the current active Check Point log file - Security (`$FWDIR/log/fw.log`) or Audit (`$FWDIR/log/fw.adtlog`). See *"fw logswitch" on page 284*.
`lslogs <options>`	Shows a list of Check Point log files - Security (`$FWDIR/log/*.log*`) or Audit (`$FWDIR/log/*.adtlog*`), located on the local server or a remote server. See *"fw lslogs" on page 288*.
`mergefiles <options>`	Merges several Check Point log files - Security (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`), into a single log file. See *"fw mergefiles" on page 291*.
`repairlog <options>`	Rebuilds pointer files for Check Point log files - Security (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`). See *"fw repairlog" on page 294*.
`sam <options>`	Manages the Suspicious Activity Monitoring (SAM) rules. See *"fw sam" on page 295*.

`sam_policy <options>`
or
`samp <options>`
	Manages the Suspicious Activity Policy editor that works with these type of rules:
	■ Suspicious Activity Monitoring (SAM) rules.
	■ Rate Limiting rules.
	See *"fw sam_policy" on page 303*.

fw fetchlogs

Description

Fetches the specified Security log files (`$FWDIR/log/*.log*`) or Audit log files (`$FWDIR/log/*.adtlog*`) from the specified Check Point server.

Important - You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).

Syntax

```
fw [-d] fetchlogs [-f <Name of Log File 1>] [-f <Name of Log File 2>]... [-f <Name of Log File N>] <Target>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-f <Name of Log File N>`	Specifies the name of the log file to fetch. Need to specify name only. **Notes:** ■ If you do not specify the log file name explicitly, the command transfers all Security log files (`$FWDIR/log/*.log*`) and all Audit log files (`$FWDIR/log/*.adtlog*`). ■ The specified log file name can include wildcards * and ? (for example, `2017-0?-*.log`). If you enter a wildcard, you must enclose it in double quotes or single quotes. ■ You can specify multiple log files in one command. You must use the `-f` parameter for each log file name pattern. ■ This command also transfers the applicable log pointer files.
`<Target>`	Specifies the remote Check Point server, with which this local Check Point server has established SIC trust. **Notes:** ■ The local and the remote servers must have established SIC trust. ■ The local server can be a Security Management Server, a Log Server, a Cluster Member. ■ The remote server can be a Security Gateway, a Cluster Member, a Log Server, or a Security Management Server in High Availability deployment. ■ You can specify the remote managed server by its main IP address or Object Name as configured in SmartConsole.

Notes:

- This command moves the specified log files from the `$FWDIR/log/` directory on the specified Check Point server.

  Meaning, it deletes the specified log files on the specified Check Point server after it copies them successfully.

- This command moves the specified log files to the `$FWDIR/log/` directory on the local Check Point server, on which you run this command.

- This command cannot fetch the *active* log files `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`.

  To fetch these active log files:

  1. Perform the log switch on the applicable Check Point server:

     See *"fw logswitch" on page 284*.

     ```
     fw logswitch [-audit] [-h <IP Address or Hostname>]
     ```

  2. Fetch the rotated log file from the applicable Check Point server:

     ```
     fw fetchlogs -f <Log File Name> <IP Address or Hostname>
     ```

- This command renames the log files it fetched from the specified Check Point server.

  The new log file name is the concatenation of these:

  - The Check Point server's name (as configured in SmartConsole).
  - Two underscore (_) characters.
  - The original log file name

  Example: `MyGW__2019-06-01_000000.log`

Example - Fetching log files from a Management Server

```
[Expert@HostName:0]# fw lslogs MyGW
     Size Log file name
        23KB 2019-05-16_000000.log
         9KB 2019-05-17_000000.log
        11KB 2019-05-18_000000.log
      5796KB 2019-06-01_000000.log
      4610KB fw.log
[Expert@HostName:0]#

[Expert@HostName:0]# fw fetchlogs -f 2019-06-01_000000 MyGW
File fetching in process. It may take some time...
File MyGW__2019-06-01_000000.log was fetched successfully
[Expert@HostName:0]#

[Expert@HostName:0]# ls $FWDIR/log/MyGW*
/opt/CPsuite-R81.20/fw1/log/MyGW__2019-06-01_000000.log
/opt/CPsuite-R81.20/fw1/log/MyGW__2019-06-01_000000.logaccount_ptr
/opt/CPsuite-R81.20/fw1/log/MyGW__2019-06-01_000000.loginitial_ptr
/opt/CPsuite-R81.20/fw1/log/MyGW__2019-06-01_000000.logptr
[Expert@HostName:0]#

[Expert@HostName:0]# fw lslogs MyGW
     Size Log file name
        23KB 2019-05-16_000000.log
         9KB 2019-05-17_000000.log
        11KB 2019-05-18_000000.log
      4610KB fw.log
[Expert@HostName:0]#
```

fw hastat

Description

Shows information about Check Point computers in High Availability configuration and their states.

Note - This command is outdated. On cluster members, run the Gaia Clish command "`show cluster state`", or the Expert mode command "`cphaprob state`".

Note - This command is outdated. On Management Servers, run the *"cpstat" on page 209* command.

Syntax

```
fw hastat [<Target1>] [<Target2>] ... [<TargetN>]
```

Parameters

Parameter	Description
<Target1> *<Target2>* ... *<TargetN>*	Specifies the Check Point computers to query. If you run this command on the Management Server, you can enter the applicable IP address, or the resolvable HostName of the managed Security Gateway or Cluster Member. If you do not specify the target, the command queries the local computer.

Example - Querying the cluster members from the Management Server

```
[Expert@MGMT:0]# fw hastat 192.168.3.52
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.52 1 active OK
[Expert@MGMT:0]#

[Expert@MGMT:0]# fw hastat 192.168.3.53
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.53 2 stand-by OK
[Expert@MGMT:0]#

[Expert@MGMT:0]# fw hastat 192.168.3.52 192.168.3.53
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.52 1 active OK
192.168.3.53 2 stand-by OK
[Expert@MGMT:0]#
```

Example - Querying the local Cluster Member

```
[Expert@Member1:0]# fw hastat
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.52 1 active OK
[Expert@Member1:0]#
```

fw kill

Description

Kills the specified Check Point processes.

Important:

- Make sure the killed process is restarted, or restart it manually. See sk97638.
- You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).

Syntax

```
fw [-d] kill [-t <Signal Number>] <Name of Process>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-t <Signal Number>`	Specifies which signal to send to the Check Point process. For the list of available signals and their numbers, run the `kill -l` command. For information about the signals, see the manual pages for the `kill` and `signal`. If you do not specify the signal explicitly, the command sends Signal 15 (`SIGTERM`). **Note** - Processes can ignore some signals.
`<Name of Process>`	Specifies the name of the Check Point process to kill. To see the names of the processes, run the `ps auxwf` command.

Example

```
fw kill fwd
```

fw log

Description

Shows the content of Check Point log files - Security (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`).

Important - You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).

Syntax

```
fw log {-h | -help}
```

```
fw [-d] log [-a] [-b "<Start Timestamp>" "<End Timestamp>"] [-c
<Action>] [{-f | -t}] [-g] [-H] [-h <Origin>] [-i] [-k {<Alert
Name> | all}] [-l] [-m {initial | semi | raw}] [-n] [-o] [-p] [-q]
[-S] [-s "<Start Timestamp>"] [-e "<End Timestamp>"] [-u
<Unification Scheme File>] [-w] [-x <Start Entry Number>] [-y <End
Entry Number>] [-z] [-#] [<Log File>]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the built-in usage. **Note** - The built-in usage does not show some of the parameters described in this table.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-a`	Shows only Account log entries.

Parameter	Description
`-b "<Start Timestamp>" "<End Timestamp>"`	Shows only entries that were logged between the specified start and end times. ■ The *<Start Timestamp>* and *<End Timestamp>* may be a date, a time, or both. ■ If date is omitted, then the command assumes the current date. ■ Enclose the "*<Start Timestamp>*" and "*<End Timestamp>* in single or double quotes (`-b 'XX' 'YY'`", or `-b "XX" "YY`). ■ You cannot use the "`-b`" parameter together with the "`-s`" or "`-e`" parameters. ■ See the date and time format below.
`-c <Action>`	Shows only events with the specified action. One of these: ■ `accept` ■ `drop` ■ `reject` ■ `encrypt` ■ `decrypt` ■ `vpnroute` ■ `keyinst` ■ `authorize` ■ `deauthorize` ■ `authcrypt` ■ `ctl` **Notes:** ■ The `fw log` command always shows the **Control** (`ctl`) actions. ■ For *login* action, use the `authcrypt`.
`-e "<End Timestamp>"`	Shows only entries that were logged before the specified time. **Notes:** ■ The *<End Timestamp>* may be a date, a time, or both. ■ Enclose the *<End Timestamp>* in single or double quotes (`-e '...'`, or `-e "..."`). ■ You cannot use the "`-e`" parameter together with the "`-b`" parameter. ■ See the date and time format below.

Parameter	Description
`-f`	This parameter: 1. Shows the saved entries that match the specified conditions. 2. After the command reaches the end of the currently opened log file, it continues to monitor the log file indefinitely and shows the new entries that match the specified conditions. **Note** - Applies only to the *active* log file `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`
`-g`	Does not show delimiters. The default behavior is: ■ Show a colon (`:`) after a field name ■ Show a semi-colon (`;`) after a field value
`-H`	Shows the High Level Log key.
`-h <Origin>`	Shows only logs that were generated by the Security Gateway with the specified IP address or object name (as configured in SmartConsole).
`-i`	Shows log UID.
`-k {<Alert Name> | all}`	Shows entries that match a specific alert type: ■ *<Alert Name>* - Show only entries that match a specific alert type: • `alert` • `mail` • `snmp_trap` • `spoof` • `user_alert` • `user_auth` ■ `all` - Show entries that match all alert types (this is the default).
`-l`	Shows both the date and the time for each log entry. The default is to show the date only once above the relevant entries, and then specify the time for each log entry.

Parameter	Description
`-m`	Specifies the log unification mode: ■ `initial` - Complete unification of log entries. The command shows one unified log entry for each ID. This is the default. If you also specify the `-f` parameter, then the output does not show any updates, but shows only entries that relate to the start of new connections. To shows updates, use the `semi` parameter. ■ `semi` - Step-by-step unification of log entries. For each log entry, the output shows an entry that unifies this entry with all previously encountered entries with the same ID. ■ `raw` - No log unification. The output shows all log entries.
`-n`	Does not perform DNS resolution of the IP addresses in the log file (this is the default behavior). This significantly speeds up the log processing.
`-o`	Shows detailed log chains - shows all the log segments in the log entry.
`-p`	Does not perform resolution of the port numbers in the log file (this is the default behavior). This significantly speeds up the log processing.
`-q`	Shows the names of log header fields.
`-S`	Shows the Sequence Number.
`-s "<Start Timestamp>"`	Shows only entries that were logged after the specified time. **Notes:** ■ The *<Start Timestamp>* may be a date, a time, or both. ■ If the date is omitted, then the command assumed the current date. ■ Enclose the *<Start Timestamp>* in single or double quotes (`-s '...'`, or `-s "..."`). ■ You cannot use the "`-s`" parameter together with the "`-b`" parameter. ■ See the date and time format below.

Parameter	Description
`-t`	This parameter: 1. Does not show the saved entries that match the specified conditions. 2. After the command reaches the end of the currently opened log file, it continues to monitor the log file indefinitely and shows the new entries that match the specified conditions. **Note** - Applies only to the *active* log file `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`
`-u <Unification Scheme File>`	Specifies the path and name of the log unification scheme file. The default log unification scheme file is: `$FWDIR/conf/log_unification_scheme.C`
`-w`	Shows the flags of each log entry (different bits used to specify the "nature" of the log - for example, control, audit, accounting, complementary, and so on).
`-x <Start Entry Number>`	Shows only entries from the specified log entry number and below, counting from the beginning of the log file.
`-y <End Entry Number>`	Shows only entries until the specified log entry number, counting from the beginning of the log file.
`-z`	In case of an error (for example, wrong field value), continues to show log entries. The default behavior is to stop.
`-#`	Show confidential logs in clear text.
`<Log File>`	Specifies the log file to read. If you do not specify the log file explicitly, the command opens the `$FWDIR/log/fw.log` log file. You can specify a switched log file.

Date and Time format

Part of timestamp	Format	Example
Date only	`MMM DD, YYYY`	`June 11, 2018`
Time only Note - In this case, the command assumes the current date.	`HH:MM:SS`	`14:20:00`
Date and Time	`MMM DD, YYYY HH:MM:SS`	`June 11, 2018 14:20:00`

Output

Each output line consists of a single log entry, whose fields appear in this format:

Note - The fields that show depends on the connection type.

```
HeaderDateHour ContentVersion HighLevelLogKey Uuid SequenceNum
Flags Action Origin IfDir InterfaceName LogId ...
```

This table describes some of the fields.

Field Header	Description	Example
`HeaderDateHour`	Date and Time	`12Jun2018 12:56:42`
`ContentVersion`	Version	`5`
`HighLevelLogKey`	High Level Log Key	`<max_null>`, or empty
`Uuid`	Log UUID	`(0x5b1f99cb,0x0,0x3403a8c0,0xc0000000)`
`SequenceNum`	Log Sequence Number	`1`

Field Header	Description	Example
`Flags`	Internal flags that specify the "nature" of the log - for example, control, audit, accounting, complementary, and so on	`428292`
`Action`	Action performed on this connection	■ `accept` ■ `dropreject` ■ `encrypt` ■ `decrypt` ■ `vpnroute` ■ `keyinst` ■ `authorize` ■ `deauthorize` ■ `authcrypt` ■ `ctl`
`Origin`	Object name of the Security Gateway that generated this log	`MyGW`
`IfDir`	Traffic direction through interface: ■ `<` - Outbound (sent by a Security Gateway) ■ `>` - Inbound (received by a Security Gateway)	■ `<` ■ `>`

Field Header	Description	Example
`InterfaceName`	Name of the Security Gateway interface, on which this traffic was logged If a Security Gateway performed some internal action (for example, log switch), then the log entry shows `daemon`	■ `eth0` ■ `daemon` ■ `N/A`
`LogId`	Log ID	`0`
`Alert`	Alert Type	■ `alert` ■ `mail` ■ `snmp_trap` ■ `spoof` ■ `user_alert` ■ `user_auth`
`OriginSicName`	SIC name of the Security Gateway that generated this log	`CN=MyGW,O=MyDomain_ Server.checkpoint.com.s6t98x`
`inzone`	Inbound Security Zone	`Local`
`outzone`	Outbound Security Zone	`External`
`service_id`	Name of the service used to inspect this connection	`ftp`
`src`	Object name or IP address of the connection's source server	`MyHost`

Field Header	Description	Example
`dst`	Object name or IP address of the connection's destination server	`MyFTPServer`
`proto`	Name of the connection's protocol	`tcp`
`sport_svc`	Source port of the connection	`64933`
`ProductName`	Name of the Check Point product that generated this log	■ `VPN-1 & FireWall-1` ■ `Application Control` ■ `FloodGate-1`
`ProductFamily`	Name of the Check Point product family that generated this log	`Network`

Examples

Example 1 - Show all log entries with both the date and the time for each log entry

```
fw log -l
```

Example 2 - Show all log entries that start after the specified timestamp

```
[Expert@MyGW:0]# fw log -l -s "June 12, 2018 12:33:00"
 12Jun2018 12:33:00 5 N/A 1 accept MyGW > N/A LogId: <max_null>; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; fg-1_client_in_rule_name: Default; fg-1_client_out_rule_name: Default; fg-1_server_in_rule_name: Host
Redirect; fg-1_server_out_rule_name: ; ProductName: FG; ProductFamily: Network;

 12Jun2018 12:33:39 5 N/A 1 drop MyGW < eth0 LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; inzone: Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_
table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid: 4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_
uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_table: TABLE_END; UP_action_table: TABLE_START; ROW_
START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc: ftp; sport_svc: 64933;
ProductFamily: Network;

... ... ...

[Expert@MyGW:0]#
```

Example 3 - Show all log entries between the specified timestamps

```
[Expert@MyGW:0]# fw log -l -b "June 12, 2018 12:33:00" 'June 12, 2018 12:34:00'
 12Jun2018 12:33:00 5 N/A 1 accept MyGW > N/A LogId: <max_null>; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; fg-1_client_in_rule_name: Default; fg-1_client_out_rule_name: Default; fg-1_server_in_rule_name: Host
Redirect; fg-1_server_out_rule_name: ; ProductName: FG; ProductFamily: Network;

 12Jun2018 12:33:39 5 N/A 1 drop MyGW < eth0 LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; inzone: Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_
table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid: 4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_
uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_table: TABLE_END; UP_action_table: TABLE_START; ROW_
START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc: ftp; sport_svc: 64933;
ProductFamily: Network;

 12Jun2018 12:33:45 5 N/A 1 ctl MyGW > LogId: <max_null>; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; description: Contracts; reason: Could not reach
"https://productcoverage.checkpoint.com/ProductCoverageService". Check DNS and Proxy configuration on the gateway.; Severity: 2;
status: Failed; version: 1.0; failure_impact: Contracts may be out-of-date; update_service: 1; ProductName: Security
Gateway/Management; ProductFamily: Network;
[Expert@MyGW:0]#
```

Example 4 - Show all log entries with action "drop"

```
[Expert@MyGW:0]# fw log -l -c drop
 12Jun2018 12:33:39 5 N/A 1 drop MyGW < eth0 LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; inzone: Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_
table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid: 4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_
uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_table: TABLE_END; UP_action_table: TABLE_START; ROW_
START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc: ftp; sport_svc: 64933;
ProductFamily: Network;
[Expert@MyGW:0]#
```

Example 5 - Show all log entries with action "drop", show all field headers, and show log flags

```
[Expert@MyGW:0]# fw log -l -q -w -c drop
 HeaderDateHour: 12Jun2018 12:33:39; ContentVersion: 5; HighLevelLogKey: <max_null>; LogUid: ; SequenceNum: 1; Flags: 428292; Action:
drop; Origin: MyGW; IfDir: <; InterfaceName: eth0; Alert: ; LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; inzone: Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_
table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid: 4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_
uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_table: TABLE_END; UP_action_table: TABLE_START; ROW_
START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc: ftp; sport_svc: 64933;
ProductFamily: Network;
[Expert@MyGW:0]#
```

Example 6 - Show only log entries from 0 to 10 (counting from the beginning of the log file)

```
[Expert@MyGW:0]# fw log -l -x 0 -y 10
... ...
[Expert@MyGW:0]#
```

fw logswitch

Description

Switches the current active log file:

1. Closes the current active log file.
2. Renames the current active log file.
3. Creates a new active log file with the default name.

Notes:

- By default, this command switches the active Security log file - `$FWDIR/log/fw.log`
- You can specify to switch the active Audit log file - `$FWDIR/log/fw.adtlog`

Important You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).

Syntax

```
fw [-d] logswitch
      [-audit] [<Name of Switched Log>]
      -h <Target> [[+ | -]<Name of Switched Log>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-audit`	Specifies to switch the active Audit log file (`$FWDIR/log/fw.adtlog`). You can use this parameter only on a Management Server.

Parameter	Description
`-h <Target>`	Specifies the remote server, on which to switch the log. **Notes:** ■ The local and the remote servers must have established SIC trust. ■ The local server can be a Security Management Server, a Log Server. ■ The remote server can be a Security Gateway, a Log Server, or a Security Management Server in High Availability deployment. ■ You can specify the remote managed server by its main IP address or Object Name as configured in SmartConsole.

`<Name of Switched Log>`	Specifies the name of the switched log file.
	Notes:
	■ If you do not specify this parameter, then a default name is:
	`<YYYY-MM-DD_HHMMSS>.log`
	`<YYYY-MM-DD_HHMMSS>.adtlog`
	For example, *2018-03-26_174455.log*
	■ If you specify the name of the switched log file, then the name of the switch log file is:
	`<Specified_Log_Name>.log`
	`<Specified_Log_Name>.adtlog`
	■ The log switch operation fails if the specified name for the switched log matches the name of an existing log file.
	■ The maximum length of the specified name of the switched log file is 230 characters.

`+`	Specifies to *copy* the active log from the remote server to the local server.
	Notes:
	■ If you specify the name of the switched log file, you must write it immediately after *this* + (plus) parameter.
	■ The command copies the active log from the remote server and saves it in the `$FWDIR/log/` directory on the local server.
	■ The default name of the saved log file is:
	`<Gateway_Object_Name>__<YYYY-MM-DD_HHMMSS>.log`
	For example, *MyGW__2018-03-26_174455.log*
	■ If you specify the name of the switched log file, then the name of the saved log file is:
	`<Gateway_Object_Name>__<Specified_Log_Name>.log`
	■ When this command copies the log file from the remote server, it compresses the file.

Parameter	Description
-	Specifies to *transfer* the active log from the remote server to the local server. **Notes:** ■ The command saves the copied active log file in the `$FWDIR/log/` directory on the local server and then deletes the switched log file on the remote server. ■ If you specify the name of the switched log file, you must write it immediately after this - (minus) parameter. ■ The default name of the saved log file is: `<Gateway_Object_Name>__<YYYY-MM-DD_HHMMSS>.log` For example, *MyGW__2018-03-26_174455.log* ■ If you specify the name of the switched log file, then the name of the saved log file is: `<Gateway_Object_Name>__<Specified_Log_Name>.log` ■ When this command transfers the log file from the remote server, it compresses the file. ■ As an alternative, you can use the *"fw fetchlogs" on page 268* command.

Compression

When this command transfers the log files from the remote server, it compresses the file with the `gzip` command (see RFC 1950 to RFC 1952 for details). The algorithm is a variation of LZ77 method. The compression ratio varies with the content of the log file and is difficult to predict. Binary data are not compressed. Text data, such as user names and URLs, are compressed.

Example - Switching the active Security log on a Security Management Server or Security Gateway

```
[Expert@MGMT:0]# fw logswitch
Log file has been switched to: 2018-06-13_182359.log
[Expert@MGMT:0]#
```

Example - Switching the active Audit log on a Security Management Server

```
[Expert@MGMT:0]# fw logswitch -audit
Log file has been switched to: 2018-06-13_185711.adtlog
[Expert@MGMT:0]#
```

Example - Switching the active Security log on a managed Security Gateway and copying the switched log

```
[Expert@MGMT:0]# fw logswitch -h MyGW +
Log file has been switched to: 2018-06-13_185451.log
[Expert@MGMT:0]#
[Expert@MGMT:0]# ls $FWDIR/log/*.log
/opt/CPsuite-R81.20/fw1/log/fw.log
/opt/CPsuite-R81.20/fw1/log/MyGW__2018-06-13_185451.log
[Expert@MGMT:0]#

[Expert@MyGW:0]# ls $FWDIR/log/*.log
/opt/CPsuite-R81.20/fw1/log/fw.log
/opt/CPsuite-R81.20/fw1/log/2018-06-13_185451.log
[Expert@MyGW:0]#
```

fw lslogs

Description

Shows a list of Security log files (`$FWDIR/log/*.log`) and Audit log files (`$FWDIR/log/*.adtlog`) residing on the local server or a remote server.

Important - You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).

Syntax

```
fw [-d] lslogs [-f <Name of Log File 1>] [-f <Name of Log File 2>]
... [-f <Name of Log File N>] [-e] [-r] [-s {name | size | stime |
etime}] [<Target>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-f <Name of Log File>`	Specifies the name of the log file to show. Need to specify only the name. **Notes:** ■ If the log file name is not specified explicitly, the command shows all Security log files (`$FWDIR/log/*.log`). ■ File names may include `*` and `?` as wildcards (for example, `2019-0?-*`). If you enter a wildcard, you must enclose it in double quotes or single quotes. ■ You can specify multiple log files in one command. You must use the "`-f`" parameter for each log file name pattern: `-f <Name of Log File 1> -f <Name of Log File 2> ... -f <Name of Log File N>`

Parameter	Description
`-e`	Shows an extended file list. It includes the following information for each log file: ■ `Size` - The total size of the log file and its related pointer files ■ `Creation Time` - The time the log file was created ■ `Closing Time` - The time the log file was closed ■ `Log File Name` - The file name
`-r`	Reverses the sort order (descending order).
`-s {name | size | stime | etime}`	Specifies the sort order of the log files using one of the following sort options: ■ `name` - The file name ■ `size` - The file size ■ `stime` - The time the log file was created (this is the default option) ■ `etime` - The time the log file was closed
<Target>	Specifies the remote Check Point server, with which this local Check Point server has established SIC trust. **Notes:** ■ The local and the remote servers must have established SIC trust. ■ The local server can be a Security Management Server, a Log Server, a Security Gateway, a Cluster Member. ■ The remote server can be a Security Gateway, a Cluster Member, a Log Server, or a Security Management Server in High Availability deployment. ■ You can specify the remote managed server by its main IP address or Object Name as configured in SmartConsole.

Example 1 - Default output

```
[Expert@HostName:0]# fw lslogs
     Size Log file name
         9KB 2019-06-14_000000.log
        11KB 2019-06-15_000000.log
         9KB 2019-06-16_000000.log
        10KB 2019-06-17_000000.log
         9KB fw.log
[Expert@HostName:0]#
```

Example 2 - Showing all log files

```
[Expert@HostName:0]# fw lslogs -f "*"
     Size Log file name
          9KB fw.adtlog
          9KB fw.log
          9KB 2019-05-29_000000.adtlog
          9KB 2019-05-29_000000.log
          9KB 2019-05-20_000000.adtlog
          9KB 2019-05-20_000000.log
[Expert@HostName:0]#
```

Example 3 - Showing only log files specified by the patterns

```
[Expert@HostName:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*'
     Size Log file name
          9KB 2019-06-14_000000.adtlog
          9KB 2019-06-14_000000.log
         11KB 2019-06-15_000000.adtlog
         11KB 2019-06-15_000000.log
[Expert@HostName:0]#
```

Example 4 - Showing only log files specified by the patterns and their extended information

```
[Expert@HostName:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*'
     Size Log file name
          9KB 2019-06-14_000000.adtlog
          9KB 2019-06-14_000000.log
         11KB 2019-06-15_000000.adtlog
         11KB 2019-06-15_000000.log
[Expert@HostName:0]#
```

Example 5 - Showing only log files specified by the patterns, sorting by name in reverse order

```
[Expert@HostName:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*' -e -s name -r
     Size Creation Time Closing Time Log file name
        11KB 14Jun2018 0:00:00 15Jun2018 0:00:00 2019-06-15_000000.log
        11KB 14Jun2018 0:00:00 15Jun2018 0:00:00 2019-06-15_000000.adtlog
         9KB 13Jun2018 18:23:59 14Jun2018 0:00:00 2019-06-14_000000.log
         9KB 13Jun2018 0:00:00 14Jun2018 0:00:00 2019-06-14_000000.adtlog
[Expert@HostName:0]#
```

Example 6 - Showing only log files specified by the patterns, from a managed Security Gateway with main IP address 192.168.3.53

```
[Expert@MGMT:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*' 192.168.3.53
     Size Log file name
        11KB 2019-06-15_000000.adtlog
        11KB 2019-06-15_000000.log
         9KB 2019-06-14_000000.log
         9KB 2019-06-14_000000.adtlog
[Expert@MGMT:0]#
```

fw mergefiles

Description

Merges several Security log files (`$FWDIR/log/*.log`) into a single log file.

Merges several Audit log files (`$FWDIR/log/*.adtlog`) into a single log file.

Important:

- Do **not** merge the *active* Security file `$FWDIR/log/fw.log` with other Security switched log files.
  Switch the active Security file `$FWDIR/log/fw.log` (with the *"fw logswitch" on page 1141* command) and only then merge it with other Security switched log files.
- Do **not** merge the *active* Audit file `$FWDIR/log/fw.adtlog` with other Audit switched log files.
  Switch the active Audit file `$FWDIR/log/fw.adtlog` (with the *"fw logswitch" on page 1141* command) and only then merge it with other Audit switched log files.
- This command unifies logs entries with the same Unique-ID (UID). If you rotate the current active log file before all the segments of a specific log arrive, this command merges the records with the same Unique ID from two different files, into one fully detailed record.
- If the size of the final merged log file exceeds 2GB, this command creates a list of merged files, where the size of each merged file size is not more than 2GB.
  The user receives this warning:

  ```
  Warning: The size of the files you have chosen to merge
  is greater than 2GB. The merge will produce two or more
  files.
  ```

  The names of merged files are:
  - *<Name of Merged Log File>*.log
  - *<Name of Merged Log File>*_1.log
  - *<Name of Merged Log File>*_2.log
  - ... ...
  - *<Name of Merged Log File>*_N.log

Important - You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).

Syntax

```
fw [-d] mergefiles {-h | -help}
```

```
fw [-d] mergefiles [-r] [-s] [-t <Time Conversion File>] <Name of Log File 1> <Name of Log File 2> ... <Name of Log File N> <Name of Merged Log File>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{-h | -help}`	Shows the built-in usage.
`-r`	Removes duplicate entries.
`-s`	Sorts the merged file by the **Time** field in log records.

`-t <Time Conversion File>`	Specifies a full path and name of a file that instructs this command how to adjust the times during the merge.
	This is required if you merge log files from Log Servers configured with different time zones.
	The file format is:
	`<IP Address of Log Server #1> <Signed Date Time #1 in Seconds>`
	`<IP Address of Log Server #2> <Signed Date Time #2 in Seconds>`
	`... ...`
	Notes
	■ You must specify the absolute path and the file name.
	■ The name of the time conversion file cannot exceed 230 characters.

Parameter	Description
<Name of Log File 1> ... <Name of Log File N>	Specifies the log files to merge. **Notes:** ■ You must specify the absolute path and the name of the input log files. ■ The name of the input log file cannot exceed 230 characters.
<Name of Merged Log File>	Specifies the output merged log file. **Notes:** ■ The name of the merged log file cannot exceed 230 characters. ■ If a file with the specified name already exists, the command stops and asks you to remove the existing file, or to specify another name. ■ The size of the merged log file cannot exceed 2 GB. In such scenario, the command creates several merged log files, each not exceeding the size limit.

Example - Merging Security log files

```
[Expert@HostName:0]# ls -l $FWDIR/*.log
-rw-rw-r-- 1 admin root 189497 Sep  7 00:00 2019-09-07_000000.log
-rw-rw-r-- 1 admin root  14490 Sep  9 09:52 2019-09-09_000000.log
-rw-rw-r-- 1 admin root  30796 Sep 10 10:56 2019-09-10_000000.log
-rw-rw-r-- 1 admin root  24503 Sep 10 13:08 fw.log
[Expert@HostName:0]#
[Expert@HostName:0]# fw mergefiles -s $FWDIR/2019-09-07_000000.log $FWDIR/2019-09-09_000000.log
$FWDIR/2019-09-10_000000.log /var/log/2019-Sep-Merged.log
[Expert@HostName:0]#
[Expert@HostName:0]# ls -l /var/log/2019-Sep-Merged.log*
-rw-rw---- 1 admin root 213688 Sep 10 13:18 /var/log/2019-Sep-Merged.log
-rw-rw---- 1 admin root   8192 Sep 10 13:18 /var/log/2019-Sep-Merged.logLuuidDB
-rw-rw---- 1 admin root     80 Sep 10 13:18 /var/log/2019-Sep-Merged.logaccount_ptr
-rw-rw---- 1 admin root   2264 Sep 10 13:18 /var/log/2019-Sep-Merged.loginitial_ptr
-rw-rw---- 1 admin root   4448 Sep 10 13:18 /var/log/2019-Sep-Merged.logptr
[Expert@HostName:0]#
```

fw repairlog

Description

Check Point Security log file (`$FWDIR/log/*.log`) and Audit log files (`$FWDIR/log/*.adtlog`) are databases, with special pointer files.

If these log pointer files become corrupted (which causes the inability to read the log file), this command can rebuild them.

Log File Type	Log File Location	Log Pointer Files

Security log	`$FWDIR/log/*.log`	`*.logptr`
		`*.logaccount_ptr`
		`*.loginitial_ptr`
		`*.logLuuidDB`

Audit log	`$FWDIR/log/*.adtlog`	`*.adtlogptr`
		`*.adtlogaccount_ptr`
		`*.adtloginitial_ptr`
		`*.adtlogLuuidDB`

Important - You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).

Syntax

```
fw [-d] repairlog [-u] <Name of Log File>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-u`	Specifies to rebuild the unification chains in the log file.
<Name of Log File>	The name of the log file to repair.

Example - Repairing the Audit log file

```
fw repairlog -u 2019-06-17_000000.adtlog
```

fw sam

Description

Manages the Suspicious Activity Monitoring (SAM) rules. You can use the SAM rules to block connections to and from IP addresses without the need to change or reinstall the Security Policy. For more information, see sk112061.

You can create the Suspicious Activity Rules in two ways:

- In SmartConsole from Monitoring Results
- In CLI with the `fw sam` command

Notes:

- VSX Gateways and VSX Cluster Members do not support Suspicious Activity Monitoring (SAM) Rules. See sk79700.
- See the "`fw sam_policy`" and "`sam_alert`" commands.
- SAM rules consume some CPU resources on Security Gateway.

  Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.
- Logs for enforced SAM rules (configured with the `fw sam` command) are stored in the `$FWDIR/log/sam.dat` file.
  By design, the file is purged when the number of stored entries reaches 100,000.
  This data log file contains the records in one of these formats:

`<type>,<actions>,<expire>,<ipaddr>`
`<type>,<actions>,<expire>,<src>,<dst>,<dport>,<ip_p>`

- SAM Requests are stored on the Security Gateway in the kernel table `sam_requests`.
- IP Addresses that are blocked by SAM rules, are stored on the Security Gateway in the kernel table `sam_blocked_ips`.

Note - To configure SAM Server settings for a Security Gateway or Cluster:

1. Connect with SmartConsole to the applicable Security Management Server or Domain Management Server.
2. From the left navigation panel, click Gateways & Servers.
3. Open the Security Gateway or Cluster object.
4. From the left tree, click **Other > SAM**.
5. Configure the settings.
6. Click **OK**.
7. Install the Access Control Policy on this Security Gateway or Cluster object.

Syntax

- **To add or cancel a SAM rule according to criteria:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM
Server>] [-f <Security Gateway>] [-t <Timeout>] [-l <Log
Type>] [-C] [-e <key=val>]+ [-r] -{n|i|I|j|J} <Criteria>
```

- **To delete all SAM rules:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM
Server>] [-f <Security Gateway>] -D
```

- **To monitor all SAM rules:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM
Server>] [-f <Security Gateway>] [-r] -M -{i|j|n|b|q} all
```

- **To monitor SAM rules according to criteria:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM
Server>] [-f <Security Gateway>] [-r] -M -{i|j|n|b|q}
<Criteria>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-v`	Enables verbose mode. In this mode, the command writes one message to *stderr* for each Security Gateway, on which the command is enforced. These messages show whether the command was successful or not.
`-s <SAM Server>`	Specifies the IP address (in the X.X.X.X format) or resolvable HostName of the Security Gateway that enforces the command. The default is `localhost`.

Parameter	Description
`-S <SIC Name of SAM Server>`	Specifies the SIC name for the SAM server to be contacted. It is expected that the SAM server has this SIC name, otherwise the connection fails. **Notes:** ■ If you do not explicitly specify the SIC name, the connection continues without SIC names comparison. ■ For more information about enabling SIC, refer to the OPSEC API Specification. ■ On VSX Gateway, run the *fw vsx showncs -vs <VSID>* command to show the SIC name for the applicable Virtual System.
`-f <Security Gateway>`	Specifies the Security Gateway, on which to enforce the action. `<Security Gateway>` can be one of these: ■ *All* - Default. Specifies to enforce the action on all managed Security Gateways, where SAM Server runs. You can use this syntax only on Security Management Server or Domain Management Server. ■ *localhost* - Specifies to enforce the action on this local Check Point server (on which the `fw sam` command is executed). You can use this syntax only on Security Gateway or StandAlone. ■ *Gateways* - Specifies to enforce the action on all objects defined as Security Gateways, on which SAM Server runs. You can use this syntax only on Security Management Server or Domain Management Server. ■ *Name of Security Gateway object* - Specifies to enforce the action on this specific Security Gateway object. You can use this syntax only on Security Management Server or Domain Management Server. ■ *Name of Group object* - Specifies to enforce the action on all specific Security Gateways in this Group object. **Notes:** ■ You can use this syntax only on Security Management Server or Domain Management Server. ■ VSX Gateways and VSX Cluster Members do not support Suspicious Activity Monitoring (SAM) Rules. See sk79700.
`-D`	Cancels all inhibit ("`-i`", "`-j`", "`-I`", "`-J`") and notify ("`-n`") parameters. **Notes:** ■ To "uninhibit" the inhibited connections, run the `fw sam` command with the "`-C`" or "`-D`" parameters. ■ It is also possible to use this command for active SAM requests.

Parameter	Description
`-C`	Cancels the `fw sam` command to inhibit connections with the specified parameters. **Notes:** ■ These connections are no longer inhibited (no longer rejected or dropped). ■ The command parameters must match the parameters in the original `fw sam` command, except for the `-t <Timeout>` parameter.
`-t <Timeout>`	Specifies the time period (in seconds), during which the action is enforced. The default is forever, or until you cancel the `fw sam` command.
`-l <Log Type>`	Specifies the type of the log for enforced action: ■ `nolog` - Does not generate Log / Alert at all ■ `short_noalert` - Generates a Log ■ `short_alert` - Generates an Alert ■ `long_noalert` - Generates a Log ■ `long_alert` - Generates an Alert (this is the default)
`-e <key=val>+`	Specifies rule information based on the keys and the provided values. Multiple keys are separated by the plus sign (+). Available keys are (each is limited to 100 characters): ■ `name` - Security rule name ■ `comment` - Security rule comment ■ `originator` - Security rule originator's username
`-r`	Specifies not to resolve IP addresses.
`-n`	Specifies to generate a "Notify" long-format log entry. **Notes:** ■ This parameter generates an alert when connections that match the specified services or IP addresses pass through the Security Gateway. ■ This action does not inhibit / close connections.
`-i`	Inhibits (drops or rejects) new connections with the specified parameters. **Notes:** ■ Each inhibited connection is logged according to the log type. ■ Matching connections are rejected.

Parameter	Description
`-I`	Inhibits (drops or rejects) new connections with the specified parameters, and closes all existing connections with the specified parameters. **Notes:** ■ Matching connections are rejected. ■ Each inhibited connection is logged according to the log type.
`-j`	Inhibits (drops or rejects) new connections with the specified parameters. **Notes:** ■ Matching connections are dropped. ■ Each inhibited connection is logged according to the log type.
`-J`	Inhibits new connections with the specified parameters, and closes all existing connections with the specified parameters. **Notes:** ■ Matching connections are dropped. ■ Each inhibited connection is logged according to the log type.
`-b`	Bypasses new connections with the specified parameters.
`-q`	Quarantines new connections with the specified parameters.
`-M`	Monitors the active SAM requests with the specified actions and criteria.
`all`	Gets all active SAM requests. This is used for monitoring purposes only.
`<Criteria>`	Criteria are used to match connections. The criteria and are composed of various combinations of the following parameters: ■ Source IP Address ■ Source Netmask ■ Destination IP Address ■ Destination Netmask ■ Port (see *IANA Service Name and Port Number Registry*) ■ Protocol Number (see *IANA Protocol Numbers*)

Parameter	Description
	Possible combinations are (see the explanations below this table): ■ src *<IP>* ■ dst *<IP>* ■ any *<IP>* ■ subsrc *<IP> <Netmask>* ■ subdst *<IP> <Netmask>* ■ subany *<IP> <Netmask>* ■ srv *<Src IP> <Dest IP> <Port> <Protocol>* ■ subsrv *<Src IP> <Src Netmask> <Dest IP> <Dest Netmask> <Port> <Protocol>* ■ subsrvs *<Src IP> <Src Netmask> <Dest IP> <Port> <Protocol>* ■ subsrvd *<Src IP> <Dest IP> <Dest Netmask> <Port> <Protocol>* ■ dstsrv *<Dest IP> <Port> <Protocol>* ■ subdstsrv *<Dest IP> <Dest Netmask> <Port> <Protocol>* ■ srcpr *<IP> <Protocol>* ■ dstpr *<IP> <Protocol>* ■ subsrcpr *<IP> <Netmask> <Protocol>* ■ subdstpr *<IP> <Netmask> <Protocol>* ■ generic *<key=val>*

Explanation for the *<Criteria>* syntax

Parameter	Description
src *<IP>*	Matches the Source IP address of the connection.
dst <IP>	Matches the Destination IP address of the connection.
any *<IP>*	Matches either the Source IP address or the Destination IP address of the connection.
subsrc *<IP> <Netmask>*	Matches the Source IP address of the connections according to the netmask.
subdst *<IP> <Netmask>*	Matches the Destination IP address of the connections according to the netmask.

Parameter	Description
`subany <IP> <Netmask>`	Matches either the Source IP address or Destination IP address of connections according to the netmask.
`srv <Src IP> <Dest IP> <Port> <Protocol>`	Matches the specific Source IP address, Destination IP address, Service (port number) and Protocol.
`subsrv <Src IP> <Netmask> <Dest IP> <Netmask> <Port> <Protocol>`	Matches the specific Source IP address, Destination IP address, Service (port number) and Protocol. Source and Destination IP addresses are assigned according to the netmask.
`subsrvs <Src IP> <Src Netmask> <Dest IP> <Port> <Protocol>`	Matches the specific Source IP address, source netmask, destination netmask, Service (port number) and Protocol.
`subsrvd <Src IP> <Dest IP> <Dest Netmask> <Port> <Protocol>`	Matches specific Source IP address, Destination IP, destination netmask, Service (port number) and Protocol.
`dstsrv <Dest IP> <Service> <Protocol>`	Matches specific Destination IP address, Service (port number) and Protocol.
`subdstsrv <Dest IP> <Netmask> <Port> <Protocol>`	Matches specific Destination IP address, Service (port number) and Protocol. Destination IP address is assigned according to the netmask.
`srcpr <IP> <Protocol>`	Matches the Source IP address and protocol.
`dstpr <IP> <Protocol>`	Matches the Destination IP address and protocol.
`subsrcpr <IP> <Netmask> <Protocol>`	Matches the Source IP address and protocol of connections. Source IP address is assigned according to the netmask.
`subdstpr <IP> <Netmask> <Protocol>`	Matches the Destination IP address and protocol of connections. Destination IP address is assigned according to the netmask.

Parameter	Description
`generic <key=val>+`	Matches the GTP connections based on the specified keys and provided values. Multiple keys are separated by the plus sign (+). Available keys are: ■ `service=gtp` ■ `imsi` ■ `msisdn` ■ `apn` ■ `tunl_dst` ■ `tunl_dport` ■ `tunl_proto`

fw sam_policy

Description

Manages the Suspicious Activity Policy editor that works with these types of rules:

- Suspicious Activity Monitoring (SAM) rules.

  See sk112061: How to create and view Suspicious Activity Monitoring (SAM) Rules.

- Rate Limiting rules.

  See sk112454: How to configure Rate Limiting rules for DoS Mitigation.

Also, see these commands:

- *"fw sam" on page 295*
- *"sam_alert" on page 405*

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax for IPv4

```
fw [-d] sam_policy
      add <options>
      batch
      del <options>
      get <options>
```

```
fw [-d] samp
      add <options>
      batch
      del <options>
      get <options>
```

Syntax for IPv6

```
fw6 [-d] sam_policy
      add <options>
      batch
      del <options>
      get <options>
```

```
fw6 [-d] samp
      add <options>
      batch
      del <options>
      get <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`add <options>`	Adds one Rate Limiting rule one at a time. See *"fw sam_policy add" on page 306*.
`batch`	Adds or deletes many Rate Limiting rules at a time. See *"fw sam_policy batch" on page 319*.
`del <options>`	Deletes one configured Rate Limiting rule one at a time. See *"fw sam_policy del" on page 321*.
`get <options>`	Shows all the configured Rate Limiting rules. See *"fw sam_policy get" on page 324*.

fw sam_policy add

Description

The "*fw sam_policy add*" and "*fw6 sam_policy add*" commands:

- Add one Suspicious Activity Monitoring (SAM) rule at a time.
- Add one Rate Limiting rule at a time.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax to configure a Suspicious Activity Monitoring (SAM) rule for IPv4

```
fw [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] ip <IP Filter Arguments>
```

Syntax to configure a Suspicious Activity Monitoring (SAM) rule for IPv6

```
fw6 [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] ip <IP Filter Arguments>
```

Syntax to configure a Rate Limiting rule for IPv4

```
fw [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] quota <Quota Filter Arguments>
```

Syntax to configure a Rate Limiting rule for IPv6

```
fw6 [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] quota <Quota Filter Arguments
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-u`	Optional. Specifies that the rule category is `User-defined`. Default rule category is `Auto`.
`-a {d | n | b}`	Mandatory. Specifies the rule action if the traffic matches the rule conditions: ■ `d` - Drop the connection. ■ `n` - Notify (generate a log) about the connection and let it through. ■ `b` - Bypass the connection - let it through without checking it against the policy rules. **Note** - Rules with action set to *Bypass* cannot have a log or limit specification. Bypassed packets and connections do not count towards overall number of packets and connection for limit enforcement of type ratio.
`-l {r | a}`	Optional. Specifies which type of log to generate for this rule for all traffic that matches: ■ `-r` - Generate a regular log ■ `-a` - Generate an alert log

Parameter	Description
`-t <Timeout>`	Optional. Specifies the time period (in seconds), during which the rule will be enforced. Default timeout is indefinite.
`-f <Target>`	Optional. Specifies the target Security Gateways, on which to enforce the Rate Limiting rule. `<Target>` can be one of these: ■ `all` - This is the default option. Specifies that the rule should be enforced on all managed Security Gateways. ■ Name of the Security Gateway or Cluster object - Specifies that the rule should be enforced only on this Security Gateway or Cluster object (the object name must be as defined in the SmartConsole). ■ Name of the Group object - Specifies that the rule should be enforced on all Security Gateways that are members of this Group object (the object name must be as defined in the SmartConsole).
`-n "<Rule Name>"`	Optional. Specifies the name (label) for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters. ■ Before each space or a backslash character in this string, you must write a backslash (\) character. Example: `"This\ is\ a\ rule\ name\ with\ a\ backslash\ \\"`
`-c "<Rule Comment>"`	Optional. Specifies the comment for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters. ■ Before each space or a backslash character in this string, you must write a backslash (\) character. Example: `"This\ is\ a\ comment\ with\ a\ backslash\ \\"`

Parameter	Description
`-o "<Rule Originator>"`	Optional. Specifies the name of the originator for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters. ■ Before each space or a backslash character in this string, you must write a backslash (\) character. Example: `"Created\ by\ John\ Doe"`
`-z "<Zone>"`	Optional. Specifies the name of the Security Zone for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters.
`ip <IP Filter Arguments>`	Mandatory (use this `ip` parameter, or the `quota` parameter). Configures the *Suspicious Activity Monitoring (SAM)* rule. Specifies the IP Filter Arguments for the SAM rule (you must use at least one of these options): `[-C] [-s <Source IP>] [-m <Source Mask>] [-d <Destination IP>] [-M <Destination Mask>] [-p <Port>] [-r <Protocol>]` See the explanations below.

Parameter	Description
`quota <Quota Filter Arguments>`	Mandatory (use this `quota` parameter, or the `ip` parameter). Configures the *Rate Limiting* rule. Specifies the Quota Filter Arguments for the Rate Limiting rule (see the explanations below): ■ `[flush true]` ■ `[source-negated {true | false}] source <Source>` ■ `[destination-negated {true | false}] destination <Destination>` ■ `[service-negated {true | false}] service <Protocol and Port numbers>` ■ `[<Limit1 Name> <Limit1 Value>] [<Limit2 Name> <Limit2 Value>] ...[<LimitN Name> <LimitN Value>]` ■ `[track <Track>]` **Important:** ■ The Quota rules are not applied immediately to the Security Gateway. They are only registered in the Suspicious Activity Monitoring (SAM) policy database. To apply all the rules from the SAM policy database immediately, add "`flush true`" in the `fw samp add` command syntax. ■ Explanation: For new connections rate (and for any rate limiting in general), when a rule's limit is violated, the Security Gateway also drops all packets that match the rule. The Security Gateway computes new connection rates on a per-second basis. At the start of the 1-second timer, the Security Gateway allows all packets, including packets for existing connections. If, at some point, during that 1 second period, there are too many new connections, then the Security Gateway blocks all remaining packets for the remainder of that 1-second interval. At the start of the next 1-second interval, the counters are reset, and the process starts over - the Security Gateway allows packets to pass again up to the point, where the rule's limit is violated.

Explanation for the *IP Filter Arguments* syntax for Suspicious Activity Monitoring (SAM) rules

Argument	Description
`-C`	Specifies that open connections should be closed.
`-s <Source IP>`	Specifies the Source IP address.
`-m <Source Mask>`	Specifies the Source subnet mask (in dotted decimal format - x.y.z.w).
`-d <Destination IP>`	Specifies the Destination IP address.
`-M <Destination Mask>`	Specifies the Destination subnet mask (in dotted decimal format - x.y.z.w).
`-p <Port>`	Specifies the port number (see *IANA Service Name and Port Number Registry*).
`-r <Protocol>`	Specifies the protocol number (see *IANA Protocol Numbers*).

Explanation for the *Quota Filter Arguments* syntax for Rate Limiting rules

Argument	Description
`flush true`	Specifies to compile and load the quota rule to the SecureXL immediately.
`[source-negated {true | false}] source <Source>`	Specifies the source type and its value: ■ `any` The rule is applied to packets sent from all sources. ■ `range:<IP Address>` or `range:<IP Address Start>-<IP Address End>` The rule is applied to packets sent from: • Specified IPv4 addresses (x.y.z.w) • Specified IPv6 addresses (xxxx:yyyy:....:zzzz) ■ `cidr:<IP Address>/<Prefix>` The rule is applied to packets sent from: • IPv4 address with Prefix from 0 to 32 • IPv6 address with Prefix from 0 to 128 ■ `cc:<Country Code>` The rule matches the country code to the source IP addresses assigned to this country, based on the Geo IP database. The two-letter codes are defined in ISO 3166-1 alpha-2. ■ `asn:<Autonomous System Number>` The rule matches the AS number of the organization to the source IP addresses that are assigned to this organization, based on the Geo IP database. The valid syntax is *ASnnnn*, where *nnnn* is a number unique to the specific organization. **Notes:** ■ Default is: `source-negated false` ■ The `source-negated true` processes all source types, *except* the specified type.

Argument	Description
`[destination-negated {true | false}] destination <Destination>`	Specifies the destination type and its value: ■ `any` The rule is applied to packets sent to all destinations. ■ `range:<IP Address>` or `range:<IP Address Start>-<IP Address End>` The rule is applied to packets sent to: • Specified IPv4 addresses (x.y.z.w) • Specified IPv6 addresses (xxxx:yyyy:...:zzzz) ■ `cidr:<IP Address>/<Prefix>` The rule is applied to packets sent to: • IPv4 address with Prefix from 0 to 32 • IPv6 address with Prefix from 0 to 128 ■ `cc:<Country Code>` The rule matches the country code to the destination IP addresses assigned to this country, based on the Geo IP database. The two-letter codes are defined in ISO 3166-1 alpha-2. ■ `asn:<Autonomous System Number>` The rule matches the AS number of the organization to the destination IP addresses that are assigned to this organization, based on the Geo IP database. The valid syntax is *ASnnnn*, where *nnnn* is a number unique to the specific organization. **Notes:** ■ Default is: `destination-negated false` ■ The `destination-negated true` will process all destination types except the specified type

Argument	Description
`[service-negated {true | false}] service <Protocol and Port numbers>`	Specifies the Protocol number (see *IANA Protocol Numbers*) and Port number (see *IANA Service Name and Port Number Registry*): ■ `<Protocol>` IP protocol number in the range 1-255 ■ `<Protocol Start>-<Protocol End>` Range of IP protocol numbers ■ `<Protocol>/<Port>` IP protocol number in the range 1-255 and TCP/UDP port number in the range 1-65535 ■ `<Protocol>/<Port Start>-<Port End>` IP protocol number and range of TCP/UDP port numbers from 1 to 65535 **Notes:** ■ Default is: `service-negated false` ■ The `service-negated true` will process all traffic except the traffic with the specified protocols and ports

Argument	Description
`[<Limit 1 Name> <Limit 1 Value>] [<Limit 2 Name> <Limit 2 Value>] ... [<Limit N Name> <Limit N Value>]`	Specifies quota limits and their values. **Note** - Separate multiple quota limits with spaces. ■ `concurrent-conns <Value>` Specifies the maximal number of concurrent active connections that match this rule. ■ `concurrent-conns-ratio <Value>` Specifies the maximal ratio of the *concurrent-conns* value to the total number of active connections through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`). ■ `pkt-rate <Value>` Specifies the maximum number of packets per second that match this rule. ■ `pkt-rate-ratio <Value>` Specifies the maximal ratio of the *pkt-rate* value to the rate of all connections through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`). ■ `byte-rate <Value>` Specifies the maximal total number of bytes per second in packets that match this rule. ■ `byte-rate-ratio <Value>` Specifies the maximal ratio of the *byte-rate* value to the bytes per second rate of all connections through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`). ■ `new-conn-rate <Value>` Specifies the maximal number of connections per second that match the rule. ■ `new-conn-rate-ratio <Value>` Specifies the maximal ratio of the *new-conn-rate* value to the rate of all connections per second through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`).

Argument	Description
`[track <Track>]`	Specifies the tracking option: ■ `source` Counts connections, packets, and bytes for specific source IP address, and not cumulatively for this rule. ■ `source-service` Counts connections, packets, and bytes for specific source IP address, and for specific IP protocol and destination port, and not cumulatively for this rule.

Examples

Example 1 - Rate Limiting rule with a range

```
fw sam_policy add -a d -l r -t 3600 quota service any source range:172.16.7.11-172.16.7.13 new-conn-rate 5 flush true
```

Explanations:

- This rule drops packets for all connections (`-a d`) that exceed the quota set by this rule, including packets for existing connections.
- This rule logs packets (`-l r`) that exceed the quota set by this rule.
- This rule will expire in 3600 seconds (`-t 3600`).
- This rule limits the rate of creation of new connections to 5 connections per second (`new-conn-rate 5`) for any traffic (`service any`) from the source IP addresses in the range 172.16.7.11 - 172.16.7.13 (`source range:172.16.7.11-172.16.7.13`).

  Note - The limit of the total number of log entries per second is configured with the *fwaccel dos config set -n <rate>* command.
- This rule will be compiled and loaded on the SecureXL, together with other rules in the Suspicious Activity Monitoring (SAM) policy database immediately, because this rule includes the "`flush true`" parameter.

Example 2 - Rate Limiting rule with a service specification

```
fw sam_policy add -a n -l r quota service 1,50-51,6/443,17/53 service-negated true source cc:QQ byte-rate 0
```

Explanations:

- This rule logs and lets through all packets (`-a n`) that exceed the quota set by this rule.
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to all packets except (`service-negated true`) the packets with IP protocol number 1, 50-51, 6 port 443 and 17 port 53 (`service 1,50-51,6/443,17/53`).
- This rule applies to all packets from source IP addresses that are assigned to the country with specified country code (`cc:QQ`).
- This rule does not let any traffic through (`byte-rate 0`) except the packets with IP protocol number 1, 50-51, 6 port 443 and 17 port 53.
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

Example 3 - Rate Limiting rule with ASN

```
fw sam_policy -a d quota source asn:AS64500,cidr:[::FFFF:C0A8:1100]/120 service any pkt-rate 0
```

Explanations:

- This rule drops (`-a d`) all packets that match this rule.
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to packets from the Autonomous System number 64500 (`asn:AS64500`).
- This rule applies to packets from source IPv6 addresses FFFF:C0A8:1100/120 (`cidr:[::FFFF:C0A8:1100]/120`).
- This rule applies to all traffic (`service any`).
- This rule does not let any traffic through (`pkt-rate 0`).
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

Example 4 - Rate Limiting rule with an Allow List

```
fw sam_policy add -a b quota source range:172.16.8.17-172.16.9.121 service 6/80
```

Explanations:

- This rule bypasses (`-a b`) all packets that match this rule.

  Note - The Access Control Policy and other types of security policy rules still apply.
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to packets from the source IP addresses in the range 172.16.8.17 - 172.16.9.121 (`range:172.16.8.17-172.16.9.121`).
- This rule applies to packets sent to TCP port 80 (`service 6/80`).
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

Example 5 - Rate Limiting rule with tracking

```
fw sam_policy add -a d quota service any source-negated true source cc:QQ concurrent-conns-ratio 655 track source
```

Explanations:

- This rule drops (`-a d`) all packets that match this rule.
- This rule does not log any packets (the `-l r` parameter is not specified).
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to all traffic (`service any`).
- This rule applies to all sources except (`source-negated true`) the source IP addresses that are assigned to the country with specified country code (`cc:QQ`).
- This rule limits the maximal number of concurrent active connections to 655/65536=~1% (`concurrent-conns-ratio 655`) for any traffic (`service any`) except (`service-negated true`) the connections from the source IP addresses that are assigned to the country with specified country code (`cc:QQ`).
- This rule counts connections, packets, and bytes for traffic only from sources that match this rule, and not cumulatively for this rule.
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

fw sam_policy batch

Description

The "*fw sam_policy batch*" and "*fw6 sam_policy batch*" commands:

- Add and delete many Suspicious Activity Monitoring (SAM) rules at a time.
- Add and delete many Rate Limiting rules at a time.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Procedure

1. **Start the batch mode**

   - For IPv4, run:

     ```
     fw sam_policy batch << EOF
     ```

   - For IPv6, run:

     ```
     fw6 sam_policy batch << EOF
     ```

2. **Enter the applicable commands**

   - Enter one "`add`" or "`del`" command on each line, on as many lines as necessary.

     Start each line with only "`add`" or "`del`" parameter (not with "`fw samp`").
   - Use the same set of parameters and values as described in these commands:
     - `fw sam_policy add`
     - `fw sam_policy del`
   - Terminate each line with a Return (ASCII 10 - Line Feed) character (press Enter).

3. **End the batch mode**

   Type `EOF` and press Enter.

Example of a Rate Limiting rule for IPv4

```
[Expert@HostName]# fw samp batch <<EOF

add -a d -l r -t 3600 -c "Limit\ conn\ rate\ to\ 5\ conn/sec from\ these\ sources" quota service
any source range:172.16.7.13-172.16.7.13 new-conn-rate 5

del <501f6ef0,00000000,cb38a8c0,0a0afffe>

add -a b quota source range:172.16.8.17-172.16.9.121 service 6/80

EOF
[Expert@HostName]#
```

fw sam_policy del

Description

The "*fw sam_policy del*" and "*fw6 sam_policy del*" commands:

- Delete one configured Suspicious Activity Monitoring (SAM) rule at a time.
- Delete one configured Rate Limiting rule at a time.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax for IPv4

```
fw [-d] sam_policy del '<Rule UID>'
```

Syntax for IPv6

```
fw6 [-d] sam_policy del '<Rule UID>'
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`'<Rule UID>'`	Specifies the UID of the rule you wish to delete. **Important:** ■ The quote marks and angle brackets (`'<...>'`) are mandatory. ■ To see the Rule UID, run the "`fw sam_policy get`" command.

Procedure

1. **List all the existing rules in the Suspicious Activity Monitoring policy database**

   List all the existing rules in the Suspicious Activity Monitoring policy database.

   - For IPv4, run:

     ```
     fw sam_policy get
     ```

   - For IPv6, run:

     ```
     fw6 sam_policy get
     ```

   The rules show in this format:

   ```
   operation=add uid=<Value1,Value2,Value3,Value4> target=...
   timeout=... action=... log= ... name= ... comment=...
   originator= ... src_ip_addr=... req_tpe=...
   ```

   Example for IPv4:

   ```
   operation=add uid=<5ac3965f,00000000,3403a8c0,0000264a>
   target=all timeout=300 action=notify log=log name=Test\ Rule
   comment=Notify\ about\ traffic\ from\ 1.1.1.1
   originator=John\ Doe src_ip_addr=1.1.1.1 req_tpe=ip
   ```

2. **Delete a rule from the list by its UID**

   - For IPv4, run:

     ```
     fw [-d] sam_policy del '<Rule UID>'
     ```

   - For IPv6, run:

     ```
     fw6 [-d] sam_policy del '<Rule UID>'
     ```

   Example for IPv4:

   ```
   fw samp del '<5ac3965f,00000000,3403a8c0,0000264a>'
   ```

3. **Add the flush-only rule**

   - For IPv4, run:

     ```
     fw samp add -t 2 quota flush true
     ```

   - For IPv6, run:

     ```
     fw6 samp add -t 2 quota flush true
     ```

   Explanation:

   The "`fw samp del`" and "`fw6 samp del`" commands only remove a rule from the persistent database. The Security Gateway continues to enforce the deleted rule until the next time you compiled and load a policy. To force the rule deletion immediately, you must enter a flush-only rule right after the "`fw samp del`" and "`fw6 samp del`" command. This flush-only rule immediately deletes the rule you specified in the previous step, and times out in 2 seconds.

   Best Practice - Specify a short timeout period for the flush-only rules. This prevents accumulation of rules that are obsolete in the database.

fw sam_policy get

Description

The "*fw sam_policy get*" and "*fw6 sam_policy get*" commands:

- Show all the configured Suspicious Activity Monitoring (SAM) rules.
- Show all the configured Rate Limiting rules.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax for IPv4

```
fw [-d] sam_policy get [-l] [-u '<Rule UID>'] [-k '<Key>' -t
<Type> [+{-v '<Value>'}] [-n]]
```

Syntax for IPv6

```
fw6 [-d] sam_policy get [-l] [-u '<Rule UID>'] [-k '<Key>' -t
<Type> [+{-v '<Value>'}] [-n]]
```

Parameters

Note - All these parameters are optional.

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-l`	Controls how to print the rules: ■ In the default format (without "`-l`"), the output shows each rule on a separate line. ■ In the list format (with "`-l`"), the output shows each parameter of a rule on a separate line. ■ See the "`fw sam_policy add`" command.
`-u '<`*`Rule UID`*`>'`	Prints the rule specified by its Rule UID or its zero-based rule index. The quote marks and angle brackets ('<...>') are mandatory.
`-k '<`*`Key`*`>'`	Prints the rules with the specified predicate key. The quote marks are mandatory.
`-t <`*`Type`*`>`	Prints the rules with the specified predicate type. For Rate Limiting rules, you must always use "`-t in`".
`+{-v '<`*`Value`*`>'}`	Prints the rules with the specified predicate values. The quote marks are mandatory.
`-n`	Negates the condition specified by these predicate parameters: ■ `-k` ■ `-t` ■ `+-v`

Examples

Example 1 - Output in the default format

```
[Expert@HostName:0]# fw samp get

operation=add uid=<5ac3965f,00000000,3403a8c0,0000264a> target=all timeout=300 action=notify
log=log name=Test\ Rule comment=Notify\ about\ traffic\ from\ 1.1.1.1 originator=John\ Doe
src_ip_addr=1.1.1.1 req_tpe=ip
```

Example 2 - Output in the list format

```
[Expert@HostName:0]# fw samp get -l

uid
<5ac3965f,00000000,3403a8c0,0000264a>
target
all
timeout
2147483647
action
notify
log
log
name
Test\ Rule
comment
Notify\ about\ traffic\ from\ 1.1.1.1
originator
John\ Doe
src_ip_addr
1.1.1.1
req_type
ip
```

Example 3 - Printing a rule by its Rule UID

```
[Expert@HostName:0]# fw samp get -u '<5ac3965f,00000000,3403a8c0,0000264a>'
0
operation=add uid=<5ac3965f,00000000,3403a8c0,0000264a> target=all timeout=300 action=notify
log=log name=Test\ Rule comment=Notify\ about\ traffic\ from\ 1.1.1.1 originator=John\ Doe
src_ip_addr=1.1.1.1 req_tpe=ip
```

Example 4 - Printing rules that match the specified filters

```
[Expert@HostName:0]# fw samp get
no corresponding SAM policy requests
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a d -l r -t 3600 quota service any source
range:172.16.7.11-172.16.7.13 new-conn-rate 5 flush true
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a n -l r quota service 1,50-51,6/443,17/53 service-negated
true source cc:QQ byte-rate 0
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a b quota source range:172.16.8.17-172.16.9.121 service
6/80
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a d quota service any source-negated true source cc:QQ
concurrent-conns-ratio 655 track source
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get
operation=add uid=<5bab3acf,00000000,3503a8c0,00003ddc> target=all timeout=indefinite
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
operation=add uid=<5bab3ac6,00000000,3503a8c0,00003dbf> target=all timeout=3586 action=drop
log=log service=any source=range:172.16.7.11-172.16.7.13 new-conn-rate=5 flush=true req_
type=quota
operation=add uid=<5bab3acc,00000000,3503a8c0,00003dd7> target=all timeout=indefinite
action=bypass source=range:172.16.8.17-172.16.9.121 service=6/80 req_type=quota
operation=add uid=<5bab3ac9,00000000,3503a8c0,00003dd5> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'service' -t in -v '6/80'
operation=add uid=<5bab3acc,00000000,3503a8c0,00003dd7> target=all timeout=indefinite
action=bypass source=range:172.16.8.17-172.16.9.121 service=6/80 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'service-negated' -t in -v 'true'
operation=add uid=<5bab3ac9,00000000,3503a8c0,00003dd5> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'source' -t in -v 'cc:QQ'
operation=add uid=<5bab3acf,00000000,3503a8c0,00003ddc> target=all timeout=indefinite
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
operation=add uid=<5bab3ac9,00000000,3503a8c0,00003dd5> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k source -t in -v 'cc:QQ' -n
operation=add uid=<5bab3ac6,00000000,3503a8c0,00003dbf> target=all timeout=3291 action=drop
log=log service=any source=range:172.16.7.11-172.16.7.13 new-conn-rate=5 flush=true req_
type=quota
operation=add uid=<5bab3acc,00000000,3503a8c0,00003dd7> target=all timeout=indefinite
action=bypass source=range:172.16.8.17-172.16.9.121 service=6/80 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'source-negated' -t in -v 'true'
operation=add uid=<5baa94e0,00000000,860318ac,00003016> target=all timeout=indefinite
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'byte-rate' -t in -v '0'
operation=add uid=<5baa9431,00000000,860318ac,00002efd> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'flush' -t in -v 'true'
operation=add uid=<5baa9422,00000000,860318ac,00002eea> target=all timeout=2841 action=drop
log=log service=any source=range:172.16.7.11-172.16.7.13 new-conn-rate=5 flush=true req_
type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'concurrent-conns-ratio' -t in -v '655'
operation=add uid=<5baa94e0,00000000,860318ac,00003016> target=all timeout=indefinite
```

```
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
[Expert@HostName:0]#
```

fwm

Description

Performs various management operations and shows various management information.

Notes:

- For debug instructions, see the description of the `fwm` process in sk97638.
- On a Multi-Domain Server, you must run these commands in the context of the applicable Domain Management Server.

Syntax

```
fwm [-d]
      dbload <options>
      exportcert <options>
      fetchfile <options>
      fingerprint <options>
      getpcap <options>
      ikecrypt <options>
      load [<options>]
      logexport <options>
      mds <options>
      printcert <options>
      sic_reset
      snmp_trap <options>
      unload [<options>]
      ver [<options>]
      verify <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.

Parameter	Description
`dbload <options>`	Downloads the user database and network objects information to the specified targets See *"fwm dbload" on page 333*.
`exportcert <options>`	Export a SIC certificate of the specified object to file. See *"fwm exportcert" on page 334*.
`fetchfile <options>`	Fetches a specified OPSEC configuration file from the specified source server. See *"fwm fetchfile" on page 335*.
`fingerprint <options>`	Shows the Check Point fingerprint. See *"fwm fingerprint" on page 337*.
`getpcap <options>`	Fetches the IPS packet capture data from the specified Security Gateway. See *"fwm getpcap" on page 339*.
`ikecrypt <options>`	Encrypts a secret with a key. See *"fwm ikecrypt" on page 341*.
`load <options>`	This command is obsolete for R80 and higher. Use the *"mgmt_cli" on page 386* command to load a policy to a managed Security Gateway. See *"fwm load" on page 342*.
`logexport <options>`	Exports a Security log file (`$FWDIR/log/*.log`) or Audit log file (`$FWDIR/log/*.adtlog`) to an ASCII file. See *"fwm logexport" on page 343*.
`mds <options>`	Shows information and performs various operations on Multi-Domain Server. See *"fwm mds" on page 348*.
`printcert <options>`	Shows a SIC certificate's details. See *"fwm printcert" on page 350*.
`sic_reset`	Resets SIC on the Management Server. See *"fwm sic_reset" on page 356*.
`snmp_trap <options>`	Sends an SNMP Trap to the specified host. See *"fwm snmp_trap" on page 357*.
`unload <options>`	Unloads the policy from the specified managed Security Gateways. See *"fwm unload" on page 360*.

Parameter	Description
`ver <options>`	Shows the Check Point version of the Management Server. See *"fwm ver" on page 364*.
`verify <options>`	This command is obsolete for R80 and higher. Use the *"mgmt_cli" on page 386* command to verify a policy. See *"fwm verify" on page 365*.

fwm dbload

Description

Copies the user database and network objects information to specified managed servers with one or more **Management** Software Blades enabled.

Important - This command is obsolete for R80 and higher.
Use the API command "`install-database`" to install the database on the applicable servers.
See the *Check Point Management API Reference* (at the top, select the correct version) .

fwm exportcert

Description

Export a SIC certificate of the specified managed object to a file.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] exportcert -obj <Name of Object> -cert <Name of CA> -file
<Output File> [-withroot] [-pem]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
<Name of Object>	Specifies the name of the managed object, whose certificate you wish to export.
<Name of CA>	Specifies the name of Certificate Authority, whose certificate you wish to export.
<Output File>	Specifies the name of the output file.
`-withroot`	Exports the certificate's root in addition to the certificate's content.
`-pem`	Save the exported information in a text file. Default is to save in a binary file.

fwm fetchfile

Description

Fetches a specified OPSEC configuration file from the specified source server.

This command supports only the `fwopsec.conf` or `fwopsec.v4x` files.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] fetchfile -r <File> [-d <Local Path>] <Source>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-r <File>`	Specifies the relative `fw1` directory. This command supports only these files: ■ `conf/fwopsec.conf` ■ `conf/fwopsec.v4x`
`-d <Local Path>`	Specifies the local directory to save the fetched file.
`<Source>`	Specifies the managed remote source server, from which to fetch the file. **Note** - The local and the remote source servers must have established SIC trust.

Example

```
[Expert@MGMT:0]# fwm fetchfile -r "conf/fwopsec.conf" -d /tmp 192.168.3.52
Fetching conf/fwopsec.conf from 192.168.3.52...
Done
[Expert@MGMT:0]#
```

fwm fingerprint

Description

Shows the Check Point fingerprint.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] fingerprint [-d]
      <IP address of Target> <SSL Port>
      localhost <SSL Port>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. The debug options are: ■ `fwm -d` Runs the complete debug of all `fwm` actions. For complete debug instructions, see the description of the `fwm` process in sk97638. ■ `fingerprint -d` Runs the debug only for the fingerprint actions.
<IP address of Target>	Specifies the IP address of a remote managed server.
<SSL Port>	Specifies the SSL port number. The default is 443.

Example 1 - Showing the fingerprint on the local Management Server

```
[Expert@MGMT:0]# fwm fingerprint localhost 443
#DN OID.1.2.840.113549.1.9.2=An optional company name,Email=Email
Address,CN=192.168.3.51,L=Locality Name (eg\, city)
#FINGER 11:A6:F7:1F:B9:F5:15:BC:F9:7B:5F:DC:28:FC:33:C5
##
[Expert@MGMT:0]#
```

Example 2 - Showing the fingerprint from a managed Security Gateway

```
[Expert@MGMT:0]# fwm fingerprint 192.168.3.52 443
#DN OID.1.2.840.113549.1.9.2=An optional company name,Email=Email
Address,CN=192.168.3.52,L=Locality Name (eg\, city)
#FINGER 5C:8E:4D:B9:B4:3A:58:F3:79:18:F1:70:99:8B:5F:2B
##
[Expert@MGMT:0]#
```

fwm getpcap

Description

Fetches the IPS packet capture data from the specified Security Gateway.

This command only works with IPS packet captures stored on the Security Gateway in the `$FWDIR/log/captures_repository/` directory.

This command does not work with other Software Blades, such as Anti-Bot and Anti-Virus that store packet captures in the `$FWDIR/log/blob/` directory on the Security Gateway.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] getpcap -g <Security Gateway> -u '{<Capture UID>}' -p
<Local Path>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`-g <Security Gateway>`	Specifies the main IP address or Name of Security Gateway object as configured in SmartConsole.
`-u '{<Capture UID>}'`	Specifies the Unique ID of the packet capture file. To see the Unique ID of the packet capture file, open the applicable log file in **SmartConsole > Logs & Monitor > Logs**.
`-p <Local Path>`	Specifies the local path to save the specified packet capture file. If you do not specify the local directory explicitly, the command saves the packet capture file in the current working directory.

Example

```
[Expert@MGMT:0]# fwm getpcap -g 192.168.162.1 -u '{0x4d79dc02,0x10000,0x220da8c0,0x1ffff}'
/var/log/
[Expert@MGMT:0]#
```

fwm ikecrypt

Description

Encrypts the password of an Endpoint VPN Client user using IKE. The resulting string must then be stored in the LDAP database.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] ikecrypt <Key> <Password>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
<Key>	Specifies the IKE Key as defined in the **LDAP Account Unit** properties window on the **Encryption** tab.
<Password>	Specifies the password for the Endpoint VPN Client user.

Example

```
[Expert@MGMT:0]# fwm ikecrypt MySecretKey MyPassword
OUQJHiNHCj6HJGH8ntnKQ7tg
[Expert@MGMT:0]#
```

fwm load

Description

Loads a policy on a managed Security Gateway.

Important - This command is obsolete for R80 and higher.
Use the API command "`install-policy`" to load a policy on a managed Security Gateway.
See the *Check Point Management API Reference* (at the top, select the correct version) .

fwm logexport

Description

Exports a Security log file (`$FWDIR/log/*.log`) or Audit log file (`$FWDIR/log/*.adtlog`) to an ASCII file.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm logexport -h
```

```
fwm [-d] logexport [{-d <Delimiter> | -s}] [-t <Table Delimiter>]
[-i <Input File>] [-o <Output File>] [{-f | -e}] [-x <Start Entry
Number>] [-y <End Entry Number>] [-z] [-n] [-p] [-a] [-u
<Unification Scheme File>] [-m {initial | semi | raw}]
```

Parameters

Parameter	Description
`-h`	Shows the built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`-d <Delimiter> | -s`	Specifies the output delimiter between fields of log entries: ■ `-d <Delimiter>` - Uses the specified delimiter. ■ `-s` - Uses the ASCII character #255 (non-breaking space) as the delimiter. **Note** - If you do not specify the delimiter explicitly, the default is a semicolon (`;`).

Parameter	Description
`-t <Table Delimiter>`	Specifies the output delimiter inside table field. Table field would look like: *ROWx:COL0,ROWx:COL1,ROWx:COL2*, and so on **Note** - If you do not specify the table delimiter explicitly, the default is a comma (`,`).
`-i <Input File>`	Specifies the name of the input log file. **Notes:** ■ This command supports only Security log file (`$FWDIR/log/*.log`) and Audit log file (`$FWDIR/log/*.adtlog`) ■ If you do not specify the input log file explicitly, the command processes the active Security log file `$FWDIR/log/fw.log`
`-o <Output File>`	Specifies the name of the output file. **Note** - If you do not specify the output log file explicitly, the command prints its output on the screen.
`-f`	After reaching the end of the currently opened log file, specifies to continue to monitor the log file indefinitely and export the new entries as well. **Note** - Applies only to the *active* log file: `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`
`-e`	After reaching the end of the currently opened log file, continue to monitor the log file indefinitely and export the new entries as well. **Note** - Applies only to the *active* log file: `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`
`-x <Start Entry Number>`	Starts exporting the log entries from the specified log entry number and below, counting from the beginning of the log file.
`-y <End Entry Number>`	Starts exporting the log entries until the specified log entry number, counting from the beginning of the log file.
`-z`	In case of an error (for example, wrong field value), specifies to continue the export of log entries. The default behavior is to stop.
`-n`	Specifies not to perform DNS resolution of the IP addresses in the log file (this is the default behavior). This significantly speeds up the log processing.

Parameter	Description
`-p`	Specifies to not to perform resolution of the port numbers in the log file (this is the default behavior). This significantly speeds up the log processing.
`-a`	Exports only Account log entries.
`-u <`*`Unification Scheme File`*`>`	Specifies the path and name of the log unification scheme file. The default log unification scheme file is: `$FWDIR/conf/log_unification_scheme.C`
`-m {initial | semi | raw}`	Specifies the log unification mode: ■ `initial` - Complete unification of log entries. The command exports one unified log entry for each ID. This is the default. If you also specify the "`-f`" parameter, then the output does not export any updates, but exports only entries that relate to the start of new connections. To export updates as well, use the "`semi`" parameter. ■ `semi` - Step-by-step unification of log entries. For each log entry, exports entry that unifies this entry with all previously encountered entries with the same ID. ■ `raw` - No log unification. Exports all log entries.

The output of the `fwm logexport` command appears in tabular format.

The first row lists the names of all log fields included in the log entries.

Each of the next rows consists of a single log entry, whose fields are sorted in the same order as the first row.

If a log entry has no information in a specific field, this field remains empty (as indicated by two successive semi-colons "`;;`").

You can control which log fields appear in the output of the command output:

Step	Instructions
1	Create the `$FWDIR/conf/logexport.ini` file: `[Expert@MGMT:0]# touch $FWDIR/conf/logexport.ini`
2	Edit the `$FWDIR/conf/logexport.ini` file: `[Expert@MGMT:0]# vi $FWDIR/conf/logexport.ini`

3	To include or exclude the log fields from the output, add these lines in the configuration file:
	`[Fields_Info]`
	`included_fields = field1,field2,field3,<REST_OF_FIELDS>,field100`
	`excluded_fields = field10,field11`
	Where:
	■ You can specify only the `included_fields` parameter, only the `excluded_fields` parameter, or both.
	■ The `num` field must always appear first. You cannot manipulate this field.
	■ The `<REST_OF_FIELDS>` is an optional reserved token that refers to a list of fields.
	• If you specify the "`-f`" parameter, then the `<REST_OF_FIELDS>` is based on a list of fields from the `$FWDIR/conf/logexport_default.C` file.
	• If you do not specify the "`-f`" parameter, then the `<REST_OF_FIELDS>` is based on the input log file.

4	Save the changes in the file and exit the Vi editor.
5	Export the logs: `fwm logexport <options>`

Example 1 - Exporting all log entries

```
[Expert@MGMT:0]# fwm logexport -i MySwitchedLog.log
Starting... There are 113 log records in the file
num;date;time;orig;type;action;alert;i/f_name;i/f_dir;product;LogId;ContextNum;origin_
id;ContentVersion;HighLevelLogKey;SequenceNum;log_sys_message;ProductFamily;fg-1_client_in_rule_
name;fg-1_client_out_rule_name;fg-1_server_in_rule_name;fg-1_server_out_rule_
name;description;status;version;comment;update_service;reason;Severity;failure_impact
0;13Jun2018;19:47:54;CXL1_192.168.3.52;control; ;;daemon;inbound;VPN-1 & FireWall-1;-1;-
1;CN=CXL1_192.168.3.52,O=MyDomain_Server.checkpoint.com.s6t98x;5;18446744073709551615;2;Log file
has been switched to: MyLog.log;Network;;;;;;;;;;;
1;13Jun2018;19:47:54;CXL1_192.168.3.52;account;accept;;;inbound;FG;-1;-1;CN=CXL1_
192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;Default;Default;;;;;;;;;
... ...
35;13Jun2018;19:55:59;CXL1_192.168.3.52;account;accept;;;inbound;FG;-1;-1;CN=CXL1_
192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;Default;Default;Host
Redirect;;;;;;;;;
36;13Jun2018;19:56:06;CXL1_192.168.3.52;control; ;;;inbound;Security Gateway/Management;-1;-
1;CN=CXL1_192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;;;;;Contracts;Started;1.0;<null>
;1;;;
... ...
47;13Jun2018;19:57:02;CXL1_192.168.3.52;control; ;;;inbound;Security Gateway/Management;-1;-
1;CN=CXL1_192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;;;;;Contracts;Failed;1.0;;1;Could
not reach "https://productcoverage.checkpoint.com/ProductCoverageService". Check DNS and Proxy
configuration on the gateway.;2;Contracts may be out-of-date
... ...
[Expert@MGMT:0]#
```

Example 2 - Exporting only log entries with specified numbers

```
[Expert@MGMT:0]# fwm logexport -i MySwitchedLog.log -x 36 -y 47
Starting... There are 113 log records in the file
num;date;time;orig;type;action;alert;i/f_name;i/f_dir;product;LogId;ContextNum;origin_
id;ContentVersion;HighLevelLogKey;SequenceNum;log_sys_message;ProductFamily;fg-1_client_in_rule_
name;fg-1_client_out_rule_name;fg-1_server_in_rule_name;fg-1_server_out_rule_
name;description;status;version;comment;update_service;reason;Severity;failure_impact
36;13Jun2018;19:56:06;CXL1_192.168.3.52;control; ;;;inbound;Security Gateway/Management;-1;-
1;CN=CXL1_192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;;;;;Contracts;Started;1.0;<null>
;1;;;
37;13Jun2018;19:56:06;CXL1_192.168.3.52;account;accept;;;inbound;FG;-1;-1;CN=CXL1_
192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;2;;Network;Default;Default;Host
Redirect;;;;;;;;;
... ...
46;13Jun2018;19:56:59;CXL1_192.168.3.52;account;accept;;;inbound;FG;-1;-1;CN=CXL1_
192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;Default;Default;Host
Redirect;;;;;;;;;
47;13Jun2018;19:57:02;CXL1_192.168.3.52;control; ;;;inbound;Security Gateway/Management;-1;-
1;CN=CXL1_192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;;;;;Contracts;Failed;1.0;;1;Could
not reach "https://productcoverage.checkpoint.com/ProductCoverageService". Check DNS and Proxy
configuration on the gateway.;2;Contracts may be out-of-date
[Expert@MGMT:0]#
```

fwm mds

Description

- Shows the Check Point version of the Multi-Domain Server.
- Rebuilds status tree for Global VPN Communities.

Note - On a Multi-Domain Server, you can run this command:

- In the context of the MDS:

```
mdsenv
```

- In the context of a Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] mds
      ver
      rebuild_global_communities_status {all | missing}
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`ver`	Shows the Check Point version of the Multi-Domain Server.
`rebuild_global_communities_status`	Rebuilds status tree for Global VPN Communities: ▪ `all` - Rebuilds status tree for all Global VPN Communities. ▪ `missing` - Rebuild status tree only for Global VPN Communities that do not have status trees.

Example

```
[Expert@MDS:0]# fwm mds ver
This is Check Point Multi-Domain Security Management R81.20 -
Build 11
[Expert@MDS:0]#
```

fwm printcert

Description

Shows a SIC certificate's details.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] printcert
      -obj <Name of Object> [-cert <Certificate Nick Name>] [-
verbose]
      -ca <CA Name> [-x509 <Name of File> [-p]] [-verbose]
      -f <Name of Binary Certificate File> [-verbose]
```

Parameters

Item	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`-obj <Name of Object>`	Specifies the name of the managed object, for which to show the SIC certificate information.
`-cert <Certificate Nick Name>`	Specifies the certificate nick name.
`-ca <CA Name>`	Specifies the name of the Certificate Authority. **Note** - Check Point CA Name is `internal_ca`.
`-x509 <Name of File>`	Specifies the name of the X.509 file.
`-p`	Specifies to show the SIC certificate as a text file.
`-f <Name of Binary Certificate File>`	Specifies the binary SIC certificate file to show.
`-verbose`	Shows the information in verbose mode.

Examples

Example 1 - Showing the SIC certificate of a Management Server

```
[Expert@MGMT:0]# fwm printcert -ca internal_ca
Subject: O=MGMT.checkpoint.com.s6t98x
Issuer: O=MGMT.checkpoint.com.s6t98x
Not Valid Before: Sun Apr 8 13:41:00 2018 Local Time
Not Valid After: Fri Jan 1 05:14:07 2038 Local Time
Serial No.: 1
Public Key: RSA (2048 bits)
Signature: RSA with SHA256
Key Usage:
        digitalSignature
        keyCertSign
        cRLSign
Basic Constraint:
        is CA
MD5 Fingerprint:
   7B:F9:7B:4C:BD:40:B9:1C:AB:2C:AE:CF:66:2E:E7:06
SHA-1 Fingerprints:
1. A6:43:3A:2B:1A:04:7F:A6:36:A6:2C:78:BF:22:D9:BC:F7:7E:4D:73
2. KEYS HEM GERM PIT ABUT ROVE RAW PA IQ FAWN NUT SLAM
[Expert@MGMT:0]#
```

Example 2 - Showing the SIC certificate of a Management Server in verbose mode

```
[Expert@MGMT:0]# fwm printcert -ca internal_ca -verbose
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] fwa_db_init: called
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] fwa_db_init: closing existing database
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] do_links_getver: strncmp failed. Returning -2
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] db_fetchkey: entering
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] PubKey:
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] Modulus:
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] ae b3 75 36 64 e4 1a 40 fe c2 ad 2f 9b 83 0b 45
f1 00 04 bc
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 3f 77 77 76 d1 de 8a cf 9f 32 78 8b d4 b1 b4 be
db 75 cc c8
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] c2 6d ff 3e aa fe f1 2b c3 0a b0 a2 a5 e0 a8 ab
45 cd 87 32
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] ac c6 9f a4 a9 ba 30 79 08 fa 59 4c d2 dc 3d 36
ca 17 d7 c1
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] b2 a2 41 f5 89 0f 00 d4 2d f2 55 d2 30 a5 32 c7
46 7a 6b 32
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 29 0f 53 9f 35 42 91 e5 7d f7 30 6d bc b3 f2 ae
f3 f0 ed 88
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] c4 d7 7d 0c 2d f6 5f c8 ed 9f 9a 57 54 79 d0 0f
0b 2f 9c 0d
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 94 2e f0 f4 66 62 f7 ae 2e f8 8e 90 08 ba 63 85
b6 46 2f b7
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] a7 01 29 9a 14 58 a8 ef eb 07 17 4e 95 8b 2f 48
5f d3 18 10
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 3f 00 d5 03 d7 fd 45 45 ca 67 5b 34 be b8 00 ae
ea 9a cd 50
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] d6 e7 a2 81 86 78 11 d7 bf 04 9f 8b 43 3f f7 36
5f ed 31 a8
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] a3 9d 8b 0a de 05 fb 5c 44 2e 29 e3 3e f4 dd 50
01 0f 86 9d
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 55 16 a3 4d f8 90 2d 13 c6 c1 28 57 f8 3e 7c 59
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] Exponent: 65537 (0x10001)
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52]
X509 Certificate Version 3
refCount: 1
Serial Number: 1
Issuer: O=MGMT.checkpoint.com.s6t98x
Subject: O=MGMT.checkpoint.com.s6t98x
Not valid before: Sun Apr 8 13:41:00 2018 Local Time
Not valid after: Fri Jan 1 05:14:07 2038 Local Time
Signature Algorithm: RSA with SHA-256 Public key: RSA (2048 bits)
Extensions:
        Key Usage:
                digitalSignature
                keyCertSign
                cRLSign
        Basic Constraint (Critical):
                is CA

[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] destroy_rand_mutex: destroy
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] cpKeyTaskManager::~cpKeyTaskManager: called.
[Expert@MGMT:0]#
```

Example 3 - Showing the SIC certificate of a managed Cluster object

```
[Expert@MGMT:0]# fwm printcert -obj CXL_192.168.3.244

printing all certificates of CXL_192.168.3.244

defaultCert:
Host Certificate (level 0):
Subject: CN=CXL_192.168.3.244 VPN Certificate,O=MGMT.checkpoint.com.s6t98x
Issuer: O=MGMT.checkpoint.com.s6t98x
Not Valid Before: Sun Jun 3 19:58:19 2018 Local Time
Not Valid After: Sat Jun 3 19:58:19 2023 Local Time
Serial No.: 85021
Public Key: RSA (2048 bits)
Signature: RSA with SHA256
Subject Alternate Names:
        IP Address: 192.168.3.244
CRL distribution points:
        http://192.168.3.240:18264/ICA_CRL2.crl
        CN=ICA_CRL2,O=MGMT.checkpoint.com.s6t98x
Key Usage:
        digitalSignature
        keyEncipherment
Basic Constraint:
        not CA
MD5 Fingerprint:
   B1:15:C7:A8:2A:EE:D1:75:92:9F:C7:B4:B9:BE:42:1B
SHA-1 Fingerprints:
1. BC:7A:D9:E2:CD:29:D1:9E:F0:39:5A:CD:7E:A9:0B:F9:6A:A7:2B:85
2. MIRE SANK DUSK HOOD HURD RIDE TROY QUAD LOVE WOOD GRIT WITH


               *****
[Expert@MGMT:0]#
```

Example 4 - Showing the SIC certificate of a managed Cluster object in verbose mode

```
[Expert@MGMT:0]# fwm printcert -obj CXL_192.168.3.244 -verbose
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] fwa_db_init: called
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] fwa_db_init: closing existing database
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] do_links_getver: strncmp failed. Returning -2

printing all certificates of CXL_192.168.3.244

[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] db_fetchkey: entering
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] 1 certificates
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] PubKey:
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] Modulus:
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] df 35 c3 45 ca 42 16 6e 21 9e 31 af c1 fd 20 0a
3d 5b 6f 5d
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] e0 a2 0c 0e fa fa 5e e5 91 9d 4e 73 77 fa db 86
0b 5e 5d 0c
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] ce af 4a a4 7b 30 ed b0 43 7d d8 93 c5 4b 01 f4
3d b5 d8 f4
... ... ...
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] 34 b1 db ac 18 4f 11 bd d2 fb 26 7d 23 74 5c d9
00 a1 58 1e
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] 60 7c 83 44 fa 1e 1e 86 fa ad 98 f7 df 24 4a 21
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] Exponent: 65537 (0x10001)
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45]
X509 Certificate Version 3
refCount: 1
Serial Number: 85021
Issuer: O=MGMT.checkpoint.com.s6t98x
Subject: CN=CXL_192.168.3.244 VPN Certificate,O=MGMT.checkpoint.com.s6t98x
Not valid before: Sun Jun 3 19:58:19 2018 Local Time
Not valid after: Sat Jun 3 19:58:19 2023 Local Time
Signature Algorithm: RSA with SHA-256 Public key: RSA (2048 bits)
Extensions:
        Key Usage:
                digitalSignature
                keyEncipherment
        Subject Alternate names:
                IP: 192.168.3.244
        Basic Constraint:
                not CA
        CRL distribution Points:
                URI: http://192.168.3.240:18264/ICA_CRL2.crl
                DN: CN=ICA_CRL2,O=MGMT.checkpoint.com.s6t98x

defaultCert:

[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] destroy_rand_mutex: destroy
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] cpKeyTaskManager::~cpKeyTaskManager: called.
                *****
[Expert@MGMT:0]#
```

fwm sic_reset

Description

Resets SIC on the Management Server.

For detailed procedure, see sk65764: How to reset SIC.

Warning:

- **Before you run this command, take a Gaia Snapshot and a full backup of the Management Server.**
  This command resets SIC between the Management Server and all its managed objects.
- **This operation breaks trust in all Internal CA certificates and SIC trust across the managed environment.**
  Therefore, we do not recommend it at all, except for real disaster recovery.

Note
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] sic_reset
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.

fwm snmp_trap

Description

Sends an SNMPv1 Trap to the specified host.

Notes:

- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- On a Multi-Domain Server, the SNMP Trap packet is sent from the IP address of the Leading Interface.

Syntax

```
fwm [-d] snmp_trap [-v <SNMP OID>] [-g <Generic Trap Number>] [-s
<Specific Trap Number>] [-p <Source Port>] [-c <SNMP Community>]
<Target> ["<Message>"]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`-v <SNMP OID>`	Specifies an optional SNMP OID to bind with the message.
`-g <Generic Trap Number>`	Specifies the generic trap number. One of these values: ■ 0 - For `coldStart` trap ■ 1 - For `warmStart` trap ■ 2 - For `linkDown` trap ■ 3 - For `linkUp` trap ■ 4 - For `authenticationFailure` trap ■ 5 - For `egpNeighborLoss` trap ■ 6 - For `enterpriseSpecific` trap (this is the default value)
`-s <Specific Trap Number>`	Specifies the unique trap type. Valid only of generic trap value is 6 (for `enterpriseSpecific`). Default value is 0.
`-p <Source Port>`	Specifies the source port, from which to send the SNMP Trap packets.
`-c <SNMP Community>`	Specifies the SNMP community.
`<Target>`	Specifies the managed target host, to which to send the SNMP Trap packets. Enter an IP address of a resolvable hostname.
`"<Message>"`	Specifies the SNMP Trap text message.

Example - Sending an SNMP Trap from a Management Server and capturing the traffic on the Security Gateway

```
[Expert@MGMT:0]# fwm snmp_trap -g 2 -c public 192.168.3.52 "My Trap Message"
[Expert@MGMT:0]#

[Expert@MyGW_192.168.3.52:0]# tcpdump -s 1500 -vvvv -i eth0 udp and host 192.168.3.51
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 1500 bytes
22:49:43.891287 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto: UDP (17), length: 103)
192.168.3.51.53450 > MyGW_192.168.3.52.snmptrap: [udp sum ok] { SNMPv1 { Trap(58) E:2620.1.1
192.168.3.240 linkDown 1486440 E:2620.1.1.11.0="My Trap Message" } }
Pressed CTRL+C
[Expert@MyGW_192.168.3.52:0]#
```

fwm unload

Description

Unloads the policy from the specified managed Security Gateways or Cluster Members.

Warning:

1. The `fwm unload` command prevents all traffic from passing through the Security Gateway (Cluster Member), because it disables the IP Forwarding in the Linux kernel on the specified Security Gateway (Cluster Member).
2. The `fwm unload` command removes all policies from the specified Security Gateway (Cluster Member).
   This means that the Security Gateway (Cluster Member) accepts all incoming connections destined to all active interfaces without any filtering or protection enabled.

Notes:

- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:
  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```
- If it is necessary to remove the current policy, but keep the Security Gateway (Cluster Member) protected, then run the *"comp_init_policy" on page 965* command on the Security Gateway (Cluster Member).
- To load the policies on the Security Gateway (Cluster Member), run one of these commands on the Security Gateway (Cluster Member), or reboot:
  - *"fw fetch" on page 1119*
  - *"cpstart" on page 1018*
- In addition, see the *"fw unloadlocal" on page 1242* command.

Syntax

```
fwm [-d] unload <GW1> <GW2> ... <GWN>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
<GW1> <GW2> ... <GWN>	Specifies the managed Security Gateways by their main IP address or Object Name as configured in SmartConsole.

Example

```
[Expert@MyGW:0]# cpstat -f policy fw

Product name: Firewall
Policy name: CXL_Policy
Policy install time: Wed Oct 23 18:23:14 2019
... ... ...
[Expert@MyGW:0]#


[Expert@MyGW:0]# sysctl -a | grep forwarding | grep -v bridge
net.ipv6.conf.bond0.forwarding = 1
net.ipv6.conf.eth1.forwarding = 1
net.ipv6.conf.eth3.forwarding = 1
net.ipv6.conf.eth2.forwarding = 1
net.ipv6.conf.eth4.forwarding = 1
net.ipv6.conf.eth5.forwarding = 1
net.ipv6.conf.eth0.forwarding = 1
net.ipv6.conf.eth6.forwarding = 1
net.ipv6.conf.default.forwarding = 1
net.ipv6.conf.all.forwarding = 1
net.ipv6.conf.lo.forwarding = 1
net.ipv4.conf.bond0.mc_forwarding = 0
net.ipv4.conf.bond0.forwarding = 1
net.ipv4.conf.eth1.mc_forwarding = 0
net.ipv4.conf.eth1.forwarding = 1
net.ipv4.conf.eth2.mc_forwarding = 0
net.ipv4.conf.eth2.forwarding = 1
net.ipv4.conf.eth0.mc_forwarding = 0
net.ipv4.conf.eth0.forwarding = 1
net.ipv4.conf.lo.mc_forwarding = 0
net.ipv4.conf.lo.forwarding = 1
net.ipv4.conf.default.mc_forwarding = 0
net.ipv4.conf.default.forwarding = 1
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.all.forwarding = 1
[Expert@MyGW:0]#


[Expert@MGMT:0]# fwm unload MyGW

Uninstalling Policy From: MyGW

 Security Policy successfully uninstalled from MyGW...

Security Policy uninstall complete.

[Expert@MGMT:0]#
```

```
[Expert@MyGW:0]# cpstat -f policy fw

Product name: Firewall
Policy name:
Policy install time:
... ... ...
[Expert@MyGW:0]#


[Expert@MyGW:0]# sysctl -a | grep forwarding | grep -v bridge
net.ipv6.conf.bond0.forwarding = 0
net.ipv6.conf.eth1.forwarding = 0
net.ipv6.conf.eth3.forwarding = 0
net.ipv6.conf.eth2.forwarding = 0
net.ipv6.conf.eth4.forwarding = 0
net.ipv6.conf.eth5.forwarding = 0
net.ipv6.conf.eth0.forwarding = 0
net.ipv6.conf.eth6.forwarding = 0
net.ipv6.conf.default.forwarding = 0
net.ipv6.conf.all.forwarding = 0
net.ipv6.conf.lo.forwarding = 0
net.ipv4.conf.bond0.mc_forwarding = 0
net.ipv4.conf.bond0.forwarding = 0
net.ipv4.conf.eth1.mc_forwarding = 0
net.ipv4.conf.eth1.forwarding = 0
net.ipv4.conf.eth2.mc_forwarding = 0
net.ipv4.conf.eth2.forwarding = 0
net.ipv4.conf.eth0.mc_forwarding = 0
net.ipv4.conf.eth0.forwarding = 0
net.ipv4.conf.lo.mc_forwarding = 0
net.ipv4.conf.lo.forwarding = 0
net.ipv4.conf.default.mc_forwarding = 0
net.ipv4.conf.default.forwarding = 0
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.all.forwarding = 0
[Expert@MyGW:0]#
```

fwm ver

Description

Shows the Check Point version of the Security Management Server.

Note - On a Multi-Domain Server, you can run this command:

- In the context of the MDS:

```
mdsenv
```

- In the context of a Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] ver [-f <Output File>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`-f <Output File>`	Specifies the name of the output file, in which to save this information.

Example

```
[Expert@MGMT:0]# fwm ver
This is Check Point Security Management Server R81.20 - Build 11
[Expert@MGMT:0]#
```

fwm verify

Important - This command is obsolete for R80 and higher. Use the *"mgmt_cli" on page 386* command to verify a policy on a managed Security Gateway.

Description

Verifies the specified policy package without installing it.

Note
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] verify <Policy Name>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
<Policy Name>	Specifies the name of the policy package as configured in SmartConsole.

Example

```
[Expert@MGMT:0]# fwm verify Standard
 Verifier messages:
Error: Rule 1 Hides rule 2 for Services & Applications: any .
[Expert@MGMT:0]#
```

inet_alert

Description

Notifies an Internet Service Provider (ISP) when a company's corporate network is under attack. This command forwards log messages generated by the alert daemon on your Check Point Security Gateway to an external Management Station. This external Management Station is usually located at the ISP site. The ISP can then analyze the alert and react accordingly.

This command uses the Event Logging API (ELA) protocol to send the alerts. The Management Station receiving the alert must be running the ELA Proxy.

If communication with the ELA Proxy is to be authenticated or encrypted, a key exchange must be performed between the external Management Station running the ELA Proxy at the ISP site and the Check Point Security Gateway generating the alert.

Procedure

Step	Instructions
1	Connect with SmartConsole to the applicable Security Management Server or Domain Management Server, which manages the applicable Security Gateway that should forward log messages to an external Management Station.
2	From the top left **Menu**, click **Global properties**.
3	Click on the **[+]** near the **Log and Alert** and click **Alerts**.
4	Clear the **Send user defined alert no. 1 to SmartView Monitor**.
5	Select the next option **Run UserDefined script under the above**.
6	Enter the applicable **inet_alert** syntax (see the *Syntax* section below).
7	Click **OK**.
8	Install the Access Control Policy on the applicable Security Gateway.

Syntax

```
inet_alert -s <IP Address> [-o] [-a <Auth Type>] [-p <Port>] [-f
<Token> <Value>] [-m <Alert Type>]
```

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

Parameters

Parameter	Description
`-s <IP Address>`	The IPv4 address of the ELA Proxy (usually located at the ISP site).
`-o`	Prints the alert log received to `stdout`. Use this option when `inet_alert` is part of a pipe syntax (`<some command> | inet_alert ...`).
`-a <Auth Type>`	Specifies the type of connection to the ELA Proxy. One of these values: ■ `ssl_opsec` - The connection is authenticated and encrypted (this is the default). ■ `auth_opsec` - The connection is authenticated. ■ `clear` - The connection is neither authenticated, nor encrypted.
`-p <Port>`	Specifies the port number on the ELA proxy. Default port is 18187.
`-f <Token> <Value>`	A field to be added to the log, represented by a `<Token> <Value>` pair as follows: ■ `<Token>` - The name of the field to be added to the log. Cannot contain spaces. ■ `<Value>` - The field's value. Cannot contain spaces. This option can be used multiple times to add multiple `<Token> <Value>` pairs to the log.

Parameter	Description
`-m <Alert Type>`	The alert to be triggered at the ISP site. This alert overrides the alert specified in the log message generated by the alert daemon. The response to the alert is handled according to the actions specified in the ISP Security Policy: These alerts execute the OS commands: ■ `alert` - Popup alert command ■ `mail` - Mail alert command ■ `snmptrap` - SNMP trap alert command ■ `spoofalert` - Anti-Spoof alert command These NetQuota and ServerQuota alerts execute the OS commands specified in the `$FWDIR/conf/objects.C`: file: `value=clientquotaalert. Parameter=clientquotaalertcmd`

Exist Status

Exit Status	Description
`0`	Execution was successful.
`102`	Undetermined error.
`103`	Unable to allocate memory.
`104`	Unable to obtain log information from `stdin`
`106`	Invalid command line arguments.
`107`	Failed to invoke the OPSEC API.

Example

```
inet_alert -s 10.0.2.4 -a clear -f product cads -m alert
```

This command specifies to perform these actions in the event of an attack:

- Establish a clear connection with the ELA Proxy located at IP address 10.0.2.4
- Send a log message to the specified ELA Proxy. Set the product field of this log message to `cads`
- Trigger the OS command specified in the SmartConsole > **Menu > Global properties > Log and Alert > Popup Alert Command** field.

ldapcmd

Description

This is an LDAP utility that controls these features:

Feature	Description
Cache	LDAP cache operations, such as emptying the cache, as well as providing debug information.
Statistics	LDAP search statistics, such as: ■ All user searches ■ Pending lookups (when two or more lookups are identical) ■ Total lookup time (the total search time for a specific lookup) ■ Cache statistics such as hits and misses These statistics are saved in the `$FWDIR/log/ldap_pid_<Process PID>.stats` file.
Logging	View the alert and warning logs.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
ldapcmd [-d <Debug Level>] -p {<Process Name> | all} <Command>
```

Parameters

Parameter	Description
`-d <Debug Level>`	Runs the command in debug mode with the specified TDERROR debug level. Valid values are from 0 (disabled) to 5 (maximal level, recommended).
`-p {<Process Name> | all}`	Runs on a specified Check Point process, or all supported Check Point processes.
`<Command>`	One of these commands: ■ `cacheclear {all | UserCacheObject | TemplateCacheObject | TemplateExtGrpCacheObject}` • `all` - Clears cache for all objects • `UserCacheObject` - Clears cache for user objects • `TemplateCacheObject` - Clears cache for template objects • `TemplateExtGrpCacheObject` - Clears cache for external template group objects ■ `cachetrace {all | UserCacheObject | TemplateCacheObject | TemplateExtGrpCacheObject}` • `all` - Traces cache for all objects • `UserCacheObject` - Traces cache for user objects • `TemplateCacheObject` - Traces cache for template objects • `TemplateExtGrpCacheObject` - Traces cache for external template group objects ■ `log {on | off}` • `on` - Creates LDAP logs • `off` - Does not create LDAP logs ■ `stat {<Print Interval in Sec> | 0}` • `<Print Interval in Sec>` - How frequently to collect the statistics • `0` - Stops collecting the statistics

ldapcompare

Description

This is an LDAP utility that performs compare queries and prints a message whether the result returned a match or not.

This utility opens a connection to an LDAP directory server, binds, and performs the comparison specified on the command line or from a specified file.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
ldapcompare [-d <Debug Level>] [<Options>] <DN> {<Attribute>
<Value> | <Attribute> <Base64 Value>}
```

Parameters

Parameter	Description
`-d <Debug Level>`	Runs the command in debug mode with the specified TDERROR debug level. Valid values are from 0 (disabled) to 5 (maximal level, recommended).
`<Options>`	See the tables below: ■ Compare options ■ Common options
`<DN>`	Specifies the Distinguished Name.
`<Attribute>`	Specifies the assertion attribute.
`<Value>`	Specifies the assertion value.
`<Base64 Value>`	Specifies the Base64 encoding of the assertion value.

Compare options

Option	Description
`-E [!]<Extension> [=<Extension Parameter>]`	Specifies the compare extensions. **Note** - The exclamation sign "!" indicates criticality. For example: `!dontUseCopy` = Do **not** use Copy
`-M`	Enables the Manage DSA IT control. Use the "`-MM`" option to make it critical.
`-P <LDAP Protocol Version>`	Specifies the LDAP protocol version. Default version is 3.
`-z`	Enables the quiet mode. The command does not print anything. You can use the command return values.

Common options

Option	Description
`-D <Bind DN>`	Specifies the LDAP Server administrator Distinguished Name.

Option	Description
`-e [!]<Extension> [=<Extension Parameter>]`	Specifies the general extensions: **Note** - The exclamation sign "!" indicates criticality. ■ `[!]assert=<Filter>` RFC 4528; an RFC 4515 filter string ■ `[!]authzid=<Authorization ID>` RFC 4370; either "`dn:<DN>`", or "`u:<Username>`" ■ `[!]chaining[=<Resolve Behavior> [/<Continuation Behavior>]]` One of these: • "chainingPreferred" • "chainingRequired" • "referralsPreferred" • "referralsRequired" ■ `[!]manageDSAit` RFC 3296 ■ `[!]noop` ■ `ppolicy` ■ `[!]postread[=<Attributes>]` RFC 4527; a comma-separated list of attributes ■ `[!]preread[=<Attributes>]` RFC 4527; a comma-separated list of attributes ■ `[!]relax` ■ `abandon` SIGINT sends the abandon signal; if critical, does not wait for SIGINT. Not really controls. ■ `cancel` SIGINT sends the cancel signal; if critical, does not wait for SIGINT. Not really controls. ■ `ignore` SIGINT ignores the response; if critical, does not wait for SIGINT. Not really controls.
`-h <LDAP Server>`	Specifies the LDAP Server server by its IP address or resolvable hostname.
`-H <LDAP URI>`	Specifies the LDAP Server Uniform Resource Identifier (s).
`-I`	Specifies to use the SASL Interactive mode.
`-n`	Dry run - shows what would be done, but does not actually do it.

Option	Description
`-N`	Specifies not to use the reverse DNS to canonicalize SASL host name.
`-o <Option>[=<Option Parameter>]`	Specifies the general options: `nettimeout={<Timeout in Sec> | none | max}`
`-O <Properties>`	Specifies the SASL security properties.
`-p <LDAP Server Port>`	Specifies the LDAP Server port. Default is 389.
`-Q`	Specifies to use the SASL Quiet mode.
`-R <Realm>`	Specifies the SASL realm.
`-U <Authentication Identity>`	Specifies the SASL authentication identity.
`-v`	Runs in verbose mode (prints the diagnostics to *stdout*).
`-V`	Prints version information (use the "`-VV`" option only).
`-w <LDAP Admin Password>`	Specifies the LDAP Server administrator password (for simple authentication).
`-W`	Specifies to prompt the user for the LDAP Server administrator password.
`-x`	Specifies to use simple authentication.
`-X <Authorization Identity>`	Specifies the SASL authorization identity (either "`dn:<DN>`", or "`u:<Username>`" option).
`-y <File>`	Specifies to read the LDAP Server administrator password from the `<File>`.
`-Y <SASL Mechanism>`	Specifies the SASL mechanism.
`-Z`	Specifies to start the TLS request. Use the "`-ZZ`" option to require successful response.

ldapmemberconvert

Description

This is an LDAP utility that ports from the "Member" attribute values in LDAP group entries to the "MemberOf" attribute values in LDAP member (User or Template) entries.

This utility converts the LDAP server data to work in either the "MemberOf" mode, or "Both" mode. The utility searches through all specified group or template entries that hold one or more "Member" attribute values and modifies each value. The utility searches through all specified group/template entries and fetches their "Member" attribute values.

Each value is the DN of a member entry. The entry identified by this DN is added to the "MemberOf" attribute value of the group/template DN at hand. In addition, the utility delete those "Member" attribute values from the group/template, unless you run the command in the "Both" mode.

When your run the command, it creates a log file `ldapmemberconvert.log` in the current working directory. The command logs all modifications done and errors encountered in that log file.

Important - Back up the LDAP server database *before* you run this conversion utility.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
ldapmemberconvert [-d <Debug Level>] -h <LDAP Server> -p <LDAP
Server Port> -D <LDAP Admin DN> -w <LDAP Admin Password> -m
<Member Attribute Name> -o <MemberOf Attribute Name> -c <Member
ObjectClass Value> [-B] [-f <File> | -g <Group DN>] [-L <LDAP
Server Timeout>] [-M <Number of Updates>] [-S <Size>] [-T <LDAP
Client Timeout>] [-Z]
```

Parameters

Parameter	Description
`-d <Debug Level>`	Runs the command in debug mode with the specified TDERROR debug level. Valid values are from 0 (disabled) to 5 (maximal level, recommended).
`-h <LDAP Server>`	Specifies the LDAP Server server by its IP address or resolvable hostname. If you do not specify the LDAP Server explicitly, the command connects to `localhost`.
`-p <LDAP Server Port>`	Specifies the LDAP Server port. Default is 389.
`-D <LDAP Admin DN>`	Specifies the LDAP Server administrator Distinguished Name.
`-w <LDAP Admin Password>`	Specifies the LDAP Server administrator password.
`-m <Member Attribute Name>`	Specifies the LDAP attribute name when fetching and (possibly) deleting a group `Member` attribute value.
`-o <MemberOf Attribute Name>`	Specifies the LDAP attribute name for adding an LDAP "`MemberOf`" attribute value.
`-c <Member ObjectClass Value>`	Specifies the LDAP "`ObjectClass`" attribute value that defines, which type of member to modify. You can specify multiple attribute values with this syntax: `-c <Member Object Class 1> -c <Member Object Class 2> ... -c <Member Object Class N>`
`-B`	Specifies to run in "`Both`" mode.

`-f <File>`	Specifies the file that contains a list of Group DNs separated by a new line:
	`<Group DN 1>`
	`<Group DN 2>`
	`...`
	`<Group DN N>`
	Length of each line is limited to 256 characters.

Parameter	Description
`-g <Group DN>`	Specifies the Group or Template Distinguished Name, on which to perform the conversion. You can specify multiple Group DNs with this syntax: `-g <Group DN 1> -g <Group DN 2> ... -g <Group DN N>`
`-L <LDAP Server Timeout>`	Specifies the Server side time limit for LDAP operations, in seconds. Default is "never".
`-M <Number of Updates>`	Specifies the maximal number of simultaneous member LDAP updates. Default is 20.
`-S <Size>`	Specifies the Server side size limit for LDAP operations, in number of entries. Default is "none".
`-T <LDAP Client Timeout>`	Specifies the Client side timeout for LDAP operations, in milliseconds. Default is "never".
`-Z`	Specifies to use SSL connection.

Notes

There are two "GroupMembership" modes. You must keep these modes consistent:

- template-to-groups
- user-to-groups

For example, if you apply conversion on LDAP users to include the "MemberOf" attributes for their groups, then this conversion has to be applied on LDAP defined templates for their groups.

Troubleshooting

Symptom:

A command fails with an error message stating the connection stopped unexpectedly when you run it with the parameter `-M <Number of Updates>`.

Root Cause:

The LDAP server could not handle that many LDAP requests simultaneously and closed the connection.

Solution:

Run the command again with a lower value for the "`-M`" parameter. The default value should be adequate, but can also cause a connection failure in extreme situations. Continue to reduce the value until the command runs normally. Each time you run the command with the same set of groups, the command continues from where it left off.

Examples

Example 1

A group is defined with the DN "`cn=cpGroup,ou=groups,ou=cp,c=us`" and these attributes:

```
...
cn=cpGroup
uniquemember="cn=member1,ou=people,ou=cp,c=us"
uniquemember="cn=member2,ou=people,ou=cp,c=us"
...
```

For the two member entries:

```
...
cn=member1
objectclass=fw1Person
...
```

and:

```
...
cn=member2
objectclass=fw1Person
...
```

Run:

```
[Expert@MGMT:0]# ldapconvert -g cn=cpGroup,ou=groups,ou=cp,c=us -h MyLdapServer -d cn=admin -w secret -m uniquemember -o memberof -c
fw1Person
```

The result for the group DN is:

```
...
cn=cpGroup
...
```

The result for the two member entries is:

```
...
cn=member1
objectclass=fw1Person
memberof="cn=cpGroup,ou=groups,ou=cp,c=us"
...
```

and:

```
...
cn=member2
objectclass=fw1Person
memberof="cn=cpGroup,ou=groups,ou=cp,c=us"
...
```

If you run the same command with the "`-B`" parameter, it produces the same result, but the group entry is not modified.

Example 2

If there is another member attribute value for the same group entry:

```
uniquemember="cn=template1,ou=people, ou=cp,c=us"
```

and the template is:

```
cn=member1
objectclass=fw1Template
```

Then after running the same command, the template entry stays intact, because of the parameter "`-c fw1Person`", but the object class of "`template1`" is "`fw1Template`".

ldapmodify

Description

This is an LDAP utility that imports users to an LDAP server. The input file must be in the LDIF format.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
ldapmodify [-d <Debug Level>] [-h <LDAP Server>] [-p <LDAP Server Port>] [-D <LDAP Admin DN>] [-w <LDAP Admin Password>] [-a] [-b] [-c] [-F] [-k] [-n] [-r] [-v] [-T <LDAP Client Timeout>] [-Z] [ -f <Input File> .ldif | < <Entry>]
```

Parameters

Parameter	Description
`-d <Debug Level>`	Runs the command in debug mode with the specified TDERROR debug level. Valid values are from 0 (disabled) to 5 (maximal level, recommended).
`-h <LDAP Server>`	Specifies the LDAP Server server by its IP address or resolvable hostname. If you do not specify the LDAP Server explicitly, the command connects to `localhost`.
`-p <LDAP Server Port>`	Specifies the LDAP Server port. Default is 389.
`-D <LDAP Admin DN>`	Specifies the LDAP Server administrator Distinguished Name.
`-w <LDAP Admin Password>`	Specifies the LDAP Server administrator password.

Parameter	Description
`-a`	Specifies that this is the LDAP "`add`" operation.
`-b`	Specifies to read values from files (for binary attributes).
`-c`	Specifies to ignore errors during continuous operation.
`-F`	Specifies to force changes on all records.
`-k`	Specifies the Kerberos bind.
`-K`	Specifies the Kerberos bind, part 1 only.
`-n`	Specifies to print the LDAP "`add`" operations, but do not actually perform them.
`-r`	Specifies to replace values, instead of adding values.
`-v`	Specifies to run in verbose mode.
`-T <`*`LDAP Client Timeout`*`>`	Specifies the Client side timeout for LDAP operations, in milliseconds. Default is "`never`".
`-Z`	Specifies to use SSL connection.
`-f <`*`Input File`*`>.ldif`	Specifies to read from the `<`*`Input File`*`>.ldif` file. The input file must be in the LDIF format.
`< <`*`Entry`*`>`	Specifies to read the entry from the *stdin*. The "`<`" character is mandatory part of the syntax. It specifies the input comes from the standard input (from the data you enter on the screen).

ldapsearch

Description

This is an LDAP utility that queries an LDAP directory and returns the results.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
ldapsearch [-d <Debug Level>] [-h <LDAP Server>] [-p <LDAP Port>]
[-D <LDAP Admin DN>] [-w <LDAP Admin Password>] [-A] [-B] [-b
<Base DN>] [-F <Separator>] [-l <LDAP Server Timeout>] [-s
<Scope>] [-S <Sort Attribute>] [-t] [-T <LDAP Client Timeout>] [-
u] [-z <Number of Search Entries>] [-Z] <Filter> [<Attributes>]
```

Parameters

Parameter	Description
`-d <Debug Level>`	Runs the command in debug mode with the specified TDERROR debug level. Valid values are from 0 (disabled) to 5 (maximal level, recommended).
`-h <LDAP Server>`	Specifies the LDAP Server server by its IP address or resolvable hostname. If you do not specify the LDAP Server explicitly, the command connects to `localhost`.
`-p <LDAP Port>`	Specifies the LDAP Server port. Default is 389.
`-D <LDAP Admin DN>`	Specifies the LDAP Server administrator Distinguished Name.
`-w <LDAP Admin Password>`	Specifies the LDAP Server administrator password.
`-A`	Specifies to retrieve attribute names only, without values.

Parameter	Description
`-B`	Specifies not to suppress the printing of non-ASCII values.
`-b <Base DN>`	Specifies the Base Distinguished Name (DN) for search.
`-F <Separator>`	Specifies the print separator character between attribute names and their values. The default separator is the equal sign (=).
`-l <LDAP Server Timeout>`	Specifies the Server side time limit for LDAP operations, in seconds. Default is "`never`".
`-s <Scope>`	Specifies the search scope. One of these: ■ `base` ■ `one` ■ `sub`
`-S <Sort Attribute>`	Specifies to sort the results by the values of this attribute.

`-t`	Specifies to write values to files in the `/tmp/` directory.
	Writes each *<attribute>-<value>* pair to a separate file named:
	`/tmp/ldapsearch-<Attribute>-<Value>`
	For example, for the `fw1color` attribute with the value `a00188`, the command writes to the file named:
	`/tmp/ldapsearch-fw1color-a00188`

`-T <LDAP Client Timeout>`	Specifies the Client side timeout for LDAP operations, in milliseconds. Default is `never`.
`-u`	Specifies to show user-friendly entry names in the output. For example: shows `cn=Babs Jensen, users, omi` instead of `cn=Babs Jensen, cn=users,cn=omi`
`-z <Number of Search Entries>`	Specifies the maximal number of entries to search on the LDAP Server.
`-Z`	Specifies to use SSL connection.
`<Filter>`	LDAP search filter compliant with RFC-1558. For example: `objectclass=fw1host`

Parameter	Description
<Attributes>	Specifies the list of attributes to retrieve. If you do not specify attributes explicitly, then the command retrieves all attributes.

Example

```
[Expert@MGMT:0]# ldapsearch -p 18185 -b cn=omi objectclass=fw1host objectclass
```

With this syntax, the command:

1. Connects to the LDAP Server to port 18185.
2. Connects to the LDAP Server with Base DN "`cn=omi`".
3. Queries the LDAP directory for "`fw1host`" objects.
4. For each object found, prints the value of its "`objectclass`" attribute.

mgmt_cli

Description

The `mgmt_cli` tool works directly with the management database on your Management Server.

Syntax on Management Server or Security Gateway running on Gaia OS

```
mgmt_cli <Command Name> <Command Parameters> <Optional Switches>
```

Syntax on SmartConsole computer running on Windows OS 32-bit

Open Windows Command Prompt and run these commands:

```
cd /d "%ProgramFiles%\CheckPoint\SmartConsole\<VERSION>\PROGRAM\"
mgmt_cli.exe <Command Name> <Command Parameters> <Optional
Switches>
```

Syntax on SmartConsole computer running on Windows OS 64-bit

Open Windows Command Prompt and run these commands:

```
cd /d "%ProgramFiles
(x86)%\CheckPoint\SmartConsole\<VERSION>\PROGRAM\"
mgmt_cli.exe <Command Name> <Command Parameters> <Optional
Switches>
```

Notes

- For a complete list of the `mgmt_cli` options, enter the `mgmt_cli` (`mgmt_cli.exe`) command and press Enter.
- For more information, see the *Check Point Management API Reference* (at the top, select the correct version) .

migrate

Important - This command is used to migrate the management database from R80.10 and lower versions.
For more information, see the *R81.20 Installation and Upgrade Guide*.

Description

Exports the management database and applicable Check Point configuration.

Imports the exported management database and applicable Check Point configuration.

Backing up and restoring in Management High Availability environment:

- To back up and restore a consistent environment, make sure to collect and restore the backups and snapshots from all servers in the High Availability environment at the same time.
- Make sure other administrators do not make changes in SmartConsole until the backup operation is completed.

For more information:

- About Gaia Backup and Gaia Snapshot, see the *R81.20 Gaia Administration Guide*.
- About Virtual Machine Snapshots, see the vendor documentation.

Notes:

- You must run this command from the Expert mode.
- If it is necessary to back up the current management database, and you do **not** plan to import it on a Management Server that runs a higher software version, then you can use the built-in command in the `$FWDIR/bin/upgrade_tools/` directory.
- If you plan to import the management database on a Management Server that runs a higher software version, then you must use the `migrate` utility from the migration tools package created specifically for that higher software version. See the **Installation and Upgrade Guide** for that higher software version.
- If this command completes successfully, it creates this log file:
  `/var/log/opt/CPshrd-R81.20/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  For example: */var/log/opt/CPshrd-R81.20/migrate-2019.06.14_11.03.46.log*
- If this command fails, it creates this log file:
  `$CPDIR/log/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  For example: */opt/CPshrd-R81.20/log/migrate-2019.06.14_11.21.39.log*

Syntax

- To see the built-in help:

```
[Expert@MGMT:0]# ./migrate -h
```

- To export the management database and configuration:

```
[Expert@MGMT:0]# cd $FWDIR/bin/upgrade_tools/
[Expert@MGMT:0]# yes | nohup ./migrate export [-l | -x] [-n]
[--exclude-uepm-postgres-db] [--include-uepm-msi-files] /<Full
Path>/<Name of Exported File> &
```

- To import the management database and configuration:

```
[Expert@MGMT:0]# cd $FWDIR/bin/upgrade_tools/
[Expert@MGMT:0]# yes | nohup ./migrate import [-l | -x] [-n]
[--exclude-uepm-postgres-db] [--include-uepm-msi-files] /<Full
Path>/<Name of Exported File>.tgz &
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`yes | nohup ./migrate ... &`	This syntax: 1. Sends the "`yes`" input to the interactive "`migrate`" command through the pipeline. 2. The "`nohup`" forces the "`migrate`" command to ignore the hangup signals from the shell. 3. The "`&`" forces the command to run in the background. As a result, when the CLI session closes, the command continues to run in the background. See: ■ sk133312 ■ https://linux.die.net/man/1/bash ■ https://linux.die.net/man/1/nohup
`export`	Exports the management database and applicable Check Point configuration.
`import`	Imports the management database and applicable Check Point configuration that were exported from another Management Server.

Parameter	Description
`-l`	Exports and imports the Check Point logs *without* log indexes in the `$FWDIR/log/` directory. **Important:** ■ The command can export only closed logs (to which the information is not currently written). ■ If you use this parameter, it can take the command a long time to complete (depends on the number of logs).
`-x`	Exports and imports the Check Point logs *with* their log indexes in the `$FWDIR/log/` directory. **Important:** ■ This parameter only supports Management Servers and Log Servers R80.10 and higher. ■ The command can export only closed logs (to which the information is not currently written). ■ If you use this parameter, it can take the command a long time to complete (depends on the number of logs and indexes).
`-n`	Runs silently (non-interactive mode) and uses the default options for each setting. **Important:** ■ If you export a management database in this mode and the specified name of the exported file matches the name of an existing file, the command overwrites the existing file without prompting. ■ If you import a management database in this mode, the "`migrate import`" command runs the "`cpstop`" command automatically.
`--exclude-uepm-postgres-db`	■ During the export operation, does not back up the PostgreSQL database from the Endpoint Security Management Server. ■ During the import operation, does not restore the PostgreSQL database on the Endpoint Security Management Server.
`--include-uepm-msi-files`	■ During the export operation, backs up the MSI files from the Endpoint Security Management Server. ■ During the import operation, restores the MSI files on the Endpoint Security Management Server.
/<Full Path>/	Absolute path to the exported database file. This path must exist.

Parameter	Description
<Name of Exported File>	■ During the export operation, specifies the name of the output file. The command automatically adds the `*.tgz` extension. ■ During the import operation, specifies the name of the exported file. You must manually enter the `*.tgz` extension in the end.

Example 1 - Export operation succeeded

```
[Expert@MGMT:0]# cd $FWDIR/bin/upgrade_tools/
[Expert@MGMT:0]# ./migrate export /var/log/Migrate_Export

You are required to close all clients to Security Management Server
or execute 'cpstop' before the Export operation begins.

Do you want to continue? (y/n) [n]? y


Copying required files...
Compressing files...

The operation completed successfully.

Location of archive with exported database: /var/log/Migrate_Export.tgz

[Expert@MGMT:0]#
[Expert@MGMT:0]# find / -name migrate-\* -type f
/var/log/opt/CPshrd-R81.20/migrate-2019.06.14_11.03.46.log
[Expert@MGMT:0]#
```

Example 2 - Export operation failed

```
[Expert@MGMT:0]# ./migrate export /var/log/My_Migrate_Export
Execution finished with errors. See log file '/opt/CPshrd-R81.20/log/migrate-2019.06.14_
11.21.39.log' for further details
[Expert@MGMT:0]#
```

migrate_server

Important - This command is used to migrate the management database from R80.20.M1, R80.20, R80.20.M2, R80.30, and higher versions.
For more information, see:

- sk135172 - Upgrade Tools
- The *R81.20 Installation and Upgrade Guide*

Description

Exports the management database and applicable Check Point configuration.

Imports the exported management database and applicable Check Point configuration.

Backing up and restoring in Management High Availability environment:

- To back up and restore a consistent environment, make sure to collect and restore the backups and snapshots from all servers in the High Availability environment at the same time.
- Make sure other administrators do not make changes in SmartConsole until the backup operation is completed.

For more information:

- About Gaia Backup and Gaia Snapshot, see the *R81.20 Gaia Administration Guide*.
- About Virtual Machine Snapshots, see the vendor documentation.

Notes:

- You must run this command from the Expert mode.
- If it is necessary to back up the current management database, and you do **not** plan to import it on a Management Server that runs a higher software version, then you can use the built-in command in the `$FWDIR/scripts/` directory.
- If you plan to import the management database on a Management Server that runs a higher software version, then you must use the `migrate_server` utility from the migration tools package created specifically for that higher software version. See the **Installation and Upgrade Guide** for that higher software version.
- If this command completes successfully, it creates this log file:
  `/var/log/opt/CPshrd-R81.20/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  For example: */var/log/opt/CPshrd-R81.20/migrate-2022.06.14_11.03.46.log*
- If this command fails, it creates this log file:
  `$CPDIR/log/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  For example: */opt/CPshrd-R81.20/log/migrate-2022 - 2026.06.14_11.21.39.log*

Important - If it is necessary to back up the current management database, and you do **not** plan to import it on a Management Server that runs a higher software version, then you must make sure the source Management Server and the target Management Server run the same Jumbo Hotfix Accumulator Take and all other private hotfixes.
To see all the installed software packages, you can run this command: `cpinfo -y all`

Syntax

- To see the built-in help:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server -h
```

- To see the build number of the installed Upgrade Tools package:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server print_installed_tools -v
R81.20
```

- To run the Pre-Upgrade Verifier:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server verify -v R81.20 [-skip_
upgrade_tools_check]
```

- To export the management database and configuration:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server export -v R81.20 [-skip_
upgrade_tools_check] [-l | -x] [--include-uepm-msi-files] [--
exclude-uepm-postgres-db] [--ignore_warnings] /<Full
Path>/<Name of Exported File>
```

- To import the management database and configuration:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server import -v R81.20 [-skip_
upgrade_tools_check] [-l | -x] [/var/log/mdss.json] [--
include-uepm-msi-files] [--exclude-uepm-postgres-db] /<Full
Path>/<Name of Exported File>.tgz
```

- To import the Domain Management Server database and configuration on a Security Management Server:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server migrate_import_domain -v
R81.20 [-skip_upgrade_tools_check] [-l | -x]
[/var/log/mdss.json] [--include-uepm-msi-files] [--exclude-
uepm-postgres-db] /<Full Path>/<Name of Exported File>.tgz
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.

Parameter	Description
`--verify_all_servers`	Runs the Pre-Export Verifier for all Management Servers and Log Servers in your environment. **Notes**: ■ This parameter is valid only for the `migrate_server verify` and `migrate_server export` operations. ■ List of servers, on which you can run the `migrate_server verify -v <VERSION> --verify_all_servers` command and the `migrate_server export -v <VERSION> --verify_all_servers` command: • Security Management Server (Primary and Secondary) • Multi-Domain Security Management Server (Primary and Secondary) • Endpoint Security Management Server (Primary and Secondary) • Endpoint Security Management Server (Primary and Secondary) • Multi-Domain Log Server ■ List of remote servers, to which the `migrate_server verify -v <VERSION> --verify_all_servers` command and the `migrate_server export -v <VERSION> --verify_all_servers` command can connect from the current server: • Security Management Server (Primary and Secondary) • Multi-Domain Security Management Server (Primary and Secondary) • Endpoint Security Management Server (Primary and Secondary) • Endpoint Security Management Server (Primary and Secondary) • Multi-Domain Log Server • Dedicated Log Servers • Dedicated SmartEvent Servers • Security Management Servers configured as a Backup of a Domain Management Server **Note** - Servers that are configured on a specific Domain on a Multi-Domain Security Management Server will be verified only if there is a Domain Server of that Domain on the current Multi-Domain Security Management Server.

Parameter	Description
`--verify_local_only`	Runs the Pre-Export Verifier only for the current Management Server / Log Server, on which you run this command. **Note** - This parameter is valid only for the `migrate_server verify` and `migrate_server export` operations.
`-skip_tools_check_on_remote`	The remote Management Server / Log Servers do not try to connect to Check Point Cloud to check for a more recent version of the Upgrade Tools. **Notes**: ■ This parameter is valid only for the `migrate_server verify` and `migrate_server export` operations. ■ This parameter is valid only when you specify the parameter `--verify_all_servers`.
`export`	Exports the management database and applicable Check Point configuration.

Parameter	Description

`import`	Imports the management database and applicable Check Point configuration that were exported from another Management Server.
	Important:
	■ This command automatically restarts Check Point services (runs the "`cpstop`" and "`cpstart`" commands).
	■ This note applies to a Multi-Domain Security Management environment, if at least one of the servers changes its IPv4 address comparing to the source server, from which you exported its database.
	You must do these steps **before** you start the upgrade and import:
	1. You must create a special JSON configuration file with the new IPv4 address(es).
	Syntax:
	`[{"name":"<Name of Server 1 Object in SmartConsole>","newIpAddress4":"<New IPv4 Address of Server 1>"},`
	`{"name":"<Name of Server 2 Object in SmartConsole>","newIpAddress4":"<New IPv4 Address of Server 2>"}]`
	Example:
	`[{"name":"MyPrimaryMultiDomainServer","newIpAddress4":"172.30.40.51"},`
	`{"name":"MySecondaryMultiDomainServer","newIpAddress4":"172.30.40.52"}]`
	2. You must call this file: **mdss.json**
	3. You must put this file on **all** servers in this directory: **/var/log/**

`migrate_import_domain`	On a Security Management Server, imports the management database and applicable Check Point configuration that were exported from a Domain Management Server. **Important** - This command automatically restarts Check Point services (runs the "`cpstop`" and "`cpstart`" commands).
`verify`	Verifies the management database and applicable Check Point configuration that were exported from another Management Server.
`-v R81.20`	Specifies the version, to which you plan to migrate / upgrade.

Parameter	Description
`-skip_ upgrade_ tools_check`	The current Management Server / Log Server, on which you run this command, does not try to connect to Check Point Cloud to check for a more recent version of the Upgrade Tools. **Best Practice** - Use this parameter on the Management Server / Log Server that is **not** connected to the Internet.
`-l`	Exports and imports the Check Point logs *without* log indexes in the `$FWDIR/log/` directory. **Important:** ■ The command can export only closed logs (to which the information is not currently written). ■ If you use this parameter, it can take the command a long time to complete (depends on the number of logs).
`-l <Days>`	Exports the specified number of previous days of logs without log indexes.
`-x`	Exports and imports the Check Point logs *with* their log indexes in the `$FWDIR/log/` directory. **Important:** ■ Before you use this parameter, it is necessary to make sure all log indexes are closed and saved. Run this command in the Expert mode and wait for the output to show "`Solr stopped`": `$RTDIR/scripts/stopSolr.sh` ■ This parameter only supports Management Servers and Log Servers R80.10 and higher. ■ The command can export only closed logs (to which the information is not currently written). ■ If you use this parameter, it can take the command a long time to complete (depends on the number of logs and indexes).
`-x <Days>`	Exports the specified number of previous days of logs with log indexes.
`-n`	Runs silently (non-interactive mode) and uses the default options for each setting.

Parameter	Description

`/var/log/mdss.json`
 	
Previously:
`-change_ips_file /<Full Path>/<Name>.json`
	Important:
	■ In the Upgrade Tools for R81.10 build higher than 996000356, the syntax is (this filename is mandatory):
	`/var/log/mdss.json`
	You must create the file **/var/log/mdss.json** and not use the parameter "**-change_ips_file**".
	■ In the Upgrade Tools for R81.10 build 996000356 and lower, the syntax was:
	`-change_ips_file /<Full Path>/<Name of JSON File>.json`
	
	Specifies the absolute path to the special JSON configuration file with new IPv4 addresses.
	This file is mandatory during an upgrade of a Multi-Domain Security Management environment.
	Even if only one of the servers migrates to a new IP address, all the other servers must get this configuration file for the import process.
	Syntax:
	`[{"name":"<Name of Server 1 Object in SmartConsole>","newIpAddress4":"<New IPv4 Address of Server 1>"},`
	`{"name":"<Name of Server 2 Object in SmartConsole>","newIpAddress4":"<New IPv4 Address of Server 2>"}]`
	Example:
	`[{"name":"MyPrimaryMultiDomainServer","newIpAddress4":"172.30.40.51"},`
	`{"name":"MySecondaryMultiDomainServer","newIpAddress4":"172.30.40.52"}]`

`--include-uepm-msi-files`	■ During the export operation, backs up the MSI files from the Endpoint Security Management Server. ■ During the import operation, restores the MSI files on the Endpoint Security Management Server.
`--exclude-uepm-postgres-db`	■ During the export operation, does not back up the PostgreSQL database from the Endpoint Security Management Server. ■ During the import operation, does not restore the PostgreSQL database on the Endpoint Security Management Server.

Parameter	Description
`--ignore_warnings` or `-ivw`	If during an upgrade procedure, the Pre-Upgrade Verifier shows warnings, you can use this parameter to ignore warnings and continue the upgrade. **Important** - To prevent issues during and after upgrade, we strongly recommend to resolve all issues and not use this parameter.
`--exclude-licenses`	■ During the export operation, does not back up the licenses from the Management Server. ■ During the import operation, does not restore the license on the Management Server.
`-force-upgrade-flow`	When the source and target servers are on the same major version: ■ "`migrate_server`" uses an accelerated flow to migrate the data. ■ This flag forces the full migration flow.
`-mask`	Hides sensitive information in exported database.
`--no_progress_bar` or `-npb`	Disables the progress bar.
`-o <Path to File>`	Path to the archived file from which to import the database.
`-sn <Name of Domain Server>`	Name of the Domain Management Server
`-dsi <IP address of Domain Server>`	IP address of the Management Server.
`-skip_logs`	Skips the import of logs (without log indexes).

Example 1 - Export operation succeeded

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server export -v R81.20 /var/log/Migrate_Export

You are required to close all clients to Security Management Server
or execute 'cpstop' before the Export operation begins.

Do you want to continue? (y/n) [n]? y


Copying required files...
Compressing files...

The operation completed successfully.

Location of archive with exported database: /var/log/Migrate_Export.tgz

[Expert@MGMT:0]#
[Expert@MGMT:0]# find / -name migrate-\* -type f
/var/log/opt/CPshrd-R81.20/migrate-2022 - 2026.06.14_11.03.46.log
[Expert@MGMT:0]#
```

Example 2 - Export operation failed

```
[Expert@MGMT:0]# ./migrate_server export /var/log/My_Migrate_Export
Execution finished with errors. See log file '/opt/CPshrd-R81.20/log/migrate-2022 - 2026.06.14_
11.21.39.log' for further details
[Expert@MGMT:0]#
```

queryDB_util

Description

Searches in the management database for objects or policy rules.

Important - This command is obsolete for R80 and higher. Use the *"mgmt_cli" on page 386* command to search in the management database for objects or policy rules according to search parameters.

rs_db_tool

Description

Manages Dynamically Assigned IP address (DAIP) gateways in a DAIP database.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

- **To add an entry to the DAIP database:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation add -name <Object Name> -ip <IPv4 Address> -ip6 <Pv6 Address> -TTL <Time-To-Live>
```

- **To fetch a specific entry from the DAIP database:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation fetch -name <Object Name>
```

- **To delete a specific entry from the DAIP database:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation delete -name <Object Name>
```

- **To list all entries in the DAIP database:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation list
```

- **To synchronize the DAIP database:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation sync
```

Note - You must run this command from the Expert mode.

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-name <Object Name>`	Specifies the name of the DAIP object.
`-ip <IPv4 Address>`	Specifies the IPv4 address of the DAIP object
`-ip6 <IPv6 Address>`	Specifies the IPv6 address of the DAIP object.
`-TTL <Time-To-Live>`	Specifies the relative time interval (in seconds), during which the entry is valid.

sam_alert

Description

For SAM v1, this utility executes Suspicious Activity Monitoring (SAM) actions according to the information received from the standard input.

For SAM v2, this utility executes Suspicious Activity Monitoring (SAM) actions with User Defined Alerts mechanism.

Important:

- You must run this command on the Management Server.
- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Notes:

- VSX Gateways and VSX Cluster Members do **not** support Suspicious Activity Monitoring (SAM) Rules. See sk79700.
- See the *"fw sam" on page 295* and *"fw sam_policy" on page 303* commands.

SAM v1 syntax

```
sam_alert [-v] [-o] [-s <SAM Server>] [-t <Time>] [-f <Security
Gateway>] [-C] {-n|-i|-I} {-src|-dst|-any|-srv}
```

Parameters for SAM v1

Parameter	Description
`-v`	Enables the verbose mode for the "`fw sam`" command.
`-o`	Specifies to print the input of this tool to the standard output (to use with pipes in a CLI syntax).
`-s <SAM Server>`	Specifies the SAM Server to be contacted. Default is "localhost".
`-t <Time>`	Specifies the time (in seconds), during which to enforce the action. The default is forever.

Parameter	Description
`-f <Security Gateway>`	Specifies the Security Gateway / Cluster object, on which to run the operation. **Important** - If you do not specify the target Security Gateway / Cluster object explicitly, this command applies to all managed Security Gateways and Clusters.
`-C`	Cancels the specified operation.
`-n`	Specifies to notify every time a connection, which matches the specified criteria, passes through the Security Gateway / ClusterXL / Security Group.
`-i`	Inhibits (drops or rejects) connections that match the specified criteria.
`-I`	Inhibits (drops or rejects) connections that match the specified criteria and closes all existing connections that match the specified criteria.
`-src`	Matches the source address of connections.
`-dst`	Matches the destination address of connections.
`-any`	Matches either the source or destination address of connections.
`-srv`	Matches specific source, destination, protocol and port.

SAM v2 syntax

```
sam_alert -v2 [-v] [-O] [-S <SAM Server>] [-t <Time>] [-f
<Security Gateway>] [-n <Name>] [-c "<Comment">] [-o
<Originator>] [-l {r | a}] -a {d | r| n | b | q | i} [-C] {-ip
|-eth} {-src|-dst|-any|-srv}
```

Parameters for SAM v2

Parameter	Description
`-v2`	Specifies to use SAM v2.
`-v`	Enables the verbose mode for the "`fw sam`" command.
`-O`	Specifies to print the input of this tool to the standard output (to use with pipes in a CLI syntax).
`-S <SAM Server>`	Specifies the SAM server to be contacted. Default is "localhost".
`-t <Time>`	Specifies the time (in seconds), during which to enforce the action. The default is forever.
`-f <Security Gateway>`	Specifies the Security Gateway / Cluster object, on which to run the operation. **Important** - If you do not specify the target Security Gateway / Cluster object explicitly, this command applies to all managed Security Gateways and Clusters.
`-n <Name>`	Specifies the name for the SAM rule. Default is empty.
`-c "<Comment>"`	Specifies the comment for the SAM rule. Default is empty. You must enclose the text in the double quotes or single quotes.
`-o <Originator>`	Specifies the originator for the SAM rule. Default is "`sam_alert`".

Parameter	Description
`-l {r | a}`	Specifies the log type for connections that match the specified criteria: ■ `r` - Regular ■ `a` - Alert Default is `None`.
`-a {d | r| n | b | q | i}`	Specifies the action to apply on connections that match the specified criteria: ■ `d` - Drop ■ `r` - Reject ■ `n` - Notify ■ `b` - Bypass ■ `q` - Quarantine ■ `i` - Inspect
`-C`	Specifies to close all existing connections that match the criteria.
`-ip`	Specifies to use IP addresses as criteria parameters.
`-eth`	Specifies to use MAC addresses as criteria parameters.
`-src`	Matches the source address of connections.
`-dst`	Matches the destination address of connections.
`-any`	Matches either the source or destination address of connections.
`-srv`	Matches specific source, destination, protocol and port.

Example

See sk110873: How to configure Security Gateway to detect and prevent port scan.

stattest

Description

Check Point AMON client to query SNMP OIDs.

You can use this command as an alternative to the standard SNMP commands for debug purposes - to make sure the applicable SNMP OIDs provide the requested information.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax to query a Regular OID

- On a Management Server / Security Gateway / Cluster Member:

```
stattest get [-d] [-h <Host>] [-p <Port>] [-x <Proxy Server>] [-v <VSID>] [-t <Timeout>] <Regular_OID_1> <Regular_OID_2> ...
<Regular_OID_N>
```

- On a Scalable Platform Security Group:

```
g_all stattest get [-d] [-h <Host>] [-p <Port>] [-x <Proxy Server>] [-v <VSID>] [-t <Timeout>] <Regular_OID_1> <Regular_OID_2>
... <Regular_OID_N>
```

Notes:

- These Regular OIDs are specified in the SNMP MIB files.
- For Check Point MIB files, see sk90470.

Syntax to query a Statistical OID

- On a Management Server / Security Gateway / Cluster Member:

```
stattest get [-d] [-h <Host>] [-p <Port>] [-x <Proxy Server>] -l <Polling Interval> -r <Polling Duration> [-v <VSID>] [-t
<Timeout>] <Statistical_OID_1> <Statistical_OID_2> ... <Statistical_OID_N>
```

- On a Scalable Platform Security Group:

```
g_all stattest get [-d] [-h <Host>] [-p <Port>] [-x <Proxy Server>] -l <Polling Interval> -r <Polling Duration> [-v <VSID>] [-t
<Timeout>] <Statistical_OID_1> <Statistical_OID_2> ... <Statistical_OID_N>
```

Notes:

- These Statistical OIDs take some time to "initialize".
- For example, to calculate an average, it is necessary to collect enough samples.
- Check Point statistical OIDs are registered in the `$CPDIR/conf/statistical_oid.conf` file.

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-h <Host>`	Specifies the remote Check Point host to query by its IP address or resolvable hostname.
`-p <Port>`	Specifies the port number, on which the AMON server listens. Default port is 18192.
`-x <Proxy Server>`	Specifies the Proxy Server by its IP address or resolvable hostname. **Note** - Use only when you query a remote host.
`-l <Polling Interval>`	Specifies the time in seconds between queries. **Note** - Use only when you query a Statistical OID.

Parameter	Description
`-r <Polling Duration>`	Specifies the time in seconds, during which to run consecutive queries. **Note** - Use only when you query a Statistical OID.
`-v <VSID>`	On a VSX Gateway, specifies the context of a Virtual Device to query.
`-t <Timeout>`	Specifies the session timeout in milliseconds.
`<Regular_OID_1> <Regular_OID_2> ... <Regular_OID_N>`	Specifies the Regular OIDs to query. **Notes:** ■ OID must not start with period. ■ Separate the OIDs with spaces. ■ You can specify up to 100 OIDs.
`<Statistical_OID_1> <Statistical_OID_2> ... <Statistical_OID_N>`	Specifies the Statistical OIDs to query. **Notes:** ■ OID must not start with period. ■ Separate the OIDs with spaces. ■ You can specify up to 100 OIDs.

Example - Query a Regular OID

Query the CPU Idle utilization at the OID 1.3.6.1.4.1.2620.1.6.7.2.3 (`procIdleTime`).

```
[Expert@HostName]# stattest get 1.3.6.1.4.1.2620.1.6.7.4.2
```

Example - Query a Statistical OID

Query the CPU Idle utilization at the OID 1.3.6.1.4.1.2620.1.6.7.2.3 (`procIdleTime`).

Information is collected with intervals of 5 seconds during 5 seconds

```
[Expert@HostName]# stattest get -l 5 -r 5 1.3.6.1.4.1.2620.1.6.7.2.3
```

threshold_config

Description

You can configure a variety of different SNMP thresholds that generate SNMP traps, or alerts.

You can use these thresholds to monitor many system components automatically without requesting information from each object or device.

You configure these SNMP Monitoring Thresholds only on the Security Management Server, Multi-Domain Server, or Domain Management Server.

During policy installation, the managed a Security Gateway and Clusters receive and apply these thresholds as part of their policy.

For more information, see sk90860: How to configure SNMP on Gaia OS.

Procedure

Step	Instructions
1	Connect to the command line on the Management Server.
2	Log in to the Expert mode.
3	On a Multi-Domain Server, switch to the context of the applicable Domain Management Server: `[Expert@HostName:0]# mdsenv <Name or IP address of Domain Management Server>`
4	Go to the Threshold Engine Configuration menu: `[Expert@HostName:0]# threshold_config`

Step	Instructions

5	Select the applicable options and configure the applicable settings (see the **Threshold Engine Configuration Options** table below).
	`Threshold Engine Configuration Options:`
	`----------`
	
	`(1) Show policy name`
	`(2) Set policy name`
	`(3) Save policy`
	`(4) Save policy to file`
	`(5) Load policy from file`
	`(6) Configure global alert settings`
	`(7) Configure alert destinations`
	`(8) View thresholds overview`
	`(9) Configure thresholds`
	
	`(e) Exit (m) Main Menu`
	
	`Enter your choice (1-9) :`

6	Exit from the Threshold Engine Configuration menu.
7	Stop the CPD daemon: `[Expert@HostName:0]# cpwd_admin stop -name CPD -path "$CPDIR/bin/cpd_admin" -command "cpd_admin stop"` See *"cpwd_admin stop" on page 248*.
8	Start the CPD daemon: `[Expert@HostName:0]# cpwd_admin start -name CPD -path "$CPDIR/bin/cpd" -command "cpd"` See *"cpwd_admin start" on page 244*.
9	Wait for 10-20 seconds.
10	Verify that CPD daemon started successfully: `[Expert@HostName:0]# cpwd_admin list | egrep "STAT|CPD"` See *"cpwd_admin list" on page 238*.
11	In SmartConsole, install the Access Control Policy on Security Gateways and Clusters.

Threshold Engine Configuration Options

Menu item	Description
`(1) Show policy name`	Shows the name of the current configured threshold policy.
`(2) Set policy name`	Configures the name for the threshold policy. If you do not specify it explicitly, then the default name is "`Default Profile`".
`(3) Save policy`	Saves the changes in the current threshold policy.
`(4) Save policy to file`	Exports the configured threshold policy to a file. If you do not specify the path explicitly, the file is saved in the current working directory.
`(5) Load policy from file`	Imports a threshold policy from a file. If you do not specify the path explicitly, the file is imported from the current working directory.
`(6) Configure global alert settings`	Configures global settings: ■ How frequently alerts are sent (configured delay must be greater than 30 seconds) ■ How many alerts are sent

`(7) Configure alert destinations`	Configures the SNMP Network Management System (NMS), to which the managed Security Gateways and Cluster Members send their SNMP alerts.
	`Configure Alert Destinations Options:`
	`----------`
	`(1) View alert destinations`
	`(2) Add SNMP NMS`
	`(3) Remove SNMP NMS`
	`(4) Edit SNMP NMS`

`(8) View thresholds overview`	Shows a list of all available thresholds and their current settings. These include: ■ Name ■ Category (see the next option "`(9)`") ■ State (disabled or enabled) ■ Threshold (threshold point, if applicable) ■ Description

Menu item	Description

(9) Configure thresholds	Shows the list of threshold categories to configure.
	`Thresholds Categories`
	`----------`
	`(1) Hardware`
	`(2) High Availability`
	`(3) Local Logging Mode Status`
	`(4) Log Server Connectivity`
	`(5) Networking`
	`(6) Resources`
	See the **Thresholds Categories** table below.

Thresholds Categories

Category	Sub-Categories

(1) Hardware	`Hardware Thresholds:`
	`----------`
	`(1) RAID volume state`
	`(2) RAID disk state`
	`(3) RAID disk flags`
	`(4) Temperature sensor reading`
	`(5) Fan speed sensor reading`
	`(6) Voltage sensor reading`

(2) High Availability	`High Availability Thresholds:`
	`----------`
	`(1) Cluster member state changed`
	`(2) Cluster block state`
	`(3) Cluster state`
	`(4) Cluster problem status`
	`(5) Cluster interface status`

(3) Local Logging Mode Status	`Local Logging Mode Status Thresholds:`
	`----------`
	`(1) Local Logging Mode`

(4) Log Server Connectivity	`Log Server Connectivity Thresholds:`
	`----------`
	`(1) Connection with log server`
	`(2) Connection with all log servers`

Category	Sub-Categories
(5) Networking	Networking Thresholds: ---------- (1) Interface Admin Status (2) Interface removed (3) Interface Operational Link Status (4) New connections rate (5) Concurrent connections rate (6) Bytes Throughput (7) Accepted Packet Rate (8) Drop caused by excessive traffic
(6) Resources	Resources Thresholds: ---------- (1) Swap Memory Utilization (2) Real Memory Utilization (3) Partition free space (4) Core Utilization (5) Core interrupts rate

Notes:

- If you run the `threshold_config` command *locally* on a Security Gateway or Cluster Members to configure the SNMP Monitoring Thresholds, then each policy installation erases these *local* SNMP threshold settings and reverts them to the *global* SNMP threshold settings configured on the Management Server that manages this Security Gateway or Cluster.
- On a Security Gateway and Cluster Members, you can save the local Threshold Engine Configuration settings to a file and load it locally later.
- The Threshold Engine Configuration is stored in the `$FWDIR/conf/thresholds.conf` file.
- In a Multi-Domain Security Management environment:
  - You can configure the SNMP thresholds in the context of Multi-Domain Server (MDS) and in the context of each individual Domain Management Server.
  - Thresholds that you configure in the context of the Multi-Domain Server are for the Multi-Domain Server only.
  - Thresholds that you configure in the context of a Domain Management Server are for that Domain Management Server and its managed Security Gateway and Clusters.
  - If an SNMP threshold applies both to the Multi-Domain Server and a Domain Management Server, then configure the SNMP threshold both in the context of the Multi-Domain Server and in the context of the Domain Management Server.
    However, in this scenario you can only get alerts from the Multi-Domain Server, if the monitored object exceeds the threshold.
    Example:
    If you configure the CPU threshold, then when the monitored value exceeds the configured threshold, it applies to both the Multi-Domain Server and the Domain Management Server. However, only the Multi-Domain Server generates SNMP alerts.

Multi-Domain Security Management Commands

For more information about Multi-Domain Server, see the *R81.20 Multi-Domain Security Management Administration Guide*.

In addition, see *"Security Management Server Commands" on page 44*.

Managing Security through API

This section describes the API Server on a Management Server and the applicable API Tools.

API

You can configure and manage the Management Server through API Requests that you send to the API Server that runs on the Management Server.

The API Server can automate daily tasks and integrate Check Point solutions with third party systems, such as virtualization, ticketing, and change management systems.

To learn more about the management APIs, to see code samples, and to take advantage of user forums, see:

- The API Documentation:
  - Online - *Check Point Management API Reference* (at the top, select the correct version)
  - Local - `https://<Server IP Address>/api_docs/#introduction`

    By default, access to the local API Documentation is disabled. Follow the instructions in sk174606.

    Note - On a Standalone server (a server which runs both a Security Management Server and a Security Gateway), the API Documentation web portal (`https://<Server IP Address>/api_docs`) stops working when you open SmartView Web Application (`https://<Server IP Address>/smartview`).
- The **Developers Network** section of *Check Point CheckMates Community*.

API Tools

You can use these tools to work with the API Server on the Management Server:

- Standalone management tool, included with Gaia operating system:

  `mgmt_cli`
- Standalone management tool, included with SmartConsole:

  `mgmt_cli.exe`

  You can copy this tool from the SmartConsole installation folder to other computers that run Windows operating system.
- Web Services APIs that allow communication and data exchange between the clients and the Management Server over the HTTP protocol.

These APIs also let other Check Point processes communicate with the Management Server over the HTTPS protocol.

`https://<IP Address of Management Server>/web_api/<command>`

Configuring the API Server

To configure the API Server:

1. Connect with SmartConsole to the Security Management Server or applicable Domain Management Server.
2. From the left navigation panel, click **Manage & Settings**.
3. In the upper left section, click **Blades**.
4. In the **Management API** section, click **Advanced Settings**.

   The **Management API Settings** window opens.
5. Configure the **Startup Settings** and the **Access Settings**.

   Configuring Startup Settings

   Select **Automatic start** to automatically start the API server when you start or reboot the Management Server.

   Notes:
   - If the Management Server has more than 4GB of RAM installed, the **Automatic start** option is activated by default during Management Server installation.
   - If the Management Server has less than 4GB of RAM, the **Automatic Start** option is deactivated.

Configuring Access Settings

Select one of these options to configure which clients can connect to the API Server:

- **Management server only** - Only the Management Server itself can connect to the API Server. This option only lets you use the `mgmt_cli` utility on the Management Server to send API requests. You cannot use SmartConsole or Web services to send API requests.
- **All IP addresses that can be used for GUI clients** - You can send API requests from all IP addresses that are defined as **Trusted Clients** in SmartConsole. This includes requests from SmartConsole, Web services, and the `mgmt_cli` utility on the Management Server.
- **All IP addresses** - You can send API requests from all IP addresses. This includes requests from SmartConsole, Web services, and the `mgmt_cli` utility on the Management Server.

6. Click **OK**.
7. In the upper left section, click **Permissions & Administrators**.
8. In the object of each applicable Administrator, make sure the assigned Permission Profile allows access to Management API.

   Instructions

   a. Edit the Administrator object.
   b. In the left panel, click **General**.
   c. In the **Permissions** section, on the right side of the selected Permission Profile, click the eye icon.

      The Permission Profile object opens in the read-only view.
   d. In the left panel, click **Management**.
   e. The permission **Management API Login** has to be selected.

      If it is not selected, then close this window and edit this Permission Profile object.
   f. Click **Close**.

9. Publish the SmartConsole session.
10. Restart the API Server on the Management Server with this command:

```
api restart
```

Notes:

- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

- The output of this command must show:

```
API started successfully
```

11. Examine the status of the API server on the Management Server with this command:

```
api status
```

Notes:

- The output of this command must show:

```
------------------------------------------
Overall API Status: Started
------------------------------------------

API readiness test SUCCESSFUL. The server is up and ready
to receive connections
```

- The output of this command may show the state of the "**API**" process as "**Stopped**" when the API access is set to "**All IP addresses that can be used for GUI clients**", and more than 200 Trusted Clients are configured:

```
Processes:

Name       State     PID       More Information
-----------------------------------------------
API        Stopped   ...
```

Discarding API Sessions with Locks or Pending Changes

Open SmartConsole and API sessions that contain locks or unpublished changes are not automatically discarded. As a result, some sessions can remain open for extended periods.

The `ENABLE_DISCARD_WORKSESSIONS_OLDER_THAN_DAYS` environment variable controls whether stale open sessions are automatically discarded. By default, this variable is disabled, and open sessions with locks or unpublished changes remain available until they are manually discarded.

When enabled, the Security Management Server periodically evaluates open sessions and discards sessions that exceed the configured age threshold.

To configure automatic discard of stale sessions:

1. Connect to the Security Management Server or Multi-Domain Server using SSH.
2. Switch to Expert mode.
3. To enable automatic discard of open sessions that contain locks or unpublished changes, set `ENABLE_DISCARD_WORKSESSIONS_OLDER_THAN_DAYS` to "`true`".

   Run:

   ```
   MDS_FWDIR/scripts/reload_env_vars.sh -e "ENABLE_DISCARD_
   WORKSESSIONS_OLDER_THAN_DAYS=true"
   ```

   ```
   $MDS_FWDIR/scripts/override_server_setting.sh -e ENABLE_DISCARD_
   WORKSESSIONS_OLDER_THAN_DAYS true
   ```
4. By default, only sessions which are open for more than 60 days are automatically discarded. To configure the number of days after which sessions are discarded, run:

   ```
   $MDS_FWDIR/scripts/reload_env_vars.sh -e "DISCARD_WORKSESSIONS_
   OLDER_THAN_DAYS=<Number_of_Days>" $MDS_FWDIR/scripts/override_
   server_setting.sh -e DISCARD_WORKSESSIONS_OLDER_THAN_DAYS
   <Number_of_Days>
   ```

   For example, to set the threshold to 30 days, run:

   ```
   $MDS_FWDIR/scripts/reload_env_vars.sh -e "DISCARD_WORKSESSIONS_
   OLDER_THAN_DAYS=30"
   $MDS_FWDIR/scripts/override_server_setting.sh -e DISCARD_
   WORKSESSIONS_OLDER_THAN_DAYS 30
   ```

Result:

When `ENABLE_DISCARD_WORKSESSIONS_OLDER_THAN_DAYS` is set to "`true`":

- The Security Management Server checks all open SmartConsole and API sessions one time per day.
- If a session remains open longer than the number of days configured in `DISCARD_WORKSESSIONS_OLDER_THAN_DAYS`, the session is automatically discarded.

cma_migrate

Description

On the applicable target Domain Management Server, imports the management database that was exported from an R7x Domain Management Server.

Note - This command updates the database schema before it imports. First, the command runs pre-upgrade verification. If no errors are found, migration continues. If there are errors, you must fix them on the source R7x Domain Management Server according to instructions in the error messages. Then do this procedure again.

For the complete procedure, see the *R81.20 Installation and Upgrade Guide*.

Syntax

```
cma_migrate /<Full Path>/<Name of R7x Domain Exported File>.tgz
/<Full Path>/<$FWDIR Directory of the New Domain Management
Server>/
```

Example

```
[Expert@R81.20_MDS:0]# cma_migrate /var/log/orig_R7x_database.tgz
/opt/CPmds-R81.20/customers/MyDomain3/CPsuite-R81.20/fw1/
```

contract_util

Description

Works with the Check Point Service Contracts.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util [-d]
    check <options>
    cpmacro <options>
    download <options>
    mgmt
    print <options>
    summary <options>
    update <options>
    verify
```

Parameters

Parameter	Description
`check <options>`	Checks whether the Security Gateway is eligible for an upgrade. See *"contract_util check" on page 52*.
`cpmacro <options>`	Overwrites the current `cp.macro` file with the specified `cp.macro` file. See *"contract_util cpmacro" on page 53*.
`download <options>`	Downloads all associated Check Point Service Contracts from the User Center, or from a local file. See *"contract_util download" on page 54*.
`mgmt`	Delivers the Service Contract information from the Management Server to the managed Security Gateways. See *"contract_util mgmt" on page 56*.
`print <options>`	Shows all the installed licenses and whether the Service Contract covers these license, which entitles them for upgrade or not. See *"contract_util print" on page 57*.

Parameter	Description
`summary <options>`	Shows post-installation summary. See *"contract_util summary" on page 58*.
`update <options>`	Updates Check Point Service Contracts from your User Center account. See *"contract_util update" on page 59*.
`verify`	Checks whether the Security Gateway is eligible for an upgrade. This command also interprets the return values and shows a meaningful message. See *"contract_util verify" on page 60*.

contract_util check

Description

Checks whether the Security Gateway is eligible for an upgrade.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util check
    {-h | -help}
    hfa
    maj_upgrade
    min_upgrade
    upgrade
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`hfa`	Checks whether the Security Gateway is eligible for an upgrade to a higher Hotfix Accumulator.
`maj_upgrade`	Checks whether the Security Gateway is eligible for an upgrade to a higher Major version.
`min_upgrade`	Checks whether the Security Gateway is eligible for an upgrade to a higher Minor version.
`upgrade`	Checks whether the Security Gateway is eligible for an upgrade.

contract_util cpmacro

Description

Overwrites the current `cp.macro` file with the specified `cp.macro` file, if the specified is newer than the current file.

For more information about the `cp.macro` file, see sk96217: What is a cp.macro file?

Syntax

```
contract_util cpmacro /<path_to>/cp.macro
```

This command shows one of these messages:

Message	Description
`CntrctUtils_ Write_cp_macro returned -1`	The `contract_util cpmacro` command failed: ■ Failed to create a temporary file. ■ Failed to write to a temporary file. ■ Failed to replace the current file.
`CntrctUtils_ Write_cp_macro returned 0`	The `contract_util cpmacro` command was able to overwrite the current file with the specified file, because the specified file is newer.
`CntrctUtils_ Write_cp_macro returned 1`	The `contract_util cpmacro` command did not overwrite the current file, because it is newer than the specified file.

contract_util download

Description

Downloads all associated Check Point Service Contracts from User Center, or from a local file.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util download
      {-h | -help}
      local
            {-h | -help}
            [{hfa | maj_upgrade | min_upgrade | upgrade}] <Service
Contract File>
      uc
            {-h | -help}
            [-i] [{hfa | maj_upgrade | min_upgrade | upgrade}]
<Username> <Password> [<Proxy Server> [<Proxy Username>:<Proxy
Password>]]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-i`	Interactive mode - prompts the user for the User Center credentials and proxy server settings.
`local`	Specifies to download the Service Contract from the local file. This is equivalent to the "`cplic contract put`" command (see *"cplic contract" on page 142*).
`uc`	Specifies to download the Service Contract from the User Center.
`hfa`	Downloads the information about a Hotfix Accumulator.
`maj_upgrade`	Downloads the information about a Major version.
`min_upgrade`	Downloads the information about a Minor version.
`upgrade`	Downloads the information about an upgrade.
<Username>	Your User Center account e-mail address.
<Password>	Your User Center account password.
<Proxy Server> `[`*<Proxy Username>*`:`*<Proxy Password>*`]`	Specifies that the connection to the User Center goes through the proxy server. ■ *<Proxy Server>* - IP address of resolvable hostname of the proxy server ■ *<Proxy Username>* - Username for the proxy server. ■ *<Proxy Password>* - Password for the proxy server. Note - If you do not specify the proxy server explicitly, the command uses the proxy server configured in the management database.
<Service Contract File>	Path to and the name of the Service Contract file. First, you must download the Service Contract file from your User Center account.

contract_util mgmt

Description

Delivers the Service Contract information from the Management Server to the managed Security Gateways.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util mgmt
```

contract_util print

Description

Shows all the installed licenses and whether the Service Contract covers these license, which entitles them for upgrade or not.

This command can show which licenses are not recognized by the Service Contract file.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util [-d] print
      {-h | -help}
      hfa
      maj_upgrade
      min_upgrade
      upgrade
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Shows a formatted table header and more information.
`hfa`	Shows the information about Hotfix Accumulator.
`maj_upgrade`	Shows the information about Major version.
`min_upgrade`	Shows the information about Minor version.
`upgrade`	Shows the information about an upgrade.

contract_util summary

Description

Shows post-installation summary and whether this Check Point server is eligible for upgrades.

Syntax

```
contract_util summary
      hfa
      maj_upgrade
      min_upgrade
      upgrade
```

Parameters

Parameter	Description
`hfa`	Shows the information about Hotfix Accumulator.
`maj_upgrade`	Shows the information about Major version.
`min_upgrade`	Shows the information about Minor version.
`upgrade`	Shows the information about an upgrade.

contract_util update

Description

Updates the Check Point Service Contracts from your User Center account.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util update
      [-proxy <Proxy Server>:<Proxy Port>]
      [-ca_path <Path to ca-bundle.crt File>]
```

Parameters

Parameter	Description
`update`	Updates Check Point Service Contracts (attached to pre-installed licenses) from your User Center account.
`-proxy <Proxy Server>:<Proxy Port>`	Specifies that the connection to the User Center goes through the proxy server: ■ *<Proxy Server>* - IP address of resolvable hostname of the proxy server. ■ *<Proxy Port>* - The applicable port on the proxy server. Note - If you do not specify the proxy explicitly, the command uses the proxy configured in the management database.
`-ca_path <Path to ca-bundle.crt File>`	Specifies the path to the Certificate Authority Bundle file (`ca-bundle.crt`). **Note** - If you do not specify the path explicitly, the command uses the default path.

contract_util verify

Description

Checks whether the Security Gateway is eligible for an upgrade.

This command is the same as the *"contract_util check" on page 52* command, but it also interprets the return values and shows a meaningful message.

For more information about Service Contract files, see sk33089: What is a Service Contract File?

Syntax

```
contract_util verify
```

cp_conf

Description

Configures or reconfigures a Check Point product installation.

Note - The available options for each Check Point server depend on the configuration and installed products.

Syntax on a Management Server

```
cp_conf
      -h
      admin <options>
      auto <options>
      ca <options>
      client <options>
      finger <options>
      lic <options>
      snmp <options>
```

Syntax on a Security Gateway / each Cluster Member in Gaia Clish or the Expert mode

```
cp_conf
      -h
      adv_routing <options>
      auto <options>
      corexl <options>
      fullha <options>
      ha <options>
      intfs <options>
      lic <options>
      sic <options>
      snmp <options>
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cp_conf
      -h
      adv_routing <options>
      auto <options>
      corexl <options>
      fullha <options>
      ha <options>
      intfs <options>
      lic <options>
      sic <options>
      snmp <options>
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cp_conf
      -h
      adv_routing <options>
      auto <options>
      corexl <options>
      fullha <options>
      ha <options>
      intfs <options>
      lic <options>
      sic <options>
      snmp <options>
```

Parameters

Parameter	Description
`-h`	Shows the entire built-in usage.
`admin <options>`	Configures Check Point system administrators for the Security Management Server. See *"cp_conf admin" on page 65*.
`adv_routing <options>`	Enables or disables the Advanced Routing feature on this Security Gateway. **Important** - Do **not** use these outdated commands. To configure Advanced Routing, see the *R81.20 Gaia Advanced Routing Administration Guide*.

Parameter	Description
`auto <options>`	Shows and configures the automatic start of Check Point products during boot. See *"cp_conf auto" on page 68*.
`ca <options>`	■ Configures the Certificate Authority's (CA) Fully Qualified Domain Name (FQDN). ■ Initializes the Internal Certificate Authority (ICA). See *"cp_conf ca" on page 70*.
`client <options>`	Configures the GUI clients that can use SmartConsole to connect to the Security Management Server. See *"cp_conf client" on page 72*.
`corexl <options>`	Enables or disables CoreXL on this Security Gateway / Cluster Member / Security Group. See *"cp_conf corexl" on page 983*.
`finger <options>`	Shows the ICA's Fingerprint. See *"cp_conf finger" on page 76*.
`fullha <options>`	Manages Full High Availability Cluster. See *"cp_conf fullha" on page 986*. **Note** - This command does **not** apply to Scalable Platforms (Maestro and Chassis).
`ha <options>`	Enables or disables cluster membership on this Security Gateway / Cluster Member. See *"cp_conf ha" on page 987*. **Note** - This command does **not** apply to Scalable Platforms (Maestro and Chassis).
`intfs <options>`	Sets the topology of interfaces on a Security Gateway / Cluster Member, which you manage with SmartProvisioning. See *"cp_conf intfs" on page 989*. **Note** - This command does **not** apply to Scalable Platforms (Maestro and Chassis).
`lic <options>`	Manages Check Point licenses. See *"cp_conf lic" on page 78*.
`sic <options>`	Manages SIC on this Security Gateway / Cluster Member / Security Group. See *"cp_conf sic" on page 994*.

Parameter	Description
`snmp <options>`	Do **not** use these outdated commands. To configure SNMP, see the *R81.20 Gaia Administration Guide* - Chapter *System Management* - Section *SNMP*.

cp_conf admin

Description

Configures Check Point system administrators for the Security Management Server.

Notes:

- Multi-Domain Server does not support this command.
- Only one administrator can be defined in the *"cpconfig" on page 134* menu. To define additional administrators, use SmartConsole.
- This command corresponds to the option **Administrator** in the *"cpconfig" on page 134* menu.

Syntax

```
cp_conf admin
      -h
      add [<UserName> <Password> {a | w | r}]
      add -gaia [{a | w | r}]
      del <UserName1> <UserName2> ...
      get
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`add [<UserName> <Password> {a | w | r}]`	Adds a Check Point system administrator: ■ *<UserName>* - Specifies the administrator's username ■ *<Password>* - Specifies the administrator's password ■ `a` - Assigns all permissions - read settings, write settings, and manage administrators ■ `w` - Assigns permissions to read and write settings only (cannot manage administrators) ■ `r` - Assigns permissions to only read settings
`add -gaia [{a | w | r}]`	Adds the Gaia administrator user `admin`: ■ `a` - Assigns all permissions - read settings, write settings, and manage administrators ■ `w` - Assigns permissions to read and write settings only (cannot manage administrators) ■ `r` - Assigns permissions to only read settings
`del <UserName1> <UserName2> ...`	Deletes the specified system administrators.
`get`	Shows the list of the configured system administrators.
`get -gaia`	Shows the management permissions assigned to the Gaia administrator user `admin`.

Example 1 - Adding a Check Point system administrator

```
[Expert@MGMT:0]# cp_conf admin add
Administrator name: admin
Administrator admin already exists.
Do you want to change Administrator's Permissions (y/n) [n] ? y

Permissions for all products (Read/[W]rite All, [R]ead Only All, [C]ustomized) c
        Permission for SmartUpdate (Read/[W]rite, [R]ead Only, [N]one) w
        Permission for Monitoring (Read/[W]rite, [R]ead Only, [N]one) w

Administrator admin was modified successfully and has
Read/Write Permission for SmartUpdate
Read/Write Permission for Monitoring
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin get

The following Administrators
are defined for this Security Management Server:

admin (Read/Write Permission for all products; )
[Expert@MGMT:0]#
```

Example 2 - Adding the Gaia administrator user

```
[Expert@MGMT:0]# cp_conf admin add -gaia
Permissions for all products (Read/[W]rite All, [R]ead Only All, [C]ustomized) c
        Permission for SmartUpdate (Read/[W]rite, [R]ead Only, [N]one) w
        Permission for Monitoring (Read/[W]rite, [R]ead Only, [N]one) w
Administrator admin was added successfully and has
Read/Write Permission for SmartUpdate
Read/Write Permission for Monitoring
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin get -gaia

The following Administrators
are defined for this Security Management Server:

admin (Read/Write Permission for all products; ) - Gaia admin
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin add -gaia a
Administrator admin already exists.

Administrator admin was modified successfully and has
Read/Write Permission for all products with Permission to Manage Administrators
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin add -gaia w
Administrator admin already exists.

Administrator admin was modified successfully and has
Read/Write Permission for all products without Permission to Manage Administrators
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf admin add -gaia r
Administrator admin already exists.

Administrator admin was modified successfully and has
Read Only Permission for all products
[Expert@MGMT:0]#
```

cp_conf auto

Description

Shows and controls which of Check Point products start automatically during boot.

Note - This command corresponds to the option **Automatic start of Check Point Products** in the *"cpconfig" on page 134* menu.

Note - On a Multi-Domain Server, use the option **Automatic Start of Multi-Domain Server** in the *"mdsconfig" on page 762*menu.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cp_conf auto
      -h
      {enable | disable} <Product1> <Product2> ...
      get all
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cp_conf auto
      -h
      {enable | disable} <Product1> <Product2> ...
      get all
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cp_conf auto
      -h
      {enable | disable} <Product1> <Product2> ...
      get all
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cp_conf auto
      -h
      {enable | disable} <Product1> <Product2> ...
      get all
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`{enable | disable} <Product1> <Product2> ...`	Controls whether the installed Check Point products start automatically during boot. This command is for Check Point use only.
`get all`	Shows which of these Check Point products start automatically during boot: ■ Check Point Security Gateway ■ QoS (former FloodGate-1) ■ SmartEvent Suite

Example from a Security Management Server

```
[Expert@MGMT:0]# cp_conf auto get all
Check Point Security Gateway is not installed

QoS is not installed

The SmartEvent Suite will start automatically at boot time.

[Expert@MGMT:0]#
```

Example from a Security Gateway

```
[Expert@GW:0] cp_conf auto get all
The Check Point Security Gateway will start automatically at boot time.

QoS will start automatically at boot time.

SmartEvent Suite is not installed.

[Expert@GW:0]#
```

cp_conf ca

Description

This command changes the settings of the Internal Certificate Authority (ICA).

Note - On a Security Management Server, this command corresponds to the option **Certificate Authority** in the *"cpconfig" on page 134* menu.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cp_conf ca
       -h
       fqdn <FQDN Name>
       init
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`fqdn <FQDN Name>`	Configures the Fully Qualified Domain Name (FQDN) for the Internal Certificate Authority (ICA). The "`<FQDN Name>`" is the text string in this format: *hostname.domainname* **Notes:** ■ The existing certificates for configured objects are **not** revoked. ■ The existing ICA certificate is **not** changed. ■ The Management Server uses the specified "`<FQDN Name>`" to configure the Certificate Revocation List Distribution Point (CRL DP) property in all certificates that the ICA generates. Refer to this command: *"cpca_client get_crldp" on page 109*
`init`	Initializes the Internal Certificate Authority (ICA).

Example

```
[Expert@MyMGMT:0]# hostname
MyMGMT
[Expert@MyMGMT:0]#

[Expert@MyMGMT:0]# domainname
checkpoint.com
[Expert@MyMGMT:0]#

[Expert@MyMGMT:0]# cp_conf ca fqdn MyMGMT.checkpoint.com
Trying to contact Certificate Authority. It might take a while...
Certificate was created successfully
MyMGMT.checkpoint.com was successfully set to the Internal CA
[Expert@MyMGMT:0]#
```

cp_conf client

Description

Configures the GUI clients that are allowed to connect with SmartConsoles to the Security Management Server.

Notes:

- Multi-Domain Server does not support this command.
- This command corresponds to the option **GUI Clients** in the *"cpconfig" on page 134* menu.

Syntax

```
cp_conf client
      add <GUI Client>
      createlist <GUI Client 1> <GUI Client 2> ...
      del <GUI Client 1> <GUI Client 2> ...
      get
```

Parameters

Parameter	Description
`-h`	Shows the built-in usage.
<GUI Client>	*<GUI Client>* can be one of these: ■ One IPv4 address (for example, 192.168.10.20), or one IPv6 address (for example, 3731:54:65fe:2::a7) ■ One hostname (for example, MyComputer) ■ "Any" - To denote all IPv4 and IPv6 addresses without restriction ■ A range of IPv4 addresses (for example, 192.168.10.0/255.255.255.0), or a range of IPv6 addresses (for example, 2001::1/128) ■ IPv4 address wildcard (for example, 192.168.10.*)
`add` *<GUI Client>*	Adds a GUI client.
`createlist` *<GUI Client 1> <GUI Client 2> ...*	Deletes the current allowed GUI clients and creates a new list of allowed GUI clients.
`del` *<GUI Client 1> <GUI Client 2> ...*	Deletes the specified the GUI clients.
`get`	Shows the allowed GUI clients.

Examples

Example 1 - Configure one IPv4 address

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add 172.20.168.15
172.20.168.15 was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
172.20.168.15
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del 172.20.168.15
172.20.168.15 was deleted successfully
[Expert@MGMT:0]#
```

Example 2 - Configure one hostname

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add MySmartConsoleHost
MySmartConsoleHost was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
MySmartConsoleHost
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del MySmartConsoleHost
MySmartConsoleHost was deleted successfully
[Expert@MGMT:0]#
```

Example 3 - Configure "Any"

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add "Any"
Any was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
Any
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del "Any"
Any was deleted successfully
[Expert@MGMT:0]#
```

Example 4 - Configure a range of IPv4 addresses

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add 172.20.168.0/255.255.255.0
172.20.168.0/255.255.255.0 was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
172.20.168.0/255.255.255.0
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del 172.20.168.0/255.255.255.0
172.20.168.0/255.255.255.0 was deleted successfully
[Expert@MGMT:0]#
```

Example 5 - Configure IPv4 address wildcard

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add 172.20.168.*
172.20.168.* was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
172.20.168.*
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client del 172.20.168.*
172.20.168.* was deleted successfully
[Expert@MGMT:0]#
```

Example 6 - Delete the current list and create a new list of allowed GUI clients

```
[Expert@MGMT:0]# cp_conf client get
There are no GUI Clients defined for this Security Management Server
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client add 172.20.168.0/255.255.255.0
172.20.168.0/255.255.255.0 was successfully added.
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
172.20.168.0/255.255.255.0
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client createlist 192.168.40.0/255.255.255.0 172.30.40.55
New list was created successfully
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
192.168.40.0/255.255.255.0
172.30.40.55
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client createlist "Any"
New list was created successfully
[Expert@MGMT:0]#

[Expert@MGMT:0]# cp_conf client get
Any
[Expert@MGMT:0]#
```

cp_conf finger

Description

Shows the Internal Certificate Authority's Fingerprint.

This fingerprint is a text string derived from the ICA certificate on the Security Management Server, Multi-Domain Server, or Domain Management Server.

This fingerprint verifies the identity of the Security Management Server, Multi-Domain Server, or Domain Management Server when you connect to it with SmartConsole.

Note - This command corresponds to the option **Certificate's Fingerprint** in the *"cpconfig" on page 134* menu.

Note - On a Multi-Domain Server:

- To see the fingerprint of the Multi-Domain Server, this command corresponds to the option **Certificate's Fingerprint** in the *"mdsconfig" on page 762* menu.
- You can run this command in these contexts:
  - To see the fingerprint of the Multi-Domain Server, run it in the context of the Multi-Domain Server:

    ```
    mdsenv
    ```

  - To see the fingerprint of a Domain Management Server, run it in the context of the applicable Domain Management Server:

    ```
    mdsenv <IP Address or Name of Domain Management Server>
    ```

Syntax

```
cp_conf finger
      -h
      get
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`get`	Shows the ICA's Fingerprint.

Example

```
[Expert@MGMT:0]# cp_conf finger get
EDNA COCO MOLE ATOM ASH MOT SAGE NINE ILL TINT HI CUBE
[Expert@MGMT:0]#
```

cp_conf lic

Description

Shows, adds and deletes Check Point licenses.

Note - This command corresponds to the option **Licenses and contracts** in the *"cpconfig" on page 134* menu.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cp_conf lic
      -h
      add -f <Full Path to License File>
      add -m <Host> <Date> <Signature Key> <SKU/Features>
      del <Signature Key>
      get [-x]
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cp_conf lic
      -h
      add -f <Full Path to License File>
      add -m <Host> <Date> <Signature Key> <SKU/Features>
      del <Signature Key>
      get [-x]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cp_conf lic
      -h
      add -f <Full Path to License File>
      add -m <Host> <Date> <Signature Key> <SKU/Features>
      del <Signature Key>
      get [-x]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cp_conf lic
      -h
      add -f <Full Path to License File>
      add -m <Host> <Date> <Signature Key> <SKU/Features>
      del <Signature Key>
      get [-x]
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`add -f <Full Path to License File>`	Adds a license from the specified Check Point license file. You get this license file in the *Check Point User Center*. This is the same command as the *"cplic db_add" on page 144*.
`add -m <Host> <Date> <Signature Key> <SKU/Features>`	Adds the license manually. You get these license details in the *Check Point User Center*. This is the same command as the *"cplic db_add" on page 144*.
`del <Signature Key>`	Delete the license based on its signature. This is the same command as the *"cplic del" on page 149*.
`get [-x]`	Shows the local installed licenses. If you specify the "`-x`" parameter, output also shows the signature key for every installed license. This is the same command as the *"cplic print" on page 153*.

Example 1 - Adding the license from the file

```
[Expert@HostName:0]# cp_conf lic add -f ~/License.lic
License was installed successfully.
[Expert@HostName:0]#

[Expert@HostName:0]# cp_conf lic get
Host            Expiration   Signature                                  Features
192.168.3.28    25Aug2019    xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx   CPMP-XXX
[Expert@HostName:0]#
```

Example 2 - Adding the license manually

```
[Expert@MyHostName:0]# cp_conf lic add -m MyHostName 25Aug2019
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx CPMP-XXX
License was successfully installed
[Expert@MyHostName:0]#

[Expert@MyHostName:0]# cp_conf lic get
Host             Expiration   Signature                                 Features
192.168.3.28     25Aug2019    xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx   CPMP-XXX
[Expert@MyHostName:0]#
```

cp_log_export

Description

Exports Check Point logs over syslog.

For more information, see sk122323 and *R81.20 Logging and Monitoring Administration Guide*.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cp_log_export
```

```
cp_log_export <command-name> help
```

Parameters

Parameter	Description
No Parameters	Shows the built-in general help.
`<command-name> help`	Shows the built help for the specified internal command.

Internal Commands

Name	Description
`add`	Configures a new Check Point Log Exporter. `cp_log_export add name <Name> target-server <Target-Server> target-port <Target-Server-Port> protocol {udp | tcp} [Optional Arguments]`
`delete`	Removes an existing Log Exporter. `cp_log_export delete name <Name>`

`reexport`	Resets the current log position and exports all logs again based on the configuration.
	`cp_log_export reexport name <Name> --apply-now`
	`cp_log_export reexport name <Name> start-position <Position of Last Exported Log> --apply-now`
	`cp_log_export reexport name <Name> start-position <Position of Gap Start> end-position <Position of Gap End> --apply-now`

`restart`	Restarts a Log Exporter process. `cp_log_export restart name <Name>`
`set`	Updates an existing Log Exporter configuration. `cp_log_export set name <Name> [<Optional Arguments>]`
`show`	Shows the current Log Exporter configuration. `cp_log_export show [<Optional Arguments>]`
`start`	Starts an existing Log Exporter process. `cp_log_export start name <Name>`
`status`	Shows a Log Exporter overview status. `cp_log_export status [<Optional Arguments>]`
`stop`	Stops an existing Log Exporter process. `cp_log_export stop name <Name>`

Internal Command Arguments

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`--apply-now`	Applies immediately any change that was done with the "`add`", "`set`", "`delete`", or "`reexport`" command.	Optional	Optional	**Mandatory**	N / A	N / A	**Mandatory**
`ca-cert <Path>`	Specifies the full path to the CA certificate file `*.pem`. **Important** - Applicable only when the value of the "`encrypted`" argument is "`true`".	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`client-cert <Path>`	Specifies the full path to the client certificate `*.p12`. **Important** - Applicable only when the value of the "`encrypted`" argument is "`true`".	Optional	Optional	N / A	N / A	N / A	N / A
`client-secret <Phrase>`	Specifies the challenge phrase used to create the client certificate `*.p12`. **Important** - Applicable only when the value of the "`encrypted`" argument is "`true`".	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`domain-server {mds | all}`	On a Multi-Domain Server, specifies the applicable Domain Management Server context. On a Multi-Domain Log Server, specifies the applicable Domain Log Server context. **Important:** ■ "`mds`" (in small letters) - Exports all logs from only the main **MDS** level. ■ "`all`" (in small letters) - Exports all logs from **all** Domains.	**Mandatory**	**Mandatory**	**Mandatory**	N / A	Optional	**Mandatory**

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`enabled {true | false}`	Specifies whether to allow the Log Exporter to start when you run the *"cpstart" on page 208* or *"mdsstart" on page 770* command. Default: `true`	Optional	Optional	N / A	N / A	N / A	N / A
`encrypted {true | false}`	Specifies whether to use TSL (SSL) encryption to send the logs. Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A
`end-position <Position>`	Specifies the end position, up to which to export the logs.	N / A	N / A	N / A	N / A	N / A	Optional
`export-attachment-ids {true | false}`	Specifies whether to add a field to the exported logs that represents the ID of log's attachment (if exists). Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`export-attachment-link {true | false}`	Specifies whether to add a field to the exported logs that represents a link to SmartView that shows the log card and automatically opens the attachment. Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A
`export-link {true | false}`	Specifies whether to add a field to the exported logs that represents a link to SmartView that shows the log card. Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`export-link-ip {true | false}`	Specifies whether to make the links to SmartView use a custom IP address (for example, for a Log Server behind NAT). **Important** - Applicable only when the value of the "`export-link`" argument is "`true`", or the value of the "`export-attachment-link`" argument is "`true`". Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A
`export-log-position {true | false}`	Specifies whether to export the log's position. Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`filter-action-in {"Action1","Action2",... | false}`	Specifies whether to export all logs that contain a specific value in the "**Action**" field. Each value must be surrounded by double quotes (""). Multiple values are supported and must be separated by a comma without spaces. To see all valid values: 1. In SmartConsole, go to the **Logs & Monitor** view and open the **Logs** tab. 2. In the top query field, enter **action:** and a letter. Examples of values:	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	▪ **Accept** ▪ **Block** ▪ **Bypass** ▪ **Detect** ▪ **Drop** ▪ **HTTPS Bypass** ▪ **HTTPS Inspect** ▪ **Prevent** ▪ **Reject** **Important** - This parameter replaces any other filter configuration that was declared earlier on this field directly in the filtering XML file. Other field filters are not overwritten.						

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`filter-blade-in {"Blade1","Blade2",... | false}`	Specifies whether to export all logs that contain a specific value in the "**Blade**" field (the object name of the Software Blade that generated these logs). Each value must be surrounded by double quotes (""). Multiple values are supported and must be separated by a comma without spaces. To see all valid values: 1. In SmartConsole, go to the **Logs & Monitor** view and open the **Logs** tab.	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	2. In the top query field, enter **blade:** and a letter. Examples of values: ■ **Anti-Bot** ■ **Firewall** ■ **HTTPS Inspection** ■ **Identity Awareness** ■ **IPS** Valid Software Blade families: ■ **Access** ■ **TP** ■ **Endpoint** ■ **Mobile**						

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	Important - This parameter replaces any other filter configuration that was declared earlier on this field directly in the filtering XML file. Other field filters are not overwritten.						

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`filter-origin-in {"Origin1","Origin2",... | false}`	Specifies whether to export all logs that contain a specific value in the "**Origin**" field (the object name of the Security Gateway / Cluster Member that generated these logs). Each origin value must be surrounded by double quotes (""). Multiple values are supported and must be separated by a comma without spaces.	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	Important - This parameter replaces any other filter configuration that was declared earlier on this field directly in the filtering XML file. Other field filters are not overwritten.						
`format {generic | cef | json | leef | logrhythm | rsa | splunk | syslog}`	Specifies the format, in which the logs are exported. Default: `syslog`	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`name "<Name>"`	Specifies the unique name of the Log Exporter configuration.	**Mandatory**	**Mandatory**	**Mandatory**	Optional. By default, applies to all.	Optional. By default, applies to all.	**Mandatory**

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	Notes: ■ Allowed characters are: Latin letters, digits ("`0-9`"), minus ("`-`"), underscore ("`_`"), and period ("`.`"). ■ Must start with a letter. ■ The minimum length is two characters. ■ The "`add`" command creates a new target directory with the specified unique name in the `$EXPORTERDIR/targets/` directory.						

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`protocol {tcp | udp}`	Specifies the Layer 4 Transport protocol to use (TCP or UDP). There is no default value.	**Mandatory**	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`read-mode {raw | semi-unified}`	Specifies the mode, in which to read the log files. ■ `raw` - Specifies to export log records without any unification. ■ `semi-unified` - Specifies to export log records with step-by-step unification. That is, for each log record, export a record that unifies this record with all previously-encountered records with the same ID.	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	Default: `semi-unified` Default: `raw`						
`reconnect-interval {<Number> | default}`	Specifies the interval (in minutes) after which the Log Exporter must connect again to the target server after the connection is lost. To disable, enter the value "`default`". There is no default value.	Optional	Optional	N / A	N / A	N / A	N / A
`start-position <Position>`	Specifies the start position, from which to export the logs.	N / A	N / A	N / A	N / A	N / A	Optional
`target-port <Target-Server-Port>`	Specifies the listening port on the target server, to which you export the logs.	**Mandatory**	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`target-server <Target-Server>`	Specifies the IP address or FQDN of the target server, to which you export the logs.	**Mandatory**	Optional	N / A	N / A	N / A	N / A
`time-in-milli {true | false}`	Specifies whether to export logs with the time resolution in milliseconds. Requires Security Gateways R81 and higher. Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A

cpca_client

Description

Execute operations on the Internal Certificate Authority (ICA).

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d]
      create_cert <options>
      double_sign <options>
      get_crldp <options>
      get_pubkey <options>
      init_certs <options>
      lscert <options>
      revoke_cert <options>
      revoke_non_exist_cert <options>
      search <options>
      set_ca_services <options>
      set_cert_validity <options>
      set_mgmt_tool <options>
      set_sign_hash <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`create_cert <options>`	Issues a SIC certificate for the Security Management Server or Domain Management Server. See *"cpca_client create_cert" on page 105*.

Parameter	Description
`double_sign <options>`	Creates a second signature for a certificate. See *"cpca_client double_sign" on page 107*.
`get_crldp <options>`	Shows how to access a CRL file from a CRL Distribution Point. See *"cpca_client get_crldp" on page 109*.
`get_pubkey <options>`	Saves the encoding of the public key of the ICA's certificate to a file. See *"cpca_client get_pubkey" on page 111*.
`init_certs <options>`	Imports a list of DNs for users and creates a file with registration keys for each user. See *"cpca_client init_certs" on page 112*.
`lscert <options>`	Shows all certificates issued by the ICA. See *"cpca_client lscert" on page 113*.
`revoke_cert <options>`	Revokes a certificate issued by the ICA. See *"cpca_client revoke_cert" on page 116*.
`revoke_non_exist_ cert <options>`	Revokes a non-existent certificate issued by the ICA. See *"cpca_client revoke_non_exist_cert" on page 119*.
`search <options>`	Searches for certificates in the ICA. See *"cpca_client search" on page 120*.
`set_ca_services <options>`	Controls the Certificate Authority Services Portal. See *"cpca_client set_ca_services" on page 123*.
`set_cert_validity <options>`	Configures the default certificate validity period for new certificates. See *"cpca_client set_cert_validity" on page 125*.
`set_mgmt_tool <options>`	Controls the ICA Management Tool. See *"cpca_client set_mgmt_tool" on page 126*.
`set_sign_hash <options>`	Sets the hash algorithm that the CA uses to sign the file hash. See *"cpca_client set_sign_hash" on page 131*.

cpca_client create_cert

Description

Issues a SIC certificate for the Security Management Server or Domain Management Server.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] create_cert [-p <CA port number>] -n "CN=<Common
Name>" -f <Full Path to PKCS12 file> [-w <Password>] [-k {SIC |
USER | IKE | ADMIN_PKG}] [-c "<Comment for Certificate>"]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <CA port number>`	Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18209.
`-n "CN=<Common Name>"`	Sets the CN to the specified `<Common Name>`.
`-f <Full Path to PKCS12 file>`	Specifies the PKCS12 file, which stores the certificate and keys.
`-w <Password>`	Optional. Specifies the certificate password.
`-k {SIC | USER | IKE | ADMIN_PKG}`	Optional. Specifies the certificate kind.
`-c "<Comment for Certificate>"`	Optional. Specifies the certificate comment (must enclose in double quotes).

Example

```
[Expert@MGMT:0]# cpca_client create_cert -n "cn=cp_mgmt" -f $CPDIR/conf/sic_cert.p12
```

cpca_client double_sign

Description

Creates a second signature for a certificate.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] double_sign [-p <CA port number>] -i <Certificate File in PEM format> [-o <Full Path to Output File>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <CA port number>`	Optional. Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18209.
`-i <Certificate File in PEM format>`	Imports the specified certificate (only in PEM format).
`-o <Full Path to Output File>`	Optional. Saves the certificate into the specified file.

Example

```
[Expert@MGMT:0]# cpca_client double_sign -i certificate.pem

 Requesting Double Signature for the following Certificate:
        refCount: 1
        Subject: Email=example@example.com,CN=http://www.example.com/,OU=ValiCert Class 2 Policy
Validation Authority,O=exampleO\, Inc.,L=ExampleL Validation Network

 Double Sign of Cert:
 ====================
 (
        : (
                :dn ("Email=example@example.com,CN=http://www.example.com/,OU=exampleOU Class 2
Policy Validation Authority,O=exampleO\, Inc.,L=exampleL Validation Network")
                :doubleSignCert (52016390... ... ...ebb67e96)
                :return_code (0)
        )
)

[Expert@MGMT:0]#
```

cpca_client get_crldp

Description

Shows the Fully Qualified Domain Name (FQDN) configured for the Internal Certificate Authority (ICA) with the "*"cp_conf ca" on page 70*" command.

The Management Server uses this FQDN:

1. To configure the Certificate Revocation List Distribution Point (CRL DP) property in all certificates that the ICA generates.
2. To create the URL for accessing the CRL.

   Example: `http://MyMGMT.checkpoint.com:18264/ICA_CRL1.crl`

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] get_crldp [-p <ICA port number>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <ICA port number>`	Optional. Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18264.

Example

```
[Expert@MyMGMT:0]# hostname
MyMGMT
[Expert@MyMGMT:0]#

[Expert@MyMGMT:0]# domainname
checkpoint.com
[Expert@MyMGMT:0]#

[Expert@MyMGMT:0]# cpca_client get_crldp
MyMGMT.checkpoint.com
[Expert@MyMGMT:0]
```

cpca_client get_pubkey

Description

Saves the encoding of the public key of the ICA's certificate to a file.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] get_pubkey [-p <CA port number>] <Full Path to Output File>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <CA port number>`	Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18209.
<Full Path to Output File>	Saves the encoding of the public key of the ICA's certificate to the specified file.

Example

```
[Expert@MGMT:0]# cpca_client get_pubkey /tmp/key.txt[Expert@MGMT:0]#
[Expert@MGMT:0]# cat /tmp/key.txt
3082010a... ... ...f98b8910
[Expert@MGMT:0]#
```

cpca_client init_certs

Description

Imports a list of Distinguished Names (DN) for users and creates a file with registration keys for each user.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] init_certs [-p <CA port number>] -i <Full Path to Input File> -o <Full Path to Output File>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <CA port number>`	Optional. Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18209.

`-i <Full Path to Input File>`	Imports the specified file.
	Make sure to use the full path.
	Make sure that there is an empty line between each DN in the specified file.
	Example:
	`...CN=test1,OU=users...`
	`<Empty Line>`
	`...CN=test2,OU=users...`

`-o <Full Path to Output File>`	Saves the registration keys to the specified file. This command saves the error messages in the `<Name of Output File>.failures` file in the same directory.

cpca_client lscert

Description

Shows all certificates issued by the ICA.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] lscert [-dn <SubString>] [-stat {Pending | Valid
| Revoked | Expired | Renewed}] [-kind {SIC | IKE | User | LDAP}]
[-ser <Certificate Serial Number>] [-dp <Certificate Distribution
Point>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-dn <SubString>`	Optional. Filters the search results to those with a DN that matches the specified `<SubString>`. This command does not support multiple values.
`-stat {Pending | Valid | Revoked | Expired | Renewed}`	Optional. Filters the search results to those with certificate status that matches the specified status. This command does not support multiple values.
`-kind {SIC | IKE | User | LDAP}`	Optional. Filters the search results to those with certificate kind that matches the specified kind. This command does not support multiple values.
`-ser <Certificate Serial Number>`	Optional. Filters the search results to those with certificate serial number that matches the specified serial number. This command does not support multiple values.
`-dp <Certificate Distribution Point>`	Optional. Filters the search results to the specified Certificate Distribution Point (CDP). This command does not support multiple values.

Example

```
[Expert@MGMT:0]# cpca_client lscert -stat Revoked
Operation succeeded. rc=0.
5 certs found.

Subject = CN=VSX2,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Revoked   Kind = SIC   Serial = 5521   DP = 0
Not_Before: Sun Apr  8 14:10:01 2018   Not_After: Sat Apr  8 14:10:01 2023

Subject = CN=VSX1,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Revoked   Kind = SIC   Serial = 9113   DP = 0
Not_Before: Sun Apr  8 14:09:02 2018   Not_After: Sat Apr  8 14:09:02 2023

Subject = CN=VSX1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Revoked   Kind = IKE   Serial = 82434   DP = 2
Not_Before: Mon May 14 19:15:05 2018   Not_After: Sun May 14 19:15:05 2023
[Expert@MGMT:0]#


[Expert@MGMT:0]# cpca_client lscert -kind IKE
Operation succeeded. rc=0.
3 certs found.

Subject = CN=VS1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Valid   Kind = IKE   Serial = 27214   DP = 1
Not_Before: Wed Apr 11 17:26:02 2018   Not_After: Tue Apr 11 17:26:02 2023

Subject = CN=VSX_Cluster VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Valid   Kind = IKE   Serial = 64655   DP = 1
Not_Before: Mon Apr  9 19:36:31 2018   Not_After: Sun Apr  9 19:36:31 2023

Subject = CN=VSX1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Revoked   Kind = IKE   Serial = 82434   DP = 2
Not_Before: Mon May 14 19:15:05 2018   Not_After: Sun May 14 19:15:05 2023
[Expert@MGMT:0]#
```

cpca_client revoke_cert

Description

Revokes a certificate issued by the ICA.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] revoke_cert [-p <CA port number>] -n "CN=<Common Name>" -s <Certificate Serial Number>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <CA port number>`	Optional. Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18209.

`-n "CN=<Common Name>"`	Specifies the certificate CN.
	To get the CN, run the *"cpca_client lscert" on page 113* command and examine the text that you see between the "`Subject =`" and the "`,O=...`".
	Example
	From this output:
	`Subject = CN=VS1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x`
	`Status = Valid Kind = IKE Serial = 27214 DP = 1`
	`Not_Before: Wed Apr 11 17:26:02 2018 Not_After: Tue Apr 11 17:26:02 2023`
	you get this syntax:
	`-n "CN=VS1 VPN Certificate`
	Note - You can use the parameter '`-n`' only, or together with the parameter "`-s`".

`-s <Certificate Serial Number>`	Specifies the certificate serial number. To see the serial number, run the *"cpca_client lscert" on page 113* command. **Note** - You can use the parameter "`-s`" only, or together with the parameter "`-n`".

Example 1 - Revoking a certificate specified by its CN

```
[Expert@MGMT:0]# cpca_client lscert
Subject = CN=VS1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Valid Kind = IKE Serial = 27214 DP = 1
Not_Before: Wed Apr 11 17:26:02 2018 Not_After: Tue Apr 11 17:26:02 2023
[Expert@MGMT:0]#
[Expert@MGMT:0]# cpca_client -d revoke_cert -n "CN=VS1 VPN Certificate"
 Certificate was revoked successfully
[Expert@MGMT:0]#
```

Example 2 - Revoking a certificate specified by its serial number.

```
[Expert@MGMT:0]# cpca_client lscert
Subject = CN=VS1 VPN Certificate,O=MyDomain_Server.checkpoint.com.s6t98x
Status = Valid Kind = IKE Serial = 27214 DP = 1
Not_Before: Wed Apr 11 17:26:02 2018 Not_After: Tue Apr 11 17:26:02 2023
[Expert@MGMT:0]#
[Expert@MGMT:0]# cpca_client -d revoke_cert -s 27214
 Certificate was revoked successfully
[Expert@MGMT:0]#
```

cpca_client revoke_non_exist_cert

Description

Revokes a non-existent certificate issued by the ICA.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] revoke_non_exist_cert -i <Full Path to Input File>
```

Parameters

Parameter	Description
`-d`	Runs the `cpca_client` command under debug.

`-i <Full Path to Input File>`	Specifies the file that contains the list of the certificate to revoke.
	You must create this file in the same format as the *"cpca_client lscert" on page 113* command prints its output.
	Example
	`Subject = CN=cp_mgmt,O=MGMT.5p72vp`
	`Status = Valid  Kind = SIC  Serial = 30287  DP = 0`
	`Not_Before: Sat Apr  7 19:40:12 2018  Not_After: Fri Apr  7 19:40:12 2023`
	`<Empty Line>`
	`Subject = CN=cp_mgmt,O=MGMT.5p72vp`
	`Status = Valid  Kind = SIC  Serial = 60870  DP = 0`
	`Not_Before: Sat Apr  7 19:40:13 2018  Not_After: Fri Apr  7 19:40:13 2023`

Note - This command saves the error messages in the `<Name of Input File>.failures` file.

cpca_client search

Description

Searches for certificates in the ICA.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] search <String> [-where {dn | comment | serial |
device_type | device_id | device_name}] [-kind {SIC | IKE | User |
LDAP}] [-stat {Pending | Valid | Revoked | Expired | Renewed}] [-
max <Maximal Number of Results>] [-showfp {y | n}]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
<String>	Specifies the text to search in the certificates. You can enter only one text string that does not contain spaces.

Parameter	Description
`-where {dn | comment | serial | device_type | device_id | device_name}`	Optional. Specifies the certificate's field, in which to search for the string: ■ `dn` - Certificate DN ■ `comment` - Certificate comment ■ `serial` - Certificate serial number ■ `device_type` - Device type ■ `device_id` - Device ID ■ `device_name` - Device Name The default is to search in all fields.
`-kind {SIC | IKE | User | LDAP}`	Optional. Specifies the certificate kind to search. You can enter multiple values in this format: `-kind <Kind1> <Kind2> <Kind3>` The default is to search for all kinds.
`-stat {Pending | Valid | Revoked | Expired | Renewed}`	Optional. Specifies the certificate status to search. You can enter multiple values in this format: `-stat <Status1> <Status2> <Status3>` The default is to search for all statuses.
`-max <Maximal Number of Results>`	Optional. Specifies the maximal number of results to show. ■ Range: 1 and greater ■ Default: 200
`-showfp {y | n}`	Optional. Specifies whether to show the certificate's fingerprint and thumbprint: ■ `y` - Shows the fingerprint and thumbprint (this is the default) ■ `n` - Does not show the fingerprint and thumbprint

Example 1

```
[Expert@MGMT:0]# cpca_client search samplecompany -where comment -kind SIC LDAP -stat Pending
Valid Renewed
```

Example 2

```
[Expert@MGMT:0]# cpca_client search 192.168.3.51 -where dnOperation succeeded. rc=0.
1 certs found.

Subject = CN=192.168.3.51,O=MGMT.5p72vp
Status = Valid Kind = SIC Serial = 73455 DP = 0
Not_Before: Sat Apr 7 19:40:12 2018 Not_After: Fri Apr 7 19:40:12 2023
Fingerprint = XXX XXX XXX XXX XXX XXX XXX XXX XXX XXX XXX XXX
Thumbprint = xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
[Expert@MGMT:0]#
```

Example 3

```
[Expert@MGMT:0]# cpca_client search 192.168.3.51 -where dn -showfp nOperation succeeded. rc=0.
1 certs found.

Subject = CN=192.168.3.51,O=MGMT.5p72vp
Status = Valid Kind = SIC Serial = 73455 DP = 0
Not_Before: Sat Apr 7 19:40:12 2018 Not_After: Fri Apr 7 19:40:12 2023
[Expert@MGMT:0]#
```

cpca_client set_ca_services

Description

This command enables and disables the Certificate Authority Services Portal on the Management Server on the TCP port 18268.

From this portal, you can download the applicable Internal Certificate Authority certificates.

For trust purposes, you can install this certificate on the applicable Security Gateways, externally managed Site to Site VPN peer gateways, Remote Access VPN clients, clients that use Clientless VPN, and so on.

Note - In R81.20, the TCP port 18264 on the Management Server is available only for the retrieval of the CRL (Certificate Revocation List).

Syntax

```
cpca_client set_ca_services {on | off}
```

Parameters

Parameter	Description
`on`	Enables the Certificate Authority Services Portal
`off`	Disables the Certificate Authority Services Portal

Procedure for a Security Management Server

Enabling the Certificate Authority Services Portal

1. Connect to the command line on the Security Management Server.
2. Log in to the Expert mode.
3. Enable the Certificate Authority Services Portal:

   ```
   cpca_client set_ca_services on
   ```

4. With a web browser, connect to:

   ```
   http://<IP Address of Security Management Server>:18268
   ```

5. Download the required certificate.
6. Install this certificate on the applicable computers.

Disabling the Certificate Authority Services Portal

1. Connect to the command line on the Security Management Server.
2. Log in to the Expert mode.
3. Disable the Certificate Authority Services Portal:

```
cpca_client set_ca_services off
```

Procedure for a Domain Management Server

Enabling the Certificate Authority Services Portal

1. Connect to the command line on the Multi-Domain Server.
2. Log in to the Expert mode.
3. Go to the context of the Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

4. Enable the Certificate Authority Services Portal:

```
cpca_client set_ca_services on
```

5. With a web browser, connect to:

```
http://<IP Address of Domain Management Server>:18268
```

6. Download the required certificate.
7. Install this certificate on the applicable computers.

Disabling the Certificate Authority Services Portal

1. Connect to the command line on the Multi-Domain Server.
2. Log in to the Expert mode.
3. Go to the context of the Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

4. Disable the Certificate Authority Services Portal:

```
cpca_client set_ca_services off
```

cpca_client set_cert_validity

Description

This command configures the default certificate validity period for new certificates.

Notes:

- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- The new certificate validity period applies only to certificate you create after this change.

Syntax

```
cpca_client set_cert_validity -k {SIC | IKE | USER} [-y <Number of Years>] [-d <Number of Days>] [-h <Number of Hours>] [-s <Number of Seconds>]
```

Parameters

Parameter	Description
`-k {SIC | IKE | USER}`	Specifies the certificate type.
`-y <Number of Years>`	Specifies the validity period in years.
`-d <Number of Days>`	Specifies the validity period in days.
`-h <Number of Hours>`	Specifies the validity period in hours.
`-s <Number of Seconds>`	Specifies the validity period in seconds.

Example

```
[Expert@MGMT:0]# cpca_client set_cert_validity -k IKE -y 3
 cert validity period was changed successfully.
[Expert@MGMT:0]#
```

cpca_client set_mgmt_tool

Description

Controls the ICA Management Tool.

This tool is disabled by default.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

See sk102837: Best Practices - ICA Management Tool configuration

Syntax

```
cpca_client [-d] set_mgmt_tool {on | off | add | remove | clean |
print} [-p <CA port number>] [{-a <Administrator DN> | -u <User
DN> | -c <Custom User DN>}]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`on`	Starts the ICA Management Tool.
`off`	Stops the ICA Management Tool.
`add`	Adds the specified administrator, user, or custom user that is permitted to use the ICA Management Tool.
`remove`	Removes the specified administrator, user, or custom user that is permitted to use the ICA Management Tool.
`clean`	Removes all administrators, users, or custom users that are permitted to use the ICA Management Tool.
`print`	Shows the configured administrators, users, or custom users that are permitted to use the ICA Management Tool.

Parameter	Description
`-p <CA port number>`	Optional. Specifies the TCP port on the Security Management Server or Domain Management Server, which is used to connect to the Certificate Authority. The default TCP port number is 18265.
`-a <Administrator DN>`	Optional. Specifies the DN of the administrator that is permitted to use the ICA Management Tool. Must specify the full DN as appears in SmartConsole **Procedure** 1. Open **Object Explorer** > **Users** 2. Open the Administrator object or a User object properties 3. Click the **Certificates** pane 4. Select the certificate and click the pencil icon 5. Click **View certificate details** 6. In the **Certificate Info** window, click the **Details** tab 7. Click the **Subject** field 8. Concatenate all fields Example: `-a "CN=ICA_Tool_Admin,OU=users,O=MGMT.s6t98x"`
`-u <User DN>`	Optional. Specifies the DN of the user that is permitted to use the ICA Management Tool. Must specify the full DN as appears in SmartConsole: **Procedure** 1. Open **Object Explorer** > **Users** 2. Open the Administrator object or a User object properties 3. Click the **Certificates** pane 4. Select the certificate and click the pencil icon 5. Click **View certificate details** 6. In the **Certificate Info** window, click the **Details** tab 7. Click the **Subject** field 8. Concatenate all fields Example: `-u "CN=ICA_Tool_User,OU=users,O=MGMT.s6t98x"`

Parameter	Description
`-c <Custom User DN>`	Optional. Specifies the DN for the custom user that is permitted to use the ICA Management Tool. Must specify the full DN as appears in SmartConsole. **Procedure** 1. Open **Object Explorer** > **Users** 2. Open the Administrator object or a User object properties 3. Click the **Certificates** pane 4. Select the certificate and click the pencil icon 5. Click **View certificate details** 6. In the **Certificate Info** window, click the **Details** tab 7. Click the **Subject** field 8. Concatenate all fields Example: `-c "CN=ICA_Tool_User,OU=users,O=MGMT.s6t98x"`

Note - If you run the "`cpca_client set_mgmt_tool`" command without the parameter "`-a`" or "`-u`", the list of the permitted administrators and users is not changed. The previously defined permitted administrators and users can start and stop the ICA Management Tool.

To connect to the ICA Management Tool

1. In SmartConsole, configure the required administrator and user objects.

   You must create a certificate for these administrators and users.

   You use this certificate to configure the permitted users in the ICA Management Tool and in the client web browsers.

2. In the command line on the Management Server, add the required administrators and users that are permitted to use the ICA Management Tool.

   ```
   cpca_client set_mgmt_tool add ...
   ```

3. In the command line on the Management Server, start the ICA Management Tool.

   ```
   cpca_client set_mgmt_tool on
   ```

4. Check the status of the ICA Management Tool:

   ```
   cpca_client set_mgmt_tool print
   ```

5. Import the administrator's / user's certificate into the Windows Certificate Store:.

   a. Right-click the *.p12 file you saved when you created the required administrator / user, and click **Install PFX**.

      The **Certificate Import Wizard** opens.

   b. In the **Store Location** section, select the applicable option:

      - **Current User** (this is the default)
      - **Local Machine**

   c. Click **Next**.

   d. Enter the same certificate password you used when you created the required administrator / user certificate.

   e. Clear **Enable strong private key protection**.

   f. Select **Mark this key as exportable**.

   g. Click **Next**.

   h. Select **Place all certificates in the following store** > click **Browse** > select **Personal** > click **OK**.

   i. Click **Next**.

   j. Click **Finish**.

6. In a web browser, connect to the ICA Management Tool:

   ```
   https://<IP Address of the Management Server>:18265
   ```

   Important - The fact that the TCP port 18265 is open is not a vulnerability. The ICA Management Tool Portal is secured and protected by SSL. In addition, only authorized administrators and users are allowed to access it using a certificate.

7. A dialog box with this message appears:

   ```
   Client Authentication

   Identification

   The Web site you want to view requests identification.

   Select the certificate to use when connecting.
   ```

8. Select the appropriate certificate for authenticating to the ICA Management Tool.
9. Click **OK**.
10. In the **Security Alert** dialog box, click **Yes**.

cpca_client set_sign_hash

Description

Sets the hash algorithm that the CA uses to sign the file hash. Also, see sk103840.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_client [-d] set_sign_hash {sha1 | sha256 | sha384 | sha512}
```

Important - After this change, you must restart the Check Point services with these commands:

- On Security Management Server, run:
  1. `cpstop`
  2. `cpstart`
- On a Multi-Domain Server, run:
  1. `mdsstop_customer <Name or IP Address of Domain Management Server>`
  2. `mdsstart_customer <Name or IP Address of Domain Management Server>`

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{sha1 | sha256 | sha384 | sha512}`	The hash algorithms that the CA uses to sign the file hash. The default algorithm is SHA-256.

Example

```
[Expert@MGMT:0]# cpca_client set_sign_hash sha256

You have selected the signature hash function SHA-256
WARNING: This hash algorithm is not supported in Check Point gateways prior to R71.
WARNING: It is also not supported on older clients and SG80 R71.

Are you sure? (y/n)
y
Internal CA signature hash changed successfully.
Note that the signature on the Internal CA certificate has not changed, but this has no security
implications.
[Expert@MGMT:0]#
[Expert@MGMT:0]# cpstop ; cpstart
```

cpca_create

Description

Creates new Check Point Internal Certificate Authority database.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cpca_create [-d] -dn <CA DN>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-dn <CA DN>`	Specifies the Certificate Authority Distinguished Name (DN).

cplic

Description

The `cplic` command manages Check Point licenses.

You can run this command in Gaia Clish or in the Expert mode.

License Management is divided into three types of commands:

Licensing Commands	Applies To	Description
Local licensing commands	Management Servers, Security Gateways and Cluster Members	You execute these commands locally on the Check Point servers.
Remote licensing commands	Management Servers only	You execute these commands on the Security Management Server or Domain Management Server. These changes affect the managed Security Gateways and Cluster Members.
License Repository commands	Management Servers only	You execute these commands on the Security Management Server or Domain Management Server. These changes affect the licenses stored in the local license repository.

For more about managing licenses, see the *R81.20 Security Management Administration Guide*.

Syntax for Local Licensing on a Management Server itself

```
cplic [-d]
      {-h | -help}
      check <options>
      contract <options>
      del <options>
      print <options>
      put <options>
```

Syntax for Remote Licensing on managed Security Gateways and Cluster Members

```
cplic [-d]
      {-h | -help}
      del <options>
      get <options>
      put <options>
      upgrade <options>
```

Syntax for License Database Operations on a Management Server

```
cplic [-d]
      {-h | -help}
      db_add <options>
      db_print <options>
      db_rm <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{-h | -help}`	Shows the applicable built-in usage.
`check <options>`	Confirms that the license includes the feature on the local Security Gateway or Management Server. See *"cplic check" on page 140*.
`contract <options>`	Manages (deletes and installs) the Check Point Service Contract on the local Check Point server. See *"cplic contract" on page 142*.
`db_add <options>`	Applies only to a Management Server. Adds licenses to the license repository on the Management Server. See *"cplic db_add" on page 144*.

Parameter	Description
`db_print <options>`	Applies only to a Management Server. Shows the details of Check Point licenses stored in the license repository on the Management Server. See *"cplic db_print" on page 146*.
`db_rm <options>`	Applies only to a Management Server. Removes a license from the license repository on the Management Server. See *"cplic db_rm" on page 148*.
`del <options>`	Deletes a Check Point license on a host, including unwanted evaluation, expired, and other licenses. See *"cplic del" on page 149*.
`del <Object Name> <options>`	Detaches a Central license from a remote managed Security Gateway or Cluster Member. See *"cplic del <object name>" on page 150*.
`get <options>`	Applies only to a Management Server. Retrieves all licenses from managed Security Gateways and Cluster Members into the license repository on the Management Server. See *"cplic get" on page 151*.
`print <options>`	Prints details of the installed Check Point licenses on the local Check Point server. See *"cplic print" on page 153*.
`put <options>`	Installs and attaches licenses on a Check Point server. See *"cplic put" on page 155*.
`put <Object Name> <options>`	Attaches one or more Central or Local licenses to a remote managed Security Gateways and Cluster Members. See *"cplic put <object name>" on page 158*.
`upgrade <options>`	Applies only to a Management Server. Upgrades licenses in the license repository with licenses in the specified license file. See *"cplic upgrade" on page 161*.

cplic check

Description

Confirms that the license includes the feature on the local Security Gateway or Management Server. See sk66245.

Syntax

```
cplic check {-h | -help}
```

```
cplic [-d] check [-p <Product>] [-v <Version>] [{-c | -count}] [-t <Date>] [{-r | -routers}] [{-S | -SRusers}] <Feature>
```

You can run this command:

- On a Management Server / Security Gateway / Cluster Member in Gaia Clish or the Expert mode
- On a Scalable Platform Security Group in Gaia gClish or the Expert mode

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <Product>`	Product, for which license information is requested. Some examples of products: ■ `fw1` - FireWall-1 infrastructure on Security Gateway / Cluster Member / Security Group (all Software Blades), or Management Server (all Software Blades) ■ `mgmt` - Multi-Domain Server infrastructure ■ `services` - Entitlement for various services ■ `cvpn` - Mobile Access ■ `etm` - QoS (FloodGate-1) ■ `eps` - Endpoint Software Blades on Management Server
`-v <Version>`	Product version, for which license information is requested.

Parameter	Description
`{-c | -count}`	Outputs the number of licenses connected to this feature.
`-t <Date>`	Checks license status on future date. Use the format **ddmmyyyy**. A feature can be valid on a given date on one license, but invalid on another.
`{-r | -routers}`	Checks how many routers are allowed. The *<Feature>* option is not needed.
`{-S | -SRusers}`	Checks how many SecuRemote users are allowed.
<Feature>	Feature, for which license information is requested.

Example from a Management Server

```
[Expert@MGMT]# cplic print -p
Host Expiration Primitive-Features
W.X.Y.Z 24Mar2016 ::CK-XXXXXXXXXXX fw1:6.0:swb fw1:6.0:comp fw1:6.0:compunlimited fw1:6.0:cluster-1 fw1:6.0:cpxmgmt_qos_u_sites
fw1:6.0:sprounl fw1:6.0:nxunlimit fw1:6.0:swp evnt:6.0:smrt_evnt fw1:6.0:fwc fw1:6.0:ca fw1:6.0:rtmui fw1:6.0:sstui fw1:6.0:fwlv
fw1:6.0:cmd evnt:6.0:alzd5 evnt:6.0:alzc1 evnt:6.0:alzs1 fw1:6.0:sstui fw1:6.0:fwlv fw1:6.0:sme10 etm:6.0:rtm_u fw1:6.0:cep1 fw1:6.0:rt
fw1:6.0:cemid fw1:6.0:web_sec_u fw1:6.0:workflow fw1:6.0:ram1 fw1:6.0:routers fw1:6.0:supmgmt fw1:6.0:supunlimit fw1:6.0:prov
fw1:6.0:atlas-unlimit fw1:6.0:filter fw1:6.0:ui psmp:6.0:psmsunlimited fw1:6.0:vpe_unlimit fw1:6.0:cluster-u fw1:6.0:remote1 fw1:6.0:aes
fw1:6.0:strong fw1:6.0:rdp fw1:6.0:des fw1:6.0:isakmp fw1:6.0:dbvr_unlimit fw1:6.0:cmpmgmt fw1:6.0:rtmmgmt fw1:6.0:fgmgmt fw1:6.0:blades
fw1:6.0:cpipv6 fw1:6.0:mgmtha fw1:6.0:remote
[Expert@MGMT]#
```

Example from a Management Server in High Availability

```
[Expert@MGMT]# cplic check -p fw1 -v 6.0 -c mgmtha
cplic check 'mgmtha': 1 licenses
[Expert@MGMT]#
```

Example from a Security Gateway

```
[Expert@GW]# cplic print -p
Host Expiration Primitive-Features
W.X.Y.Z 23Mar2016 ::CK-XXXXXXXXXXX fw1:6.0:swb fw1:6.0:abot fw1:6.0:ips fw1:6.0:appi fw1:6.0:aspm fw1:6.0:av1000 fw1:6.0:urlf fw1:6.0:av
fw1:6.0:vsx5 fw1:6.0:cpls fw1:6.0:cluster-u fw1:6.0:mpu fw1:6.0:sxl_vpn fw1:6.0:sxl_fw fw1:6.0:sxl_ppk fw1:6.0:connect fw1:6.0:pam
etm:6.0:fgcountunl etm:6.0:fg etm:6.0:tclog etm:6.0:fgvpn fw1:6.0:identity cvpn:6.0:ccvunl cvpn:6.0:cvpnunlimited fw1:6.0:des
fw1:6.0:strong fw1:6.0:encryption cvpn:6.0:cvpn fw1:6.0:dlp evnt:6.0:smrt_evnt fw1:6.0:ipsa fw1:6.0:spcps fw1:6.0:pam
fw1:6.0:enchostsunlimit fw1:6.0:aes fw1:6.0:rdp fw1:6.0:isakmp fw1:6.0:xlate fw1:6.0:auth fw1:6.0:content fw1:6.0:sync fw1:6.0:fm
fw1:6.0:blades fw1:6.0:sr5000 fw1:6.0:hostsunlimit fw1:6.0:mc_all_8 fw1:6.0:multicore
[Expert@GW]#
```

Example from a Cluster Member

```
[Expert@GW]# cplic check cluster-u
cplic check 'cluster-u': license valid
[Expert@GW]#
[Expert@GW]# cplic check -c cluster-u
cplic check 'cluster-u': 9 licenses
[Expert@GW]#
```

cplic contract

Description

Deletes the Check Point Service Contract on the local Check Point server.

Installs the Check Point Service Contract on the local Check Point server.

Note

- For more information about Service Contract files, see sk33089: What is a Service Contract File?
- If you install a Service Contract on a managed Security Gateway / Cluster Member / Scalable Platform Security Group, you must update the license repository on the applicable Management Server - either with the *"cplic get" on page 151* command, or in SmartUpdate.

Syntax

```
cplic contract -h
```

```
cplic [-d] contract
      del
            -h
            <Service Contract ID>
      put
            -h
            [{-o | -overwrite}] <Service Contract File>
```

You can run this command:

- On a Management Server / Security Gateway / Cluster Member in Gaia Clish or the Expert mode
- On a Scalable Platform Security Group in Gaia gClish or the Expert mode

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`del`	Deletes the Service Contract from the `$CPDIR/conf/cp.contract` file on the local Check Point server.
`put`	Merges the Service Contract to the `$CPDIR/conf/cp.contract` file on the local Check Point server.
<Service Contract ID>	ID of the Service Contract.
`{-o | -overwrite}`	Specifies to overwrite the current Service Contract.
<Service Contract File>	Path to and the name of the Service Contract file. First, you must download the Service Contract file from your *Check Point User Center* account.

cplic db_add

Description

Adds licenses to the license repository on the Management Server.

When you add Local licenses to the license repository, Management Server automatically attaches them to the managed Security Gateway / Cluster Member with the matching IP address.

When you add Central licenses, you must manually attach them.

Note - You get the license details in the *Check Point User Center*.

Syntax

```
cplic db_add {-h | -help}
```

```
cplic [-d] db_add -l <License File> [<Host>] [<Expiration Date>]
[<Signature>] [<SKU/Features>]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-l <License File>`	Name of the file that contains the license.
<Host>	Hostname or IP address of the Security Management Server / Domain Management Server.
<Expiration Date>	The license expiration date.
<Signature>	The license signature string. For example: `aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m` Case sensitive. Hyphens are optional.

Parameter	Description
<SKU/Features>	The SKU of the license summarizes the features included in the license. For example, `CPSUITE-EVAL-3DES-vNG`

Example

If the file `192.0.2.11.lic` contains one or more licenses, the command "`cplic db_add -l 192.0.2.11.lic`" produces output similar to:

```
[Expert@MGMT]# cplic db_add -l 192.0.2.11.lic
Adding license to database ...
Operation Done
[Expert@MGMT]#
```

cplic db_print

Description

Shows the details of Check Point licenses stored in the license repository on the Management Server.

Syntax

```
cplic db_print {-h | -help}
```

```
cplic [-d] db_print {<Object Name> | -all} [{-n | -noheader}] [-x]
[{-t | -type}] [{-a | -attached}]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
<Object Name>	Prints only the licenses attached to *<Object Name>*. *<Object Name>* is the name of the Security Gateway / Cluster Member object as defined in SmartConsole.
`-all`	Prints all the licenses in the license repository.
`{-n | -noheader}`	Prints licenses with no header.
`-x`	Prints licenses with their signatures.
`{-t | -type}`	Prints licenses with their type: Central or Local.
`{-a | -attached}`	Shows to which object the license is attached. Useful, if the parameter "`-all`" is specified.

Example

```
[Expert@MGMT:0]# cplic db_print -all
 Retrieving license information from database ...

The following licenses appear in the database:
==============================================
Host             Expiration Features
192.168.3.28     25Aug2019  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx CPMP-XXX  CK-XXXXXXXXXXX
[Expert@MGMT:0]#

[Expert@MGMT:0]# cplic db_print -all -x -a
 Retrieving license information from database ...

The following licenses appear in the database:
==============================================
Host             Expiration Features
192.168.3.28     25Aug2019  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx CPMP-XXX  CK-XXXXXXXXXXX  MGMT
[Expert@MGMT:0]#
```

cplic db_rm

Description

Removes a license from the license repository on the Management Server.

After you remove the license from the repository, it can no longer use it.

Warning - You can run this command ONLY after you detach the license with the *"cplic del" on page 149* command.

Syntax

```
cplic db_rm {-h | -help}
cplic [-d] db_rm <Signature>
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
<Signature>	The signature string within the license. To see the license signature string, run the *"cplic print" on page 153* command.

Example

```
[Expert@MGMT:0]# cplic db_rm 2f540abb-d3bcb001-7e54513e-kfyigpwn
```

cplic del

Description

Deletes a Check Point license on a host, including unwanted evaluation, expired, and other licenses.

This command can delete a license on both local server, and on remote managed servers.

Syntax

```
cplic del {-h | -help}
cplic [-d] del [-F <Output File>] <Signature> <Object Name>
```

You can run this command:

- On a Management Server / Security Gateway / Cluster Member in Gaia Clish or the Expert mode
- On a Scalable Platform Security Group in Gaia gClish or the Expert mode

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-F <Output File>`	Saves the command output to the specified file.
`<Signature>`	The signature string within the license. To see the license signature string, run the *"cplic print" on page 153* command.
`<Object Name>`	The name of the Security Gateway / Cluster Member object as configured in SmartConsole.

cplic del <object name>

Description

Detaches a Central license from a remote managed Security Gateway or Cluster Member.

When you run this command, it automatically updates the license repository.

The Central license remains in the license repository as an unattached license.

Syntax

```
cplic del {-h | -help}
```

```
cplic [-d] del <Object Name> [-F <Output File>] [-ip <Dynamic IP Address>] <Signature>
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
<Object Name>	The name of the Security Gateway / Cluster Member object as defined in SmartConsole.
`-F` *<Output File>*	Saves the command output to the specified file.
`-ip` *<Dynamic IP Address>*	Deletes the license on the DAIP Security Gateway with the specified IP address. **Note** - If this parameter is used, then object name must be a DAIP Security Gateway.
<Signature>	The signature string within the license. To see the license signature string, run the *"cplic print" on page 153* command.

cplic get

Description

Retrieves all licenses from managed Security Gateways and Cluster Members into the license repository on the Management Server.

This command helps synchronize the license repository with the managed Security Gateways and Cluster Members.

When you run this command, it updates the license repository with all local changes.

Syntax

```
cplic get {-h | -help}
```

```
cplic [-d] get
      -all
      <IP Address>
      <Host Name>
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-all`	Retrieves licenses from all Security Gateways and Cluster Members in the managed network.
<IP Address>	The IP address of the Security Gateway / Cluster Member, from which licenses are to be retrieved.
<Host Name>	The name of the Security Gateway / Cluster Member object as defined in SmartConsole, from which licenses are to be retrieved.

Example

If the Security Gateway with the object name `MyGW` contains four Local licenses, and the license repository contains two other Local licenses, the command "`cplic get MyGW`" produces output similar to this:

```
[Expert@MGMT:0]# cplic get MyGW
Get retrieved 4 licenses.
Get removed 2 licenses.
[Expert@MGMT:0]#
```

cplic print

Description

Prints details of the installed Check Point licenses on the local Check Point server.

Note - On a Security Gateway / Cluster Member / Scalable Platform Security Group, this command prints all installed licenses (both Local and Central).

Syntax

```
cplic print {-h | -help}
```

```
cplic [-d] print[{-n | -noheader}] [-x] [{-t | -type}] [-F <Output File>] [{-p | -preatures}] [-D]
```

You can run this command:

- On a Management Server / Security Gateway / Cluster Member in Gaia Clish or the Expert mode
- On a Scalable Platform Security Group in Gaia gClish or the Expert mode

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{-n | -noheader}`	Prints licenses with no header.
`-x`	Prints licenses with their signature.
`{-t | -type]`	Prints licenses showing their type: Central or Local.
`-F <Output File>`	Saves the command output to the specified file.
`{-p | -preatures}`	Prints licenses resolved to primitive features.
`-D`	On a Multi-Domain Server, prints only Domain licenses.

Example 1

```
[Expert@HostName:0]# cplic print
Host             Expiration   Features
192.168.3.28     25Aug2019    CPMP-XXX  CK-XXXXXXXXXXX
[Expert@HostName:0]#
```

Example 2

```
[Expert@HostName:0]# cplic print -x
Host             Expiration   Signature                          Features
192.168.3.28     25Aug2019    xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx   CPMP-XXX  CK-XXXXXXXXXXX
[Expert@HostName:0]#
```

cplic put

Description

Installs one or more Local licenses on a Check Point server.

Note - You get the license details in the *Check Point User Center*.

Syntax

```
cplic put {-h | -help}
```

```
cplic [-d] put [{-o | -overwrite}] [{-c | -check-only}] [{-s | -select}] [-F <Output File>] [{-P | -Pre-boot}] [{-k | -kernel-only}] -l <License File> [<Host>] [<Expiration Date>] [<Signature>] [<SKU/Features>]
```

You can run this command:

- On a Management Server / Security Gateway / Cluster Member in Gaia Clish or the Expert mode
- On a Scalable Platform Security Group in Gaia gClish or the Expert mode

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{-o | -overwrite}`	On a Security Gateway / Cluster Member / Scalable Platform Security Group, this command erases only the local licenses, but not central licenses that are installed remotely.
`{-c | -check-only}`	Verifies the license. Checks if the IP of the license matches the Check Point server and if the signature is valid.
`{-s | -select}`	Selects only the local license whose IP address matches the IP address of the Check Point server.

Parameter	Description
`-F <Output File>`	Saves the command output to the specified file.
`{-P | -Pre-boot}`	Use this option after you have upgraded and before you reboot the Check Point server. Use of this option will prevent certain error messages.
`{-K | -kernel-only}`	Pushes the current valid licenses to the kernel. For use by Check Point Support only.
`-l <License File>`	Name of the file that contains the license.
`<Host>`	Hostname or IP address of the Security Gateway / Cluster Member / Scalable Platform Security Group for a local license. Hostname or IP address of the Security Management Server / Domain Management Server for a central license.
`<Expiration Date>`	The license expiration date.
`<Signature>`	The signature string within the license. Case sensitive. The hyphens are optional.
`<SKU/Features>`	The SKU of the license summarizes the features included in the license. For example: `CPSUITE-EVAL-3DES-vNG`

Copy and paste the parameters from the license received from the User Center:

Parameter	Description
`host`	The IPv4 address of the external interface (in quad-dot notation).
`expiration date`	The license expiration date. It can be `never`.
`signature`	The license signature string. Case sensitive. The hyphens are optional.
`SKU/features`	A string listing the SKU and the Certificate Key of the license. The SKU of the license summarizes the features included in the license. For example: `CPSB-SWB CPSB-ADNC-M CK0123456789ab`

Example

```
[Expert@HostName:0]# cplic put -l License.lic
Host Expiration SKU
192.168.2.3 14Jan2016  CPSB-SWB CPSB-ADNC-M CK0123456789ab
[Expert@HostName:0]#
```

cplic put <object name>

Description

Attaches one or more Central or Local licenses to a remote managed Security Gateways and Cluster Members.

When you run this command, it automatically updates the license repository.

Note

- You get the license details in the *Check Point User Center*.
- You can attach more than one license.

Syntax

```
cplic put {-h | -help}
```

```
cplic [-d] put <Object Name> [-ip<Dynamic IP Address> ] [-F
<Output File>] -l <License File> [<Host>] [<Expiration Date>]
[<Signature>] [<SKU/Feature>]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
<Object Name>	The name of the Security Gateway / Cluster Member object, as defined in SmartConsole.
`-ip` *<Dynamic IP Address>*	Installs the license on the Security Gateway with the specified IP address. This parameter is used to install a license on a Security Gateway with dynamically assigned IP address (DAIP). **Note** - If you use this parameter, then the object name must be that of a DAIP Security Gateway.
`-F` *<Output File>*	Saves the command output to the specified file.
`-l` *<License File>*	Installs the licenses from the *<License file>*.
<Host>	Hostname or IP address of the Security Management Server / Domain Management Server.
<Expiration Date>	The license expiration date.
<Signature>	The license signature string. Case sensitive. The hyphens are optional.
<SKU/Features>	The SKU of the license summarizes the features included in the license. For example: `CPSUITE-EVAL-3DES-vNG`

Copy and paste the parameters from the license received from the User Center:

Parameter	Description
`host`	The IP address of the external interface (in quad-dot notation). The last part cannot be 0 or 255.
`expiration date`	The license expiration date. It can be `never`.
`signature`	The license signature string. Case sensitive. The hyphens are optional.
`SKU/features`	A string listing the SKU and the Certificate Key of the license. The SKU of the license summarizes the features included in the license. For example: `CPSB-SWB CPSB-ADNC-M CK0123456789ab`

cplic upgrade

Description

Upgrades licenses in the license repository with licenses in the specified license file.

Note - You get this license file in the *Check Point User Center*.

Syntax

```
cplic upgrade {-h | -help}
cplic [-d] upgrade -l <Input File>
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-l <Input File>`	Upgrades the licenses in the license repository and Check Point Security Gateways / Cluster Members to match the licenses in the specified file.

Example

This example explains the procedure to upgrade the licenses in the license repository.

There are two Software Blade licenses in the input file:

- One license does not match any license on a remote managed Security Gateway.
- The other license matches an NGX-version license on a managed Security Gateway that has to be upgraded.

Workflow in this example:

1. Upgrade the Security Management Server to the latest version.

   Ensure that there is connectivity between the Security Management Server and the Security Gateways with the previous product versions.

2. Import all licenses into the license repository.

   You can also do this after you upgrade the products on the remote Security Gateways.

3. Run this command:

```
cplic get -all
```

Example:

```
[Expert@MyMGMT]# cplic get -all
Getting licenses from all modules ...
MyGW:
Retrieved 1 licenses
```

4. To see all the licenses in the repository, run this command:

   ```
   cplic db_print -all -a
   ```

   Example:

   ```
   [Expert@MyMGMT]# cplic db_print -all -a
   Retrieving license information from database ...

   The following licenses appear in the database:
   ================================================
   Host Expiration Features
   192.0.2.11 Never CPFW-FIG-25-53 CK49C3A3CC7121 MyGW1
   192.0.2.11 26Nov2017 CPSB-SWB CPSB-ADNC-M CK0123456789ab MyGW2
   ```

5. In the *Check Point User Center*, view the licenses for the products that were upgraded from version NGX to a Software Blades license.

   You can also create new upgraded licenses.

6. Download a file containing the upgraded licenses.

   Only download licenses for the products that were upgraded from version NGX to Software Blades.

7. If you did not import the version NGX licenses into the repository, import the version NGX licenses now.

   Use this command:

   ```
   cplic get -all
   ```

8. Run the license upgrade command:

   ```
   cplic upgrade -l <Input File>
   ```

   - The licenses in the downloaded license file and in the license repository are compared.
   - If the certificate keys and features match, the old licenses in the repository and in the remote Security Gateways are updated with the new licenses.
   - A report of the results of the license upgrade is printed.

For more about managing licenses, see the *R81.20 Security Management Administration Guide*.

cpmiquerybin

Description

The `cpmiquerybin` utility connects to a specified database, runs a user-defined query and shows the query results.

The results can be a collection of Security Gateway sets or a tab-delimited list of specified fields from each retrieved object.

The default database of the query tool is based on the shell environment settings.

To connect to a Domain Management Server database, run *"mdsenv" on page 766* and define the necessary environment variables.

Use the Domain Management Server name or IP address as the first parameter.

Notes:

- You can see complete documentation of the `cpmiquerybin` utility, with the full query syntax, examples, and a list of common attributes in sk65181.
- The `MISSING_ATTR` string shows when you use an attribute name that does not exist in the objects in query result.

Syntax

```
cpmiquerybin <query_result_type> <database> <table> <query> [-a
<attributes_list>]
```

Parameters

Parameter	Description
<query_result_type>	Query result in one of these formats: ■ `attr` - Returns values from one or more specified fields for each object. Use the "`-a`" parameter followed by a comma separated list of fields. ■ `object` - Shows Security Gateway sets containing data of each retrieved object.
<database>	Name of the database file in quotes. For example, "`mdsdb`". Use empty double quotes `""` to run the query on the default database.
<table>	Name of the database table that contains the data.
<query>	One or more query strings in a comma separated list. Use empty double quotes (`""`) to return all objects in the database table. You can use the asterisk character (*) as a wildcard replacement for one or more matching characters in your query string.
`-a` *<attributes_list>*	If you use the "`query_result_type`" parameter, you must specify one or more attributes in a comma-delimited list (without spaces) of object fields. You can return all object names with the special string: `__name__`

Return Values

- **0** - Query returns data successfully
- **1** - Query does not return data or there is a query syntax error

Example - Viewing the names of the currently defined network objects

```
[Expert@HostName:0]# cpmiquerybin attr "" network_objects "" -a __name__
DMZZone
WirelessZone
ExternalZone
InternalZone
AuxiliaryNet
LocalMachine_All_Interfaces
CPDShield
InternalNet
LocalMachine
DMZNet
[Expert@HostName:0]#
```

cppkg

Description

Manages the SmartUpdate software packages repository on the Security Management Server.

Important - Installing software packages with the SmartUpdate is not supported for Security Gateways running on Gaia OS.

Syntax

```
cppkg
      add <options>
      {del | delete} <options>
      get
      getroot
      print
      setroot <options>
```

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run `mdsenv`).

Parameters

Parameter	Description
`add <options>`	Adds a SmartUpdate software package to the repository. See *"cppkg add" on page 173*.
`{del | delete} <options>`	Deletes a SmartUpdate software package from the repository. See *"cppkg delete" on page 174*.
`get`	Updates the list of the SmartUpdate software packages in the repository. See *"cppkg get" on page 176*.
`getroot`	Shows the path to the root directory of the repository (the value of the environment variable `$SUROOT`). See *"cppkg getroot" on page 177*.
`print`	Prints the list of SmartUpdate software packages in the repository. See *"cppkg print" on page 178*.
`setroot <options>`	Configures the path to the root directory of the repository. See *"cppkg setroot" on page 179*.

cppkg add

Description

Adds a SmartUpdate software package to the SmartUpdate software packages repository.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).
- This command does not overwrite existing packages. To overwrite an existing package, you must first delete the existing package.
- You get the SmartUpdate software packages from the *Check Point Support Center*.

Syntax

```
cppkg add <Full Path to Package | DVD Drive [Product]>
```

Parameters

Parameter	Description
<Full Path to Package>	Specifies the full local path on the computer to the SmartUpdate software package.
DVD Drive `[Product]`	Specifies the DVD root path. Example: `/mnt/CPR80`

Example - Adding R77.20 HFA_75 (R77.20.75) firmware package for 1100 Appliances

```
[Expert@MGMT:0]# cppkg print
Vendor          Product              Version    OS                   Minor Version
-------------------------------------------------------------------------------
[Expert@MGMT:0]#

[Expert@MGMT:0]# cppkg add /var/log/CP1100_6.0_4_0_-.tgz
Adding package to the repository
Getting the package type...
Extracting the package files...
Copying package to the repository...
Package was successfully added to the repository
[Expert@MGMT:0]#

[Expert@MGMT:0]# cppkg print
Vendor          Product              Version    OS                   Minor Version
-------------------------------------------------------------------------------
Check Point     CP1100               R77.20     Gaia Embedded        R77.20
[Expert@MGMT:0]#
```

ppkg delete

Description

Deletes SmartUpdate software packages from the SmartUpdate software packages repository.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).

Syntax

```
cppkg del ["<Vendor>" "<Product>" "<Major Version>" "<OS>" "<Minor Version>"]
```

```
cppkg delete ["<Vendor>" "<Product>" "<Major Version>" "<OS>" "<Minor Version>"]
```

Parameters

Parameter	Description
`del | delete`	When you do not specify optional parameters, the command runs in the interactive mode. The command shows the menu with applicable options.
`"<Vendor>"`	Specifies the package vendor. Enclose in double quotes.
`"<Product>"`	Specifies the product name. Enclose in double quotes.
`"<Major Version>"`	Specifies the package Major Version. Enclose in double quotes.
`"<OS>"`	Specifies the package OS. Enclose in double quotes.
`"<Minor Version>"`	Specifies the package Minor Version. Enclose in double quotes.

Notes:

- To see the values for the optional parameters, run the *"cppkg print" on page 178* command.
- You must specify all optional parameters, or no parameters.

Example 1 - Interactive mode

```
[Expert@MGMT:0]# cppkg delete

Select package:
--------------------
(0) Delete all
(1) CP1100 Gaia Embedded Check Point R77.20 R77.20

(e) Exit

Enter your choice : 1

You chose to delete 'CP1100 Gaia Embedded Check Point R77.20 R77.20', Is this correct? [y/n] : y

Package was successfully removed from the repository
[Expert@MGMT:0]#
```

Example 2 - Manually deleting the specified package

```
Expert@MGMT:0]# cppkg print
Vendor          Product              Version    OS                  Minor Version
-------------------------------------------------------------------------------
Check Point     CP1100               R77.20     Gaia Embedded       R77.20
[Expert@MGMT:0]#

[Expert@MGMT:0]# cppkg delete "Check Point" "CP1100" "R77.20" "Gaia Embedded" "R77.20"
Package was successfully removed from the repository
[Expert@MGMT:0]#
```

cppkg get

Description

Updates the list of the SmartUpdate software packages in the SmartUpdate software packages repository based on the real content of the repository.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).

Syntax

```
cppkg get
```

Example

```
[Expert@MGMT:0]# cppkg get
Update successfully completed
[Expert@MGMT:0]#
```

cppkg getroot

Description

Shows the path to the root directory of the SmartUpdate software packages repository (the value of the environment variable `$SUROOT`)

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).

Syntax

```
cppkg getroot
```

Example

```
[Expert@MGMT:0]# cppkg getroot
[cppkg 7119 4128339728]@MGMT[29 May 19:16:06] Current repository root is set to :
/var/log/cpupgrade/suroot
[Expert@MGMT:0]#
```

cppkg print

Description

Prints the list of SmartUpdate software packages in the SmartUpdate software packages repository.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).

Syntax

```
cppkg print
```

Example - R77.20 HFA_75 (R77.20.75) firmware package for 1100 Appliances

```
[Expert@MGMT:0]# cppkg print
Vendor          Product              Version    OS                  Minor Version
-------------------------------------------------------------------------------
Check Point     CP1100               R77.20     Gaia Embedded       R77.20
[Expert@MGMT:0]#
```

cppkg setroot

Description

Configures the path to the root directory of the SmartUpdate software packages repository.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the MDS (run the `mdsenv` command).
- The default path is: `/var/log/cpupgrade/suroot`
- When changing repository root directory:
  - This command copies the software packages from the old repository to the new repository. A package in the new location is overwritten by a package from the old location, if the packages have the same name.
  - This command updates the value of the environment variable `$SUROOT` in the Check Point Profile shell scripts (`$CPDIR/tmp/.CPprofile.sh` and `$CPDIR/tmp/.CPprofile.csh`).

Syntax

```
cppkg setroot <Full Path to Repository Root Directory>
```

Example

```
[Expert@MGMT:0]# cppkg setroot /var/log/my_directory

Repository root is set to : /var/log/cpupgrade/suroot

Note : When changing repository root directory :

       1. Old repository content will be copied into the new repository
       2. A package in the new location will be overwritten by a package in the old
          location, if the packages have the same name

Change the current repository root ? [y/n] : y

The new repository directory does not exist. Create it ? [y/n] : y

Repository root was set to : /var/log/my_directory

Notice : To complete the setting of your directory, reboot the machine!
[Expert@MGMT:0]#
```

cpprod_util

Description

This utility works with Check Point Registry (`$CPDIR/registry/HKLM_registry.data`) without manually opening it:

- Shows which Check Point products and features are enabled on this Check Point server.
- Enables and disables Check Point products and features on this Check Point server.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpprod_util CPPROD_GetValue "<Product>" "<Parameter>" {0|1}
```

```
cpprod_util CPPROD_SetValue "<Product>" "<Parameter>" {1|4}
"<Value>" {0|1}
```

```
cpprod_util -dump
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpprod_util CPPROD_GetValue "<Product>" "<Parameter>" {0|1}
```

```
cpprod_util CPPROD_SetValue "<Product>" "<Parameter>" {1|4}
"<Value>" {0|1}
```

```
cpprod_util -dump
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpprod_util CPPROD_GetValue "<Product>" "<Parameter>" {0|1}
```

```
cpprod_util CPPROD_SetValue "<Product>" "<Parameter>" {1|4}
"<Value>" {0|1}
```

```
cpprod_util -dump
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpprod_util CPPROD_GetValue "<Product>" "<Parameter>" {0|1}
```

```
g_all cpprod_util CPPROD_SetValue "<Product>" "<Parameter>" {1|4}
"<Value>" {0|1}
```

```
g_all cpprod_util -dump
```

Parameters

Parameter	Description
`CPPROD_GetValue`	Gets the configuration status of the specified product or feature: ■ 0 - Disabled ■ 1 - Enabled
`CPPROD_SetValue`	Sets the configuration for the specified product or feature. **Important** - Do not run these commands unless explicitly instructed by Check Point Support or R&D to do so.
"<*Product*>"	Specifies the product or feature.
"<*Parameter*>"	Specifies the configuration parameter for the specified product or feature.
"<*Value*>"	Specifies the value of the configuration parameter for the specified product or feature: ■ One of these integers: 0, 1, 4 ■ A string
`dump`	Creates a dump file of the Check Point Registry (`$CPDIR/registry/HKLM_registry.data`) in the current working directory. The name of the output file is `RegDump`.

Notes

- On a Multi-Domain Server, you must run this command in the context of the relevant Domain Management Server.
- If you run the "`cpprod_util`" command without parameters, it prints:
  - The list of all available products and features (for example, "`FwIsFirewallMgmt`", "`FwIsLogServer`", "`FwIsStandAlone`")
  - The type of the expected argument when you configure a product or feature ("`no-parameter`", "`string-parameter`", or "`integer-parameter`")
  - The type of the returned output ("`status-output`", or "`no-output`")
- To redirect the output of the "`cpprod_util`" command, it is necessary to redirect the *stderr* to *stdout*:

  ```
  cpprod_util <options> > <output file> 2>&1
  ```

  Example:

  ```
  cpprod_util > /tmp/output_of_cpprod_util.txt 2>&1
  ```

Examples

Example - Showing a list of all installed Check Point Products Packages on a Management Server

```
[Expert@MGMT:0]# cpprod_util CPPROD_GetInstalledProducts
CPFC
IDA
MGMT
FW1
SecurePlatform
NGXCMP
EdgeCmp
SFWCMP
SFWR75CMP
SFWR77CMP
FLICMP
R75CMP
R7520CMP
R7540CMP
R76CMP
R77CMP
PROVIDER-1
Reporting Module
SmartLog
CPinfo
VSEC
DIAG
[Expert@MGMT:0]#
```

Example - Checking if this Check Point server is configured as a Management Server

```
[Expert@MGMT:0]# cpprod_util FwIsFirewallMgmt
1
[Expert@MGMT:0]#
```

Example - Checking if this Check Point server is configured as a Standalone

```
[Expert@MGMT:0]# cpprod_util FwIsStandAlone
0
[Expert@MGMT:0]#
```

Example - Checking if this Management Server is configured as a Primary in High Availability

```
[Expert@MGMT:0]# cpprod_util FwIsPrimary
1
[Expert@MGMT:0]#
```

Example - Checking if this Management Server is configured as Active in High Availability

```
[Expert@MGMT:0]# cpprod_util FwIsActiveManagement
1
[Expert@MGMT:0]#
```

Example - Checking if this Management Server is configured as Backup in High Availability

```
[Expert@MGMT:0]# cpprod_util FwIsSMCBackup
1
[Expert@MGMT:0]#
```

Example - Checking if this Check Point server is configured as a dedicated Log Server

```
[Expert@MGMT:0]# cpprod_util FwIsLogServer
1
[Expert@MGMT:0]#
```

Example - Checking if on this Management Server the SmartProvisioning blade is enabled

```
[Expert@MGMT:0]# cpprod_util FwIsAtlasManagement
1
[Expert@MGMT:0]#
```

Example - Checking if on this Management Server the SmartEvent Server blade is enabled

```
[Expert@MGMT:0]# cpprod_util RtIsAnalyzerServer
1
[Expert@MGMT:0]#
```

Example - Checking if on this Management Server the SmartEvent Correlation Unit blade is enabled

```
[Expert@MGMT:0]# cpprod_util RtIsAnalyzerCorrelationUnit
1
[Expert@MGMT:0]#
```

Example - Checking if on this Management Server the Endpoint Policy Management blade is enabled

```
[Expert@MGMT:0]# cpprod_util UepmIsInstalled
1
[Expert@MGMT:0]#
```

Example - Checking if this Management Server is configured as Endpoint Policy Server

```
[Expert@MGMT:0]# cpprod_util UepmIsPolicyServer
0
[Expert@MGMT:0]#
```

Example - Showing a list of all installed Check Point Products Packages on a Security Gateway

```
[Expert@MyGW:0]# cpprod_util CPPROD_GetInstalledProducts
CPFC
IDA
MGMT
FW1
SecurePlatform
CPinfo
DIAG
PPACK
CVPN
[Expert@MyGW:0]#
```

Example - Checking if this Security Gateway is configured as a VSX Gateway

```
[Expert@MyGW:0]# cpprod_util FwIsVSX
0
[Expert@MyGW:0]#
```

Example - Checking if on this Security Gateway the QoS blade is enabled

```
[Expert@MyGW:0]# cpprod_util FwIsFloodGate
1
[Expert@MyGW:0]#
```

Example - Checking if on this Security Gateway the SmartProvisioning is enabled

```
[Expert@MyGW:0]# cpprod_util FwIsAtlasModule
0
[Expert@MyGW:0]#
```

Example - Checking if this Security Gateway is configured in Bridge Mode

```
[Expert@MyGW:0]# cpprod_util FwIsBridge
0
[Expert@MyGW:0]#
```

Example - Checking if this Security Gateway is a member of Full HA cluster

```
[Expert@MyGW:0]# cpprod_util FwIsFullHA
0
[Expert@MyGW:0]#
```

Example - Checking if this Security Gateway is configured with Dynamically Assigned IP (DAIP)

```
[Expert@MyGW:0]# cpprod_util FwIsDAG
0
[Expert@MyGW:0]#
```

Example - Checking if this Security Gateway is configured with IPv6 addresses

```
[Expert@MyGW:0]# cpprod_util FwIsFireWallIPv6
1
[Expert@MyGW:0]#
```

cprid

Description

Manages the Check Point Remote Installation Daemon (`cprid`).

This daemon is used for remote upgrade and installation of Check Point products on the managed Security Gateways.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run these commands in the context of the MDS (run `mdsenv`).

Commands

Syntax	Description
`cpridstart`	Starts the Check Point Remote Installation Daemon (`cprid`).
`cpridstop`	Stops the Check Point Remote Installation Daemon (`cprid`).
`run_cprid_restart`	Stops and then starts the Check Point Remote Installation Daemon (`cprid`).

cprinstall

Description

Performs installation of Check Point product packages and associated operations on remote managed Security Gateways.

Important - Installing software packages with this command is not supported for Security Gateways that run on Gaia OS.

Notes:

- This command requires a license for SmartUpdate.
- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- On the remote Security Gateways these are required:
  - SIC Trust must be established between the Security Management Server and the Security Gateway.
  - The `cpd` daemon must run.
  - The `cprid` daemon must run.

Syntax

```
cprinstall
      boot <options>
      cprestart <options>
      cpstart <options>
      cpstop <options>
      delete <options>
      get <options>
      install <options>
      revert <options>
      show <options>
      snapshot <options>
      transfer <options>
      uninstall <options>
      verify <options>
```

Parameters

Parameter	Description
`boot <options>`	Reboots the managed Security Gateway. See *"cprinstall boot" on page 190*.
`cprestart <options>`	Runs the `cprestart` command on the managed Security Gateway. See *"cprinstall cprestart" on page 191*.
`cpstart <options>`	Runs the `cpstart` command on the managed Security Gateway. See *"cprinstall cpstart" on page 192*.
`cpstop <options>`	Runs the `cpstop` command on the managed Security Gateway. See *"cprinstall cpstop" on page 193*.
`delete <options>`	Deletes a snapshot (backup) file on the managed Security Gateway. See *"cprinstall delete" on page 194*.
`get <options>`	■ Gets details of the products and the operating system installed on the managed Security Gateway. ■ Updates the management database on the Security Management Server. See *"cprinstall get" on page 195*.
`install <options>`	Installs Check Point products on the managed Security Gateway. See *"cprinstall install" on page 196*.
`revert <options>`	Restores the managed Security Gateway that runs on SecurePlatform OS from a snapshot saved on that Security Gateway. See *"cprinstall revert" on page 199*.
`show <options>`	Displays all snapshot (backup) files on the managed Security Gateway that runs on SecurePlatform OS. See *"cprinstall show" on page 200*.
`snapshot <options>`	Creates a snapshot on the managed Security Gateway that runs on SecurePlatform OS and saves it on that Security Gateway. See *"cprinstall snapshot" on page 201*.
`transfer <options>`	Transfers a software package from the repository to the managed Security Gateway without installing the package. See *"cprinstall transfer" on page 202*.
`uninstall <options>`	Uninstalls Check Point products on the managed Security Gateway. See *"cprinstall uninstall" on page 204*.

Parameter	Description
`verify <options>`	Confirms these operations were successful: ■ If a specific product can be installed on the managed Security Gateway. ■ That the operating system and currently installed products the managed Security Gateway are appropriate for the software package. ■ That there is enough disk space to install the product the managed Security Gateway. ■ That there is a CPRID connection with the managed Security Gateway. See *"cprinstall verify" on page 206*.

cprinstall boot

Description

Reboots the managed Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall boot <Object Name>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example

```
[Expert@MGMT]# cprinstall boot MyGW
```

cprinstall cprestart

Description

Runs the `cprestart` command on the managed Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- All Check Point products on the managed Security Gateway must be of the same version.

Syntax

```
cprinstall cprestart <Object Name>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example

```
[Expert@MGMT:0]# cprinstall cprestart MyGW
```

cprinstall cpstart

Description

Runs the `cpstart` command on the managed Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- All Check Point products on the managed Security Gateway must be of the same version.

Syntax

```
cprinstall cpstart <Object Name>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example

```
[Expert@MGMT]# cprinstall cpstart MyGW
```

cprinstall cpstop

Description

Runs the `cpstop` command on the managed Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- All Check Point products on the managed Security Gateway must be of the same version.

Syntax

```
cprinstall cpstop {-proc | -nopolicy} <Object Name>
```

Parameters

Parameter	Description
`-proc`	Kills the Check Point daemons and Security Servers, while it maintains the active Security Policy running in the Check Point kernel. Rules with generic *Allow*, *Drop* or *Reject* action based on services, continue to work.
`-nopolicy`	Kills the Check Point daemons and Security Servers and unloads the Security Policy from the Check Point kernel.
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example

```
[Expert@MGMT]# cprinstall cpstop -proc MyGW
```

cprinstall delete

Description

Deletes a snapshot (backup) file on the managed Security Gateway that runs on SecurePlatform OS.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall delete <Object Name> <Snapshot File>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
<Snapshot File>	Specifies the name of the snapshot (backup) on SecurePlatform OS.

Example

```
[Expert@MGMT]# cprinstall delete MyGW Snapshot25Apr2017
```

cprinstall get

Description

- Gets details of the products and the operating system installed on the managed Security Gateway.
- Updates the management database on the Security Management Server.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall get <Object Name>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example:

```
[Expert@MGMT]# cprinstall get MyGW
Checking cprid connection...
Verified
Operation completed successfully
Updating machine information...
Update successfully completed
'Get Gateway Data' completed successfully
Operating system   Major Version      Minor Version
-------------------------------------------------------------------
SecurePlatform     R75.20             R75.20

Vendor             Product            Major Version       Minor Version
-------------------------------------------------------------------
Check Point        VPN-1 Power/UTM    R75.20              R75.20
Check Point        SecurePlatform     R75.20              R75.20
Check Point        SmartPortal        R75.20              R75.20
[Expert@MGMT]#
```

cprinstall install

Description

Installs Check Point products on the managed Security Gateway.

Important - Installing software packages with this command is not supported for Security Gateways that run Gaia OS.

Notes:

- Before transferring the software package, this command runs the *"cprinstall verify" on page 206* command.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- To see the values for the package attributes, run the *"cppkg print" on page 178* command.

Syntax

```
cprinstall install [-boot] [-backup] [-skip_transfer] <Object
Name> "<Vendor>" "<Product>" "<Major Version>" "<Minor Version>"
```

Parameters

Parameter	Description
`-boot`	Reboots the managed Security Gateway after installing the package. **Note** - Only reboot after ALL products have the same version. Reboot is canceled in certain scenarios.
`-backup`	Creates a snapshot on the managed Security Gateway before installing the package. **Note** - Only on Security Gateways that runs on SecurePlatform OS.
`-skip_ transfer`	Skip the transfer of the package.
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
"*<Vendor>*"	Specifies the package vendor. Enclose in double quotes. Example: ■ `checkpoint` ■ `Check Point`
"*<Product>*"	Specifies the product name. Enclose in double quotes. Examples: ■ `SVNfoundation` ■ `firewall` ■ `floodgate` ■ `CP1100` ■ `VPN-1 Power/UTM` ■ `SmartPortal`
"*<Major Version>*"	Specifies the package Major Version. Enclose in double quotes.
"*<Minor Version>*"	Specifies the package Minor Version. Enclose in double quotes.

Example

```
[Expert@MGMT]# cprinstall install -boot MyGW "checkpoint" "firewall" "R75" "R75.20"

Installing firewall R75.20 on MyGW...
Info : Testing Check Point Gateway
Info : Test completed successfully.
Info : Transferring Package to Check Point Gateway
Info : Extracting package on Check Point Gateway
Info : Installing package on Check Point Gateway
Info : Product was successfully applied.
Info : Rebooting the Check Point Gateway
Info : Checking boot status
Info : Reboot completed successfully.
Info : Checking Check Point Gateway
Info : Operation completed successfully.
[Expert@MGMT]#
```

cprinstall revert

Description

Restores the managed Security Gateway that runs on SecurePlatform OS from a snapshot saved on that Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall revert <Object Name> <Snapshot File>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
<Snapshot File>	Name of the SecurePlatform snapshot file. To see the names of the saved snapshot files, run the *"cprinstall show" on page 200* command.

cprinstall show

Description

Displays all snapshot (backup) files on the managed Security Gateway that runs on SecurePlatform OS.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall show <Object Name>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.

Example

```
[Expert@MGMT]# cprinstall show GW1
SU_backup.tzg
[Expert@MGMT]#
```

cprinstall snapshot

Description

Creates a snapshot on the managed Security Gateway that runs on SecurePlatform OS and saves it on that Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
cprinstall snapshot <Object Name> <Snapshot File>
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
<Snapshot File>	Name of the SecurePlatform snapshot file. To see the names of the saved snapshot files, run the *"cprinstall show" on page 200* command.

cprinstall transfer

Description

Transfers a software package from the repository to the managed Security Gateway without installing the package.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- To see the values for the package attributes, run the *"cppkg print" on page 178* command.

Syntax

```
cprinstall transfer <Object Name> "<Vendor>" "<Product>" "<Major Version>" "<Minor Version>"
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
"*<Vendor>*"	Specifies the package vendor. Enclose in double quotes. Example: ■ `checkpoint` ■ `Check Point`
"*<Product>*"	Specifies the product name. Enclose in double quotes. Examples: ■ `SVNfoundation` ■ `firewall` ■ `floodgate` ■ `CP1100`
"*<Major Version>*"	Specifies the package major version. Enclose in double quotes.
"*<Minor Version>*"	Specifies the package minor version. Enclose in double quotes.

cprinstall uninstall

Description

Uninstalls Check Point products on the managed Security Gateway.

Important - Uninstalling software packages with this command is not supported for Security Gateways running on Gaia OS.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- Before uninstalling product packages, this command runs the *"cprinstall verify" on page 206* command.
- After uninstalling a product package, you must run the *"cprinstall get" on page 195* command.
- To see the values for the package attributes, run the *"cppkg print" on page 178* command.

Syntax

```
cprinstall uninstall [-boot] <Object Name> "<Vendor>" "<Product>"
"<Major Version>" "<Minor Version>"
```

Parameters

Parameter	Description
`-boot`	Reboots the managed Security Gateway after uninstalling the package. **Note** - Reboot is canceled in certain scenarios.
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
"*<Vendor>*"	Specifies the package vendor. Enclose in double quotes. Example: ■ `checkpoint` ■ `Check Point`
"*<Product>*"	Specifies the product name. Enclose in double quotes. Examples: ■ `SVNfoundation` ■ `firewall` ■ `floodgate` ■ `CP1100`
"*<Major Version>*"	Specifies the package major version. Enclose in double quotes.
"*<Minor Version>*"	Specifies the package minor version. Enclose in double quotes.

Example

```
[Expert@MGMT]# cprinstall uninstall MyGW "checkpoint" "firewall" "R75.20" "R75.20"
Uninstalling firewall R75.20 from MyGW...
Info : Removing package from Check Point Gateway
Info : Product was successfully applied.
Operation Success. Please get network object data to complete the operation.
[Expert@MGMT]#
[Expert@MGMT]# cprinstall get
```

cprinstall verify

Description

Confirms these operations were successful:

- If a specific product can be installed on the managed Security Gateway.
- That the operating system and currently installed products the managed Security Gateway are appropriate for the software package.
- That there is enough disk space to install the product the managed Security Gateway.
- That there is a CPRID connection with the managed Security Gateway.

Notes:

- You must run this command from the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```
- To see the values for the package attributes, run the *"cppkg print" on page 178* command.

Syntax

```
cprinstall verify <Object Name> "<Vendor>" "<Product>" "<Major
Version>" ["<Minor Version>"]
```

Parameters

Parameter	Description
<Object Name>	The name of the Security Gateway object as configured in SmartConsole.
"*<Vendor>*"	Specifies the package vendor. Enclose in double quotes. Example: ■ `checkpoint` ■ `Check Point`
"*<Product>*"	Specifies the product name. Enclose in double quotes. Examples: ■ `SVNfoundation` ■ `firewall` ■ `floodgate` ■ `CP1100` ■ `VPN-1 Power/UTM` ■ `SmartPortal`
"*<Major Version>*"	Specifies the package major version. Enclose in double quotes.
"*<Minor Version>*"	Specifies the package minor version. Enclose in double quotes. This parameter is optional.

Example 1 - Verification succeeds

```
[Expert@MGMT]# cprinstall verify MyGW "checkpoint" "SVNfoundation" "R75.20"
Verifying installation of SVNfoundation R75.20 on MyGW...
Info : Testing Check Point Gateway.
Info : Test completed successfully.
Info : Installation Verified, The product can be installed.
```

Example 2 - Verification fails

```
[Expert@MGMT]# cprinstall verify MyGW "checkpoint" "SVNfoundation" "R75.20"
Verifying installation of SVNfoundation R75.20 on MyGW...
Info : Testing Check Point Gateway
Info : SVN Foundation R75 is already installed on 192.0.2.134
Operation Success. Product cannot be installed, did not pass dependency check.
```

cpstat

Description

Shows the status and statistics information for Check Point applications.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpstat [-d] [-h <Host>] [-p <Port>] [-s <SICname>] [-f <Flavor>]
[-o <Polling Interval> [-c <Count>] [-e <Period>]] <Application
Flag>
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpstat [-d] [-h <Host>] [-p <Port>] [-s <SICname>] [-f <Flavor>]
[-o <Polling Interval> [-c <Count>] [-e <Period>]] <Application
Flag>
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpstat [-d] [-h <Host>] [-p <Port>] [-s <SICname>] [-f <Flavor>]
[-o <Polling Interval> [-c <Count>] [-e <Period>]] <Application
Flag>
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpstat [-d] [-h <Host>] [-p <Port>] [-s <SICname>] [-f
<Flavor>] [-o <Polling Interval> [-c <Count>] [-e <Period>]]
<Application Flag>
```

Note - You can write the parameters in the syntax in any order.

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. The output shows the SNMP queries and SNMP responses for the applicable SNMP OIDs.
`-h <Host>`	Optional. When you run this command on a Management Server, this parameter specifies the managed Security Gateway / ClusterXL object. *<Host>* is an IPv4 address, a resolvable hostname, or a DAIP object name. The default is `localhost`. **Note** - On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:`mdsenv <IP Address or Name of Domain Management Server>`.
`-p <Port>`	Optional. Port number of the Application Monitoring (AMON) server. The default port is 18192.
`-s <SICname>`	Optional. Secure Internal Communication (SIC) name of the Application Monitoring (AMON) server.
`-f <Flavor>`	Optional. Specifies the type of the information to collect. If you do not specify a flavor explicitly, the command uses the first flavor in the *<Application Flag>*. To see all flavors, run the `cpstat` command without any parameters.

Parameter	Description
`-o <Polling Interval>`	Optional. Specifies the polling interval (in seconds) - how frequently the command collects and shows the information. Examples: ■ 0 - The command shows the results only once and the stops (this is the default value). ■ 5 - The command shows the results every 5 seconds in the loop. ■ 30 - The command shows the results every 30 seconds in the loop. ■ N - The command shows the results every N seconds in the loop. Use this parameter together with the "`-c <Count>`" parameter and the "`-e <Period>`" parameter. Example: `cpstat os -f perf -o 2`
`-c <Count>`	Optional. Specifies how many times the command runs and shows the results before it stops. You must use this parameter together with the "`-o <Polling Interval>`" parameter. Examples: ■ 0 - The command shows the results repeatedly every <*Polling Interval*> (this is the default value). ■ 10 - The command shows the results 10 times every <*Polling Interval*> and then stops. ■ 20 - The command shows the results 20 times every <*Polling Interval*> and then stops. ■ N - The command shows the results N times every <*Polling Interval*> and then stops. Example: `cpstat os -f perf -o 2 -c 2`

Parameter	Description
`-e <Period>`	Optional. Specifies the time (in seconds), over which the command calculates the statistics. You must use this parameter together with the "`-o <Polling Interval>`" parameter. You can use this parameter together with the "`-c <Count>`" parameter. Example: `cpstat os -f perf -o 2 -c 2 -e 60`
`<Application Flag>`	Mandatory. See the table below with flavors for the application flags.

These flavors are available for the application flags

Note - The available flags depend on the enabled Software Blades. Some flags are supported only by a Security Gateway / ClusterXL, and some flags are supported only by a Management Server.

Feature or Software Blade	Flag	Flavors
List of enabled Software Blades	`blades`	`fw, ips, av, urlf, vpn, cvpn, aspm, dlp, appi, anti_bot, default, content_awareness, threat-emulation, default`
Operating System	`os`	`default, ifconfig, routing, routing6, memory, old_memory, cpu, disk, perf, multi_cpu, multi_disk, raidInfo, sensors, power_supply, hw_info, all, average_cpu, average_memory, statistics, updates, licensing, connectivity, vsx`
Firewall	`fw`	`default, interfaces, policy, perf, hmem, kmem, inspect, cookies, chains, fragments, totals, totals64, ufp, http, ftp, telnet, rlogin, smtp, pop3, sync, log_connection, all`

Feature or Software Blade	Flag	Flavors
HTTPS Inspection	`https_inspection`	`default, hsm_status, all`
Identity Awareness	`identityServer`	`default, authentication, logins, ldap, components, adquery, idc, muh`
Application Control	`appi`	`default, subscription_status, update_status, RAD_status, top_last_hour, top_last_day, top_last_week, top_last_month`
URL Filtering	`urlf`	`default, subscription_status, update_status, RAD_status, top_last_hour, top_last_day, top_last_week, top_last_month`
IPS	`ips`	`default, statistics, all`
Anti-Virus	`ci`	`default`
Threat Prevention	`antimalware`	`default, scanned_hosts, scanned_mails, subscription_status, update_status, ab_prm_contracts, av_prm_contracts, ab_prm_contracts, av_prm_contracts`

Feature or Software Blade	Flag	Flavors
Threat Emulation	threat-emulation	default, general_statuses, update_status, scanned_files, malware_detected, scanned_on_cloud, malware_on_cloud, average_process_time, emulated_file_size, queue_size, peak_size, file_type_stat_file_scanned, file_type_stat_malware_detected, file_type_stat_cloud_scanned, file_type_stat_cloud_malware_scanned, file_type_stat_filter_by_analysis, file_type_stat_cache_hit_rate, file_type_stat_error_count, file_type_stat_no_resource_count, contract, downloads_information_current, downloading_file_information, queue_table, history_te_incidents, history_te_comp_hosts
Threat Extraction	scrub	default, subscription_status, threat_extraction_statistics
Mobile Access	cvpn	cvpnd, sysinfo, products, overall
VSX	vsx	default, stat, traffic, conns, cpu, all, memory, cpu_usage_per_core
IPSec VPN	vpn	default, product, IKE, ipsec, traffic, compression, accelerator, nic, statistics, watermarks, all
Data Loss Prevention	dlp	default, dlp, exchange_agents, fingerprint
Content Awareness	ctnt	default
QoS	fg	all
High Availability	ha	default, all
Policy Server for Remote Access VPN clients	polsrv	default, all

Feature or Software Blade	Flag	Flavors
Desktop Policy Server for Remote Access VPN clients	`dtps`	`default, all`
LTE / GX	`gx`	`default, contxt_create_info, contxt_delete_info, contxt_update_info, contxt_path_mng_info, GXSA_GPDU_info, contxt_initiate_info, gtpv2_create_info, gtpv2_delete_info, gtpv2_update_info, gtpv2_path_mng_info, gtpv2_cmd_info, all`
Management Server	`mg`	`default, log_server, indexer`
Certificate Authority	`ca`	`default, crl, cert, user, all`
SmartEvent	`cpsemd`	`default`
SmartEvent Correlation Unit	`cpsead`	`default`
Log Server	`ls`	`default`
CloudGuard Controller	`vsec`	`default`
SmartReporter	`svr`	`default`
Provisioning Agent	`PA`	`default`
Thresholds configured with the "`threshold_config`" command	`thresholds`	`default, active_thresholds, destinations, error`
Historical status values	`persistency`	`product, TableConfig, SourceConfig`

Examples

Example - Interfaces on a Security Gateway

```
[Expert@MyGW:0]# cpstat -f interfaces fw

Network interfaces
-------------------------------------------------------------------------------------------------
-----------------------
|Name|IP           |Netmask      |Flags|Peer name|Remote IP|Topology|Proxy
name|Slaves|Ports|IPv6 Address|IPv6 Len|
-------------------------------------------------------------------------------------------------
-----------------------
|eth0|192.168.30.40|255.255.255.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
|eth1| 172.30.60.80|255.255.255.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
|eth2|      0.0.0.0|      0.0.0.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
|eth3|      0.0.0.0|      0.0.0.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
|eth4|      0.0.0.0|      0.0.0.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
|eth5|      0.0.0.0|      0.0.0.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
|eth6|      0.0.0.0|      0.0.0.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
|eth7|      0.0.0.0|      0.0.0.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
-------------------------------------------------------------------------------------------------
-----------------------

[Expert@MyGW:0]#
```

Example - Policy on a Security Gateway

```
[Expert@MyGW:0]# cpstat -f default fw

Policy name:  MyGW_Policy
Install time: Wed May 23 18:14:32 2018


Interface table
----------------------------------------
|Name|Dir|Total   |Accept|Deny    |Log|
----------------------------------------
|eth0|in | 2393126| 32589| 2360537| 52|
|eth0|out|   33016| 33016|       0|  0|
|eth1|in | 2360350|     0| 2360350|  0|
|eth1|out|       0|     0|       0|  0|
|eth2|in | 2360350|     0| 2360350|  0|
|eth2|out|       0|     0|       0|  0|
|eth3|in | 2348704|     0| 2348704|  1|
|eth3|out|       0|     0|       0|  0|
|eth4|in | 2360350|     0| 2360350|  0|
|eth4|out|       0|     0|       0|  0|
----------------------------------------
|    |   |11855896| 65605|11790291| 53|
----------------------------------------

... ... [truncated for brevity] ... ...

[Expert@MyGW:0]#
```

Example - CPU utilization

```
[Expert@HostName:0]# cpstat -f cpu os
CPU User Time (%):   1
CPU System Time (%): 0
CPU Idle Time (%):   99
CPU Usage (%):       1
CPU Queue Length:    -
CPU Interrupts/Sec:  172
CPUs Number:         8

[Expert@HostName:0]#
```

Example - Performance

```
[Expert@HostName:0]# cpstat os -f perf -o 2 -c 2 -e 60

Total Virtual Memory (Bytes):            12417720320
Active Virtual Memory (Bytes):           3741331456
Total Real Memory (Bytes):               8231063552
Active Real Memory (Bytes):              3741331456
Free Real Memory (Bytes):                4489732096
Memory Swaps/Sec:                        -
Memory To Disk Transfers/Sec:            -
CPU User Time (%):                       0
CPU System Time (%):                     0
CPU Idle Time (%):                       100
CPU Usage (%):                           0
CPU Queue Length:                        -
CPU Interrupts/Sec:                      135
CPUs Number:                             8
Disk Servicing Read\Write Requests Time: -
Disk Requests Queue:                     -
Disk Free Space (%):                     61
Disk Total Free Space (Bytes):           12659716096
Disk Available Free Space (Bytes):       11606188032
Disk Total Space (Bytes):                20477751296


Total Virtual Memory (Bytes):            12417720320
Active Virtual Memory (Bytes):           3741556736
Total Real Memory (Bytes):               8231063552
Active Real Memory (Bytes):              3741556736
Free Real Memory (Bytes):                4489506816
Memory Swaps/Sec:                        -
Memory To Disk Transfers/Sec:            -
CPU User Time (%):                       3
CPU System Time (%):                     0
CPU Idle Time (%):                       97
CPU Usage (%):                           3
CPU Queue Length:                        -
CPU Interrupts/Sec:                      140
CPUs Number:                             8
Disk Servicing Read\Write Requests Time: -
Disk Requests Queue:                     -
Disk Free Space (%):                     61
Disk Total Free Space (Bytes):           12659716096
Disk Available Free Space (Bytes):       11606188032
Disk Total Space (Bytes):                20477751296

[Expert@HostName:0]#
```

Example - List of current connected sessions on a Management Server

```
[Expert@MGMT:0]# cpstat -f default mg

Product Name:  Check Point Security Management Server
Major version: 6
Minor version: 0
Build number:  994000031
Is started:    1
Active status: active
Status:        OK

Connected clients
-----------------------------------------------------
|Client type |Administrator|Host        |Database lock|
-----------------------------------------------------
|SmartConsole|admin        |JOHNDOE-PC  |false        |
-----------------------------------------------------

[Expert@MGMT:0]#
```

cpwd_admin

Description

The Check Point WatchDog (`cpwd`) is a process that invokes and monitors critical processes such as Check Point daemons on the local server, and attempts to restart them if they fail.

Among the processes monitored by Watchdog are `fwm`, `fwd`, `cpd`, `DAService`, and others.

The list of monitored processes depends on the installed and configured Check Point products and Software Blades.

The Check Point WatchDog writes monitoring information to the `$CPDIR/log/cpwd.elg` log file.

The `cpwd_admin` utility shows the status of the monitored processes, and configures the Check Point WatchDog.

There are two types of Check Point WatchDog monitoring

Monitoring	Description
Passive	WatchDog restarts the process only when the process terminates abnormally. In the output of the `cpwd_admin list` command, the `MON` column shows `N` for passively monitored processes.
Active	WatchDog checks the process status every predefined interval. WatchDog makes sure the process is alive, as well as properly functioning (not stuck on deadlocks, frozen, and so on). In the output of the `cpwd_admin list` command, the `MON` column shows `Y` for actively monitored processes. The list of actively monitored processes is predefined by Check Point. Users cannot change or configure it.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin
      config <options>
      del <options>
      detach <options>
      exist
      flist <options>
      getpid <options>
      kill
      list <options>
      monitor_list
      start <options>
      start_monitor
      stop <options>
      stop_monitor
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin
      config <options>
      del <options>
      detach <options>
      exist
      flist <options>
      getpid <options>
      kill
      list <options>
      monitor_list
      start <options>
      start_monitor
      stop <options>
      stop_monitor
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin
      config <options>
      del <options>
      detach <options>
      exist
      flist <options>
      getpid <options>
      kill
      list <options>
      monitor_list
      start <options>
      start_monitor
      stop <options>
      stop_monitor
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin
      config <options>
      del <options>
      detach <options>
      exist
      flist <options>
      getpid <options>
      kill
      list <options>
      monitor_list
      start <options>
      start_monitor
      stop <options>
      stop_monitor
```

Parameters

Parameter	Description
`config <options>`	Configures the Check Point WatchDog. See *"cpwd_admin config" on page 224*.

Parameter	Description
`del <options>`	Temporarily deletes a monitored process from the WatchDog database of monitored processes. See *"cpwd_admin del" on page 229*.
`detach <options>`	Temporarily detaches a monitored process from the WatchDog monitoring. See *"cpwd_admin detach" on page 231*.
`exist`	Checks whether the WatchDog process `cpwd` is alive. See *"cpwd_admin exist" on page 233*.
`flist <options>`	Saves the status of all monitored processes to a `$CPDIR/tmp/cpwd_list_<Epoch Timestamp>.lst` file. See *"cpwd_admin flist" on page 234*.
`getpid <options>`	Shows the PID of a monitored process. See *"cpwd_admin getpid" on page 236*.
`kill <options>`	Terminates the WatchDog process `cpwd`. See *"cpwd_admin kill" on page 237*. **Important** - Do **not** run this command unless explicitly instructed by Check Point Support or R&D to do so.
`list`	Prints the status of all monitored processes on the screen. See *"cpwd_admin list" on page 238*.
`monitor_list`	Prints the status of actively monitored processes on the screen. See *"cpwd_admin monitor_list" on page 243*.
`start <options>`	Starts a process as monitored by the WatchDog. See *"cpwd_admin start" on page 244*.
`start_monitor`	Starts the active WatchDog monitoring - WatchDog monitors the predefined processes actively. See *"cpwd_admin start_monitor" on page 247*.
`stop <options>`	Stops a monitored process. See *"cpwd_admin stop" on page 248*.
`stop_monitor`	Stops the active WatchDog monitoring - WatchDog monitors all processes only passively. See *"cpwd_admin stop_monitor" on page 250*.

cpwd_admin config

Description

Configures the Check Point WatchDog.

Important - After changing the WatchDog configuration parameters, you must restart the WatchDog process with the "`cpstop`" and "`cpstart`" commands (which restart *all* Check Point processes).

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin config
      -h
      -a <options>
      -d <options
      -p
      -r
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin config
      -h
      -a <options>
      -d <options
      -p
      -r
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin config
      -h
      -a <options>
      -d <options
      -p
      -r
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin config
      -h
      -a <options>
      -d <options
      -p
      -r
```

Parameters

Parameter	Description
`-h`	Shows built-in usage.
`-a <Configuration_Parameter_1>=<Value_1> <Configuration_Parameter_2>=<Value_2> ... <Configuration_Parameter_N>=<Value_N>`	Adds the WatchDog configuration parameters. **Note** - Spaces are not allowed between the name of the configuration parameter, the equal sign, and the value.
`-d <Configuration_Parameter_1> <Configuration_Parameter_2> ... <Configuration_Parameter_N>`	Deletes the WatchDog configuration parameters that user added with the "`cpwd_admin config -a`" command.
`-p`	Shows the WatchDog configuration parameters that user added with the "`cpwd_admin config -a`" command.
`-r`	Restores the default WatchDog configuration.

These are the available configuration parameters and the accepted values:

Configuration Parameter	Accepted Values	Description
`default_ctx`	Text string up to 128 characters	On a VSX Gateway, configures the CTX value that is assigned to monitored processes, for which no CTX is specified.
`display_ctx`	■ 0 (default) ■ 1	On a VSX Gateway, configures whether the WatchDog shows the `CTX` column in the output of the `cpwd_admin list` command (between the `APP` and the `PID` columns): ■ 0 - Does not show the `CTX` column ■ 1 - Shows the `CTX` column

Configuration Parameter	Accepted Values	Description
`no_limit`	■ Range: -1, 0, >0 ■ Default: 5	If `rerun_mode=1`, specifies the maximal number of times the WatchDog tries to restart a process. ■ -1 - Always tries to restart ■ 0 - Never tries to restart ■ >0 - Tries this number of times
`num_of_procs`	■ Range: 30 - 3000 ■ Default: 3000	Configures the maximal number of processes managed by the WatchDog.
`rerun_mode`	■ 0 ■ 1 (default)	Configures whether the WatchDog restarts processes after they fail: ■ 0 - Does not restart a failed process. Monitor and log only. ■ 1 - Restarts a failed process (this is the default).
`reset_ startups`	■ Range: > 0 ■ Default: 3600	Configures the time (in seconds) the WatchDog waits after the process starts and before the WatchDog resets the process's `startup_counter` to 0. To see the process's startup counter, in the output of the `cpwd_admin list` command, refer to the `#START` column.
`sleep_mode`	■ 0 ■ 1 (default)	Configures how the WatchDog restarts the process: ■ 0 - Ignores timeout and restarts the process immediately ■ 1 - Waits for the duration of `sleep_timeout`
`sleep_ timeout`	■ Range: 0 - 3600 ■ Default: 60	If `rerun_mode=1`, specifies how much time (in seconds) passes from a process failure until WatchDog tries to restart it.
`stop_timeout`	■ Range: > 0 ■ Default: 60	Configures the time (in seconds) the WatchDog waits for a process stop command to complete.

Configuration Parameter	Accepted Values	Description
`zero_timeout`	■ Range: > 0 ■ Default: 7200	After failing `no_limit` times to restart a process, the WatchDog waits `zero_timeout` seconds before it tries again. The value of the `zero_timeout` must be greater than the value of the `timeout`.

The WatchDog saves the user defined configuration parameters in the `$CPDIR/registry/HKLM_registry.data` file in the "`: (Wd_Config`" section:

```
("CheckPoint Repository Set"
  : (SOFTWARE
    : (CheckPoint
      : (CPshared
        :CurrentVersion (6.0)
        : (6.0
        ... ...
          : (reserved
          ... ...
            : (Wd
                : (Wd_Config
                    :Configuration_Parameter_1 ("[4]Value_1")
                    :Configuration_Parameter_2 ("[4]Value_2")
                )
            )
          ... ...
```

Example

```
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -a sleep_timeout=120 no_limit=12
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog Configuration parameters are:
sleep_timeout : 120
no_limit : 12
[Expert@HostName:0]#
[Expert@HostName:0]# cpstop ; cpstart
[Expert@HostName:0]#

[Expert@HostName:0]# cpwd_admin config -r
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
[Expert@HostName:0]# cpstop ; cpstart
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
```

cpwd_admin del

Description

Temporarily deletes a monitored process from the WatchDog database of monitored processes.

Notes:

- WatchDog stops monitoring the detached process, but the process stays alive.
- The *"cpwd_admin list" on page 238* command does not show the deleted process anymore.
- This change applies until all Check Point services restart during boot, or with the *"cpstart" on page 208* command.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin del -name <Application Name>
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin del -name <Application Name> [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin del -name <Application Name> [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin del -name <Application Name> [-ctx <VSID>]
```

Parameters

Parameter	Description
<Application Name>	Name of the monitored Check Point process as you see in the output of the *"cpwd_admin list" on page 238* command in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`
`-ctx <VSID>`	On a VSX Gateway, specifies the context of the applicable Virtual System.

Example

```
[Expert@HostName:0]# cpwd_admin del -name FWD
cpwd_admin:
successful Del operation
[Expert@HostName:0]#
```

cpwd_admin detach

Description

Temporarily detaches a monitored process from the WatchDog monitoring.

Notes:

- WatchDog stops monitoring the detached process, but the process stays alive.
- The *"cpwd_admin list" on page 238* command does not show the detached process anymore.
- This change applies until all Check Point services restart during boot, or with the *"cpstart" on page 208* command.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin detach -name <Application Name>
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin detach -name <Application Name> [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin detach -name <Application Name> [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin detach -name <Application Name> [-ctx <VSID>]
```

Parameters

Parameter	Description
<Application Name>	Name of the monitored Check Point process as you see in the output of the *"cpwd_admin list" on page 238* command in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`
`-ctx <VSID>`	On a VSX Gateway, specifies the context of the applicable Virtual System.

Example

```
[Expert@HostName:0]# cpwd_admin detach -name FWD
cpwd_admin:
successful Detach operation
[Expert@HostName:0]#
```

cpwd_admin exist

Description

Checks whether the WatchDog process `cpwd` is alive.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin exist
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin exist
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin exist
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin exist
```

Example

```
[Expert@HostName:0]# cpwd_admin exist
 cpwd_admin: cpWatchDog is running
[Expert@HostName:0]#
```

cpwd_admin flist

Description

Saves the status of all WatchDog monitored processes to a file.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin flist [-full]
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin flist [-full] [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin flist [-full] [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin flist [-full] [-ctx <VSID>]
```

Parameters

Parameter	Description
`-full`	Shows the verbose output.
`-ctx <VSID>`	On a VSX Gateway, specifies the context of the applicable Virtual System.

Output

Column	Description
APP	Shows the WatchDog name of the monitored process.
CTX	On a VSX Gateway, shows the VSID, in which the monitored process runs.
PID	Shows the PID of the monitored process.
STAT	Shows the status of the monitored process: ■ E - executing ■ T - terminated
#START	Shows how many times the WatchDog started the monitored process.
START_TIME	Shows the time when the WatchDog started the monitored process for the last time.
SLP/LIMIT	In verbose output, shows the values of the sleep_timeout and no_limit configuration parameters (see *"cpwd_admin config" on page 224*).
MON	Shows how the WatchDog monitors this process (see the explanation for the *"cpwd_admin" on page 220*): ■ Y - Active monitoring ■ N - Passive monitoring
COMMAND	Shows the command the WatchDog run to start this process.

Example

```
[Expert@HostName:0]# cpwd_admin flist
/opt/CPshrd-R81.20/tmp/cpwd_list_1564617600.lst
[Expert@HostName:0]#
```

cpwd_admin getpid

Description

Shows the PID of a WatchDog monitored process.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin getpid -name <Application Name>
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin getpid -name <Application Name> [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin getpid -name <Application Name> [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin getpid -name <Application Name> [-ctx <VSID>]
```

Parameters

Parameter	Description
<Application Name>	Name of the monitored Check Point process as you see in the output of the *"cpwd_admin list" on page 238* command in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`
`-ctx <VSID>`	On VSX Gateway, specifies the context of the applicable Virtual System.

Example

```
[Expert@HostName:0]# cpwd_admin getpid -name FWD
5640
[Expert@HostName:0]#
```

cpwd_admin kill

Description

Terminates the WatchDog process `cpwd`.

Important - Do **not** run this command unless explicitly instructed by Check Point Support or R&D to do so.
To restart the WatchDog process, you must restart all Check Point services with the *"cpstop" on page 219* and *"cpstart" on page 208* commands.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin kill
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin kill
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin kill
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin kill
```

cpwd_admin list

Description

Prints the status of all WatchDog monitored processes on the screen.

Note - By default, WatchDog monitors a maximum of 3000 processes.
To increase this threshold, use the command "`cpwd_admin config -a num_of_procs=<value>`".
See *"cpwd_admin config" on page 224*.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin list [-full]
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin list [-full] [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin list [-full] [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin list [-full] [-ctx <VSID>]
```

Parameters

Parameter	Description
`-full`	Shows the verbose output.
`-ctx <VSID>`	On a VSX Gateway, specifies the context of the applicable Virtual System.

Output

Column	Description
APP	Shows the WatchDog name of the monitored process.
CTX	On a VSX Gateway, shows the VSID, in which the monitored process runs.
PID	Shows the PID of the monitored process.
STAT	Shows the status of the monitored process: ■ E - executing ■ T - terminated
#START	Shows how many times the WatchDog started the monitored process.
START_TIME	Shows the time when the WatchDog started the monitored process for the last time.
SLP/LIMIT	In verbose output, shows the values of the sleep_timeout and no_limit configuration parameters (see *"cpwd_admin config" on page 224*).
MON	Shows how the WatchDog monitors this process (see the explanation for the *"cpwd_admin" on page 220*): ■ Y - Active monitoring ■ N - Passive monitoring
COMMAND	Shows the command the WatchDog run to start this process.

Examples

Example - Default output on a Management Server

```
[Expert@HostName:0]# cpwd_admin list
APP          PID    STAT  #START  START_TIME             MON  COMMAND
CPVIEWD      19738  E     1       [17:50:44] 31/5/2019   N    cpviewd
HISTORYD     0      T     0       [17:54:44] 31/5/2019   N    cpview_historyd
CPD          19730  E     1       [17:54:45] 31/5/2019   Y    cpd
SOLR         19935  E     1       [17:50:55] 31/5/2019   N    java_solr /opt/CPrt-
R81.20/conf/jetty.xml
RFL          19951  E     1       [17:50:55] 31/5/2019   N    LogCore
SMARTVIEW    19979  E     1       [17:50:55] 31/5/2019   N    SmartView
INDEXER      20032  E     1       [17:50:55] 31/5/2019   N    /opt/CPrt-R81.20/log_indexer/log_
indexer
SMARTLOG_SERVER 20100  E     1       [17:50:55] 31/5/2019   N    /opt/CPSmartLog-
R81.20/smartlog_server
CP3DLOGD     20237  E     1       [17:50:55] 31/5/2019   N    cp3dlogd
EPM          20251  E     1       [17:50:56] 31/5/2019   N    startEngine
DASERVICE    20404  E     1       [17:50:59] 31/5/2019   N    DAService_script
[Expert@HostName:0]#
```

Example - Default output on a Security Gateway

```
[Expert@HostName:0]# cpwd_admin list
APP         CTX         PID    STAT  #START  START_TIME             MON  COMMAND
FWK_FORKER  0           4180   E     1       [18:14:04] 23/5/2019   N    fwk_forker
FWK_WD      0           4182   E     1       [18:14:04] 23/5/2019   N    fwk_wd -i 1 -i6 0
CPSICDEMUX  0           5383   E     1       [18:14:14] 23/5/2019   N    cpsicdemux
CPVIEWD     0           5407   E     1       [18:14:15] 23/5/2019   N    cpviewd
HISTORYD    0           5410   E     1       [18:14:15] 23/5/2019   N    cpview_historyd
SXL_STATD   0           5413   E     1       [18:14:15] 23/5/2019   N    sxl_statd
CPD         0           5420   E     1       [18:14:15] 23/5/2019   Y    cpd
MPDAEMON    0           5436   E     1       [18:14:16] 23/5/2019   N    mpdaemon /opt/CPshrd-
R81.20/log/mpdaemon.elg /opt/CPshrd-R81.20/conf/mpdaemon.conf
CI_CLEANUP  0           5626   E     1       [18:14:26] 23/5/2019   N    avi_del_tmp_files
CIHS        0           5628   E     1       [18:14:26] 23/5/2019   N    ci_http_server -j -f
/opt/CPsuite-R81.20/fw1/conf/cihs.conf
FWD         0           5640   E     1       [18:14:26] 23/5/2019   N    fwd
RAD         0           6330   E     1       [18:14:28] 23/5/2019   N    rad
DASERVICE   0           8604   E     1       [18:14:43] 23/5/2019   N    DAService_script
[Expert@HostName:0]#
```

Example - Verbose output on a Management Server

```
[Expert@HostName:0]# cpwd_admin list -full
APP         PID    STAT  #START  START_TIME             SLP/LIMIT  MON
-------------------------------------------------------------------------------
CPVIEWD     19738  E     1       [17:50:44] 31/5/2019   60/5       N
            PATH = /opt/CPshrd-R81.20/bin/cpviewd
            COMMAND = cpviewd
-------------------------------------------------------------------------------
HISTORYD    0      T     0       [17:54:44] 31/5/2019   60/5       N
            PATH = /opt/CPshrd-R81.20/bin/cpview_historyd
            COMMAND = cpview_historyd
-------------------------------------------------------------------------------
CPD         19730  E     1       [17:54:45] 31/5/2019   60/5       Y
            PATH = /opt/CPshrd-R81.20/bin/cpd
            COMMAND = cpd
-------------------------------------------------------------------------------
SOLR        19935  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPrt-R81.20/bin/java_solr
            COMMAND = java_solr /opt/CPrt-R81.20/conf/jetty.xml
-------------------------------------------------------------------------------
RFL         19951  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPrt-R81.20/bin/LogCore
            COMMAND = LogCore
-------------------------------------------------------------------------------
SMARTVIEW   19979  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPrt-R81.20/bin/SmartView
            COMMAND = SmartView
-------------------------------------------------------------------------------
INDEXER     20032  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPrt-R81.20/log_indexer/log_indexer
            COMMAND = /opt/CPrt-R81.20/log_indexer/log_indexer
-------------------------------------------------------------------------------
SMARTLOG_SERVER 20100  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPSmartLog-R81.20/smartlog_server
            COMMAND = /opt/CPSmartLog-R81.20/smartlog_server
            ENV = LANG=C
-------------------------------------------------------------------------------
CP3DLOGD    20237  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPuepm-R81.20/bin/cp3dlogd
            COMMAND = cp3dlogd
-------------------------------------------------------------------------------
EPM         20251  E     1       [17:50:56] 31/5/2019   60/5       N
            PATH = /opt/CPuepm-R81.20/bin/startEngine
            COMMAND = startEngine
-------------------------------------------------------------------------------
DASERVICE   20404  E     1       [17:50:59] 31/5/2019   60/5       N
            PATH = /opt/CPda/bin/DAService_script
            COMMAND = DAService_script
[Expert@HostName:0]#
```

Example - Verbose output on a Security Gateway

```
[Expert@HostName:0]# cpwd_admin list -full
APP         CTX        PID    STAT  #START  START_TIME             SLP/LIMIT  MON
-------------------------------------------------------------------------------
FWK_FORKER 0           4180   E     1       [18:14:04] 23/5/2019   60/5       N
                       PATH = /opt/CPsuite-R81.20/fw1/bin/fwk_forker
                       COMMAND = fwk_forker
-------------------------------------------------------------------------------
FWK_WD     0           4182   E     1       [18:14:04] 23/5/2019   3/u        N
                       PATH = /opt/CPsuite-R81.20/fw1/bin/fwk_wd
                       COMMAND = fwk_wd -i 1 -i6 0
-------------------------------------------------------------------------------
CPSICDEMUX 0           5383   E     1       [18:14:14] 23/5/2019   60/5       N
                       PATH = /opt/CPshrd-R81.20/bin/cpsicdemux
                       COMMAND = cpsicdemux
-------------------------------------------------------------------------------
CPVIEWD    0           5407   E     1       [18:14:15] 23/5/2019   60/5       N
                       PATH = /opt/CPshrd-R81.20/bin/cpviewd
                       COMMAND = cpviewd
-------------------------------------------------------------------------------
HISTORYD   0           5410   E     1       [18:14:15] 23/5/2019   60/5       N
                       PATH = /opt/CPshrd-R81.20/bin/cpview_historyd
                       COMMAND = cpview_historyd
-------------------------------------------------------------------------------
SXL_STATD  0           5413   E     1       [18:14:15] 23/5/2019   60/5       N
                       PATH = /opt/CPsuite-R81.20/fw1/bin/sxl_statd
                       COMMAND = sxl_statd
-------------------------------------------------------------------------------
CPD        0           5420   E     1       [18:14:15] 23/5/2019   60/5       Y
                       PATH = /opt/CPshrd-R81.20/bin/cpd
                       COMMAND = cpd
-------------------------------------------------------------------------------
MPDAEMON   0           5436   E     1       [18:14:16] 23/5/2019   60/5       N
                       PATH = /opt/CPshrd-R81.20/bin/mpdaemon
                       COMMAND = mpdaemon /opt/CPshrd-R81.20/log/mpdaemon.elg /opt/CPshrd-
R81.20/conf/mpdaemon.conf
-------------------------------------------------------------------------------
CI_CLEANUP 0           5626   E     1       [18:14:26] 23/5/2019   60/5       N
                       PATH = /opt/CPsuite-R81.20/fw1/bin/avi_del_tmp_files
                       COMMAND = avi_del_tmp_files
-------------------------------------------------------------------------------
CIHS       0           5628   E     1       [18:14:26] 23/5/2019   60/5       N
                       PATH = /opt/CPsuite-R81.20/fw1/bin/ci_http_server
                       COMMAND = ci_http_server -j -f /opt/CPsuite-R81.20/fw1/conf/cihs.conf
-------------------------------------------------------------------------------
FWD        0           5640   E     1       [18:14:26] 23/5/2019   60/5       N
                       PATH = /opt/CPsuite-R81.20/fw1/bin/fw
                       COMMAND = fwd
-------------------------------------------------------------------------------
RAD        0           6330   E     1       [18:14:28] 23/5/2019   60/5       N
                       PATH = /opt/CPsuite-R81.20/fw1///bin/rad
                       COMMAND = rad
-------------------------------------------------------------------------------
DASERVICE  0           8604   E     1       [18:14:43] 23/5/2019   60/5       N
                       PATH = /opt/CPda/bin/DAService_script
                       COMMAND = DAService_script
[Expert@HostName:0]#
```

cpwd_admin monitor_list

Description

Prints the status of actively monitored processes on the screen.

See the explanation about the active monitoring in *"cpwd_admin" on page 220*.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin monitor_list
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin monitor_list
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin monitor_list
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin monitor_list
```

Example

```
[Expert@HostName:0]# cpwd_admin monitor_list
cpwd_admin:
APP        FILE_NAME                      NO_MSG_TIMES   LAST_MSG_TIME
CPD        CPD_5420_4714.mntr             0/10           [19:00:33] 31/5/2019
[Expert@HostName:0]#
```

cpwd_admin start

Description

Starts a process as monitored by the WatchDog.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin start -name <Application Name> -path "<Full Path to
Executable>" -command "<Command Syntax>" [-env {inherit | <Env_
Var>=<Value>] [-slp_timeout <Timeout>] [-retry_limit {<Limit> |
u}]
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin start -name <Application Name> [-ctx <VSID>] -path
"<Full Path to Executable>" -command "<Command Syntax>" [-env
{inherit | <Env_Var>=<Value>] [-slp_timeout <Timeout>] [-retry_
limit {<Limit> | u}]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin start -name <Application Name> [-ctx <VSID>] -path
"<Full Path to Executable>" -command "<Command Syntax>" [-env
{inherit | <Env_Var>=<Value>] [-slp_timeout <Timeout>] [-retry_
limit {<Limit> | u}]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin start -name <Application Name> [-ctx <VSID>] -
path "<Full Path to Executable>" -command "<Command Syntax>" [-env
{inherit | <Env_Var>=<Value>] [-slp_timeout <Timeout>] [-retry_
limit {<Limit> | u}]
```

Parameters

Parameter	Description
`-name <Application Name>`	Name, under which the `cpwd_admin list` command shows the monitored process in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`
`-ctx <VSID>`	On a VSX Gateway, specifies the context of the applicable Virtual System.
`-path "<Full Path to Executable>"`	The full path (with or without Check Point environment variables) to the executable including the executable name. Must enclose in double quotes. Examples: ■ For FWM: "`$FWDIR/bin/fwm`" ■ For FWD: "`/opt/CPsuite-R81.20/fw1/bin/fw`" ■ For CPD: "`$CPDIR/bin/cpd`" ■ For CPM: "`/opt/CPsuite-R81.20/fw1/scripts/cpm.sh`" ■ For SICTUNNEL: "`/opt/CPshrd-R81.20/bin/cptnl`"
`-command "<Command Syntax>"`	The command and its arguments to run. Must enclose in double quotes. Examples: ■ For FWM: "`fwm`" ■ For FWM on Multi-Domain Server: "`fwm mds`" ■ For FWD: "`fwd`" ■ For CPD: "`cpd`" ■ For CPM: "`/opt/CPsuite-R81.20/fw1/scripts/cpm.sh -s`" ■ For SICTUNNEL: "`/opt/CPshrd-R81.20/bin/cptnl -c "/opt/CPuepm-R81.20/engine/conf/cptnl_srv.conf"`"

Parameter	Description
`-env {inherit | <Env_ Var>=<Value>}`	Configures whether to inherit the environment variables from the shell. ■ `inherit` - Inherits all the environment variables (WatchDog supports up to 80 environment variables) ■ *<Env_Var>=<Value>* - Assigns the specified value to the specified environment variable
`-slp_timeout <Timeout>`	Configures the specified value of the "`sleep_timeout`" configuration parameter. See *"cpwd_admin config" on page 224*.
`-retry_limit {<Limit> | u}`	Configures the value of the "`retry_limit`" configuration parameter. See *"cpwd_admin config" on page 224*. ■ *<Limit>* - Tries to restart the process the specified number of times ■ `u` - Tries to restart the process unlimited number of times

Example

For the list of process and the applicable syntax, see sk97638.

cpwd_admin start_monitor

Description

Starts the active WatchDog monitoring. WatchDog monitors the predefined processes actively.

See the explanation for the *"cpwd_admin" on page 220* command.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin start_monitor
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin start_monitor
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin start_monitor
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin start_monitor
```

Example

```
[Expert@HostName:0]# cpwd_admin start_monitor
cpwd_admin:
CPWD has started to perform active monitoring on Check Point services/processes
[Expert@HostName:0]#
```

cpwd_admin stop

Description

Stops a WatchDog monitored process.

Important - This change does **not** survive reboot.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin stop -name <Application Name> [-path "<Full Path to
Executable>" -command "<Command Syntax>" [-env {inherit | <Env_
Var>=<Value>]
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin stop -name <Application Name> [-ctx <VSID>] [-path
"<Full Path to Executable>" -command "<Command Syntax>" [-env
{inherit | <Env_Var>=<Value>]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin stop -name <Application Name> [-ctx <VSID>] [-path
"<Full Path to Executable>" -command "<Command Syntax>" [-env
{inherit | <Env_Var>=<Value>]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin stop -name <Application Name> [-ctx <VSID>] [-
path "<Full Path to Executable>" -command "<Command Syntax>" [-env
{inherit | <Env_Var>=<Value>]
```

Parameters

Parameter	Description
`-name <Application Name>`	Name under which the `cpwd_admin list` command shows the monitored process in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`
`-ctx <VSID>`	On a VSX Gateway, specifies the context of the applicable Virtual System.
`-path "<Full Path to Executable>"`	The full path (with or without Check Point environment variables) to the executable including the executable name. Must enclose in double quotes. Examples: ■ For FWM: "`$FWDIR/bin/fwm`" ■ For FWD: "`/opt/CPsuite-R81.20/fw1/bin/fw`" ■ For CPD: "`$CPDIR/bin/cpd_admin`"
`-command "<Command Syntax>"`	The command and its arguments to run. Must enclose in double quotes. Examples: ■ For FWM: "`fw kill fwm`" ■ For FWD: "`fw kill fwd`" ■ For CPD: "`cpd_admin stop`"
`-env {inherit | <Env_Var>=<Value>}`	Configures whether to inherit the environment variables from the shell. ■ `inherit` - Inherits all the environment variables (WatchDog supports up to 80 environment variables) ■ `<Env_Var>=<Value>` - Assigns the specified value to the specified environment variable

Example

For the list of process and the applicable syntax, see sk97638.

cpwd_admin stop_monitor

Description

Stops the active WatchDog monitoring. WatchDog monitors all processes only passively.

See the explanation for the *"cpwd_admin" on page 220* command.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin stop_monitor
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin stop_monitor
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin stop_monitor
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin stop_monitor
```

Example

```
[Expert@HostName:0]# cpwd_admin stop_monitor
cpwd_admin:
CPWD has stopped performing active monitoring on Check Point services/processes
[Expert@HostName:0]#
```

dbedit

Description

Edits the management database - the `$FWDIR/conf/objects_5_0.C` file - on the Security Management Server or Domain Management Server. See sk13301.

Important - Do NOT run this command, unless explicitly instructed by Check Point Support or R&D to do so. Otherwise, you can corrupt settings in the management database.

Syntax

```
dbedit -help
```

```
dbedit [-globallock] [{-local | -s <Management_Server>}] [{-u
<Username> | -c <Certificate>}] [-p <Password>] [-f <File_Name>
[ignore_script_failure] [-continue_updating]] [-r "<Open_Reason_
Text>"] [-d <Database_Name>] [-listen] [-readonly] [-session]
```

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Parameters

Parameter	Description
`-help`	Prints the general help.
`-globallock`	When you work with the dbedit utility, it partially locks the management database. If a user configures objects in SmartConsole at the same time, it causes problems in the management database. This option does not let SmartConsole, or a dbedit user to make changes in the management database. When you specify this option, the dbedit commands run on a copy of the management database. After you make the changes with the `dbedit` commands and run the `savedb` command, the dbedit utility saves and commits your changes to the actual management database.
`-local`	Connects to the localhost (127.0.0.1) without using username/password. If you do not specify this parameter, the dbedit utility asks how to connect.

Parameter	Description
`-s <Management_Server>`	Specifies the Security Management Server - by IP address or HostName. If you do not specify this parameter, the dbedit utility asks how to connect.
`-u <Username>`	Specifies the username, with which the dbedit utility connects to the Security Management Server. Mandatory parameter when you specify the "`-s <Management_Server>`" parameter.
`-c <Certificate>`	Specifies the user's certificate file, with which the dbedit utility connects to the Security Management Server. Mandatory parameter when you specify the "`-s <Management_Server>`" parameter.
`-p <Password>`	Specifies the user's password, with which the dbedit utility connects to the Security Management Server. Mandatory parameter when you specify the "`-s <Management_Server>`" and "`-u <Username>`" parameters.
`-f <File_Name>`	Specifies the file that contains the applicable dbedit internal commands (see the section "*dbedit Internal Commands*" below): ■ `create <object_type> <object_name>` ■ `modify <table_name> <object_name> <field_name> <value>` ■ `update <table_name> <object_name>` ■ `delete <table_name> <object_name>` ■ `print <table_name> <object_name>` ■ `quit` **Note** - Each command is limited to 4096 characters.
`ignore_script_failure`	Continues to execute the dbedit internal commands in the file and ignores errors. You can use it when you specify the "`-f <File_Name>`" parameter.
`-continue_updating`	Continues to update the modified objects, even if the operation fails for some of the objects (ignores the errors and runs the `update_all` command at the end of the script). You can use it when you specify the "`-f <File_Name>`" parameter.
`-r "<Open_Reason_Text>"`	Specifies the reason for opening the database in read-write mode (default mode).

Parameter	Description
`-d <Database_Name>`	Specifies the name of the database, to which the dbedit utility should connect (for example, `mdsdb`).
`-listen`	The dbedit utility "listens" for changes (use this mode for advanced troubleshooting with the assistance of Check Point Support). The dbedit utility prints its internal messages when a change occurs in the management database.
`-readonly`	Specifies to open the management database in read-only mode.
`-session`	Session Connectivity.

`dbedit` Internal Commands

Note - To see the available tables, class names (object types), attributes and values, connect to Management Server with Database Tool (GuiDBEdit Tool) (see sk13009).

Command	Description, Syntax, Examples
`-h`	**Description:** Prints the general help. **Syntax:** `dbedit> -h`

`-q`
 	
`quit`
	Description:
	Quits from dbedit.
	Syntax:
	`dbedit> -q`
	`dbedit> quit [-update_all | -noupdate]`
	Examples:
	■ Exit the utility and commit the remaining modified objects (interactive mode):
	`dbedit> quit`
	■ Exit the utility and update all the remaining modified objects:
	`dbedit> quit -update_all`
	■ Exit the utility and discard all modifications:
	`dbedit> quit -no_update`

Command	Description, Syntax, Examples

`update`	**Description:**
	Saves the specified object in the specified table (for example, "`network_objects`", "`services`", "`users`").
	Syntax:
	`dbedit> update <table_name> <object_name>`
	Example:
	Save the object *My_Service* in the table *services*:
	`dbedit> update services My_Service`

`update_all`	**Description:** Saves all the modified objects. **Syntax:** `dbedit> update_all`

`_print_set`	**Description:**
	Prints the specified object from the specified table (for example, "`network_objects`", "`services`", "`users`") as it appears in the `$FWDIR/conf/objects_5_0.C` file (sets of attributes).
	Syntax:
	`dbedit> _print_set <table_name> <object_name>`
	Example:
	Print the object *My_Obj* from the table *network_objects*:
	`dbedit> print network_objects My_Obj`

`print`	**Description:**
	Prints the list of attributes of the specified object from the specified table (for example, "`network_objects`", "`properties`", "`services`", "`users`").
	Syntax:
	`dbedit> print <table_name> <object_name>`
	Examples:
	■ Print the object *My_Obj* from the table *network_objects* (in "Network Objects"):
	`dbedit> print network_objects my_obj`
	■ Print the object *firewall_properties* from the table *properties* (in "Global Properties"):
	`dbedit> print properties firewall_properties`

Command	Description, Syntax, Examples

`printxml`	**Description:**
	Prints in XML format the list of attributes of the specified object from the specified table (for example, "`network_objects`", "`properties`", "`services`", "`users`").
	You can export the settings from a Management Server to an XML file that you can use later with external automation systems.
	Syntax:
	`dbedit> printxml <table_name> [<object_name>]`
	Examples:
	■ Print the object *My_Obj* from the table *network_objects*:
	`dbedit> printxml network_objects my_obj`
	■ Print the object *firewall_properties* from the table *properties* (in "Global Properties"):
	`dbedit> printxml properties firewall_ properties`

`printbyuid`	**Description:**
	Prints the attributes of the object specified by its UID (appears in the `$FWDIR/conf/objects_5_0.C` file at the beginning of the object as "`chkpf_uid ({...})`").
	Syntax:
	`dbedit> printbyuid {object_id}`
	Example:
	Print the attributes of the object with the specified UID:
	`dbedit> printbyuid {D3833F1D-0A58-AA42-865F-39BFE3C126F1}`

Command	Description, Syntax, Examples

`query`	**Description:**
	Prints all the objects in the specified table.
	Optionally, you can query for objects with specific attribute and value - query is separated by a comma after "`query <table_name>`" (spaces are not allowed between the `<attribute>` and `'<value>'`).
	Syntax:
	`dbedit> query <table_name> [ , <attribute>='<value>' ]`
	Examples:
	■ Print all objects in the table *users*:
	`dbedit> query users`
	■ Print all objects in the table *network_objects* that are defined as Management Servers:
	`dbedit> query network_objects, management='true'`
	■ Print all objects in the table *services* with the name *ssh*:
	`command_sdbedit> query services, name='ssh'`
	■ Print all objects in the table *services* with the port *22*:
	`dbedit> query services, port='22'`
	■ Print all objects with the IP address *10.10.10.10*:
	`dbedit> query network_objects, ipaddr='10.10.10.10'`

`whereused`	**Description:**
	Checks where the specified object used in the database.
	Prints the number of places, where this object is used and relevant information about each such place.
	Syntax:
	`dbedit> whereused <table_name> <object_name>`
	Example:
	Check where the object *My_Obj* is used:
	`dbedit> whereused network_objects My_Obj`

Command	Description, Syntax, Examples

`create`	**Description:**
	Creates an object of specified type (with its default values) in the database.
	Restrictions apply to the object's name:
	■ Object names can have a maximum of 100 characters.
	■ Objects names can contain only ASCII letters, numbers, and dashes.
	■ Reserved words will be blocked by the Management Server (refer to sk40179).
	Syntax:
	`dbedit> create <object_type> <object_name>`
	Example:
	Create the service object *My_Service* of the type *tcp_service* (with its default values):
	`dbedit> create tcp_service my_service`

`delete`	**Description:**
	Deletes an object from the specified table.
	Syntax:
	`dbedit> delete <table_name> <object_name>`
	Example:
	Delete the service object *My_Service* from the table *services*:
	`dbedit> delete services my_service`

Command	Description, Syntax, Examples

`modify`	**Description:**
	Modifies the value of specified attribute in the specified object in the specified table (for example, "`network_objects`", "`services`", "`users`") in the management database.
	Syntax:
	`dbedit> modify <table_name> <object_name> <field_name> <value>`
	Examples:
	■ Modify the color to *red* in the object *My_Service* in the table *services*:
	`dbedit> modify services My_Service color red`
	■ Add a comment to the object *MyObj*:
	`dbedit> modify network_objects MyObj comments "Created by fwadmin with dbedit"`
	■ Set the value of the global property *ike_use_largest_possible_subnets* in the table *properties* to *false*:
	`dbedit> modify properties firewall_properties ike_use_largest_possible_subnets false`
	■ Create a new interface on the Security Gateway *My_FW* and modify its attributes - set the IP address / Mask and enable Anti-Spoofing on interface with *"Element Index"=3* (check the attributes of the object *My_FW* in Database Tool (GuiDBEdit Tool) (see sk13009)):

Command	Description, Syntax, Examples

```
dbedit> addelement network_objects My_FW
interfaces interface
dbedit> modify network_objects My_FW
interfaces:3:officialname NAME_OF_INTERFACE
dbedit> modify network_objects My_FW
interfaces:3:ipaddr IP_ADDRESS
dbedit> modify network_objects My_FW
interfaces:3:netmask NETWORK_MASK
dbedit> modify network_objects My_FW
interfaces:3:security:netaccess:access
specific
dbedit> modify network_objects My_FW
interfaces:3:security:netaccess:allowed
network_objects:group_name
dbedit> modify network_objects My_FW
interfaces:3:security:netaccess:perform_anti_
spoofing true
dbedit> modify network_objects MyObj FieldA
LINKSYS
```

- In the Owned Object *MyObj* change the value of *FieldB* to *NewVal*:

```
dbedit> modify network_objects MyObj
FieldA:FieldB NewVal
```

- In the Linked Object *MyObj* change the value of *FieldA* from *B* to *C*:

```
dbedit> modify network_objects MyObj FieldA
B:C
```

Command	Description, Syntax, Examples

`lock`	**Description:**
	Locks the specified object (by administrator) in the specified table (for example, "`network_objects`", "`services`", "`users`") from being modified by other users.
	For example, if you connect from a remote server to this Management Server with *admin1* and lock an object, you are be able to connect with *admin2*, but are not able to modify the locked object, until *admin1* releases the lock.
	Syntax:
	`dbedit> lock <table_name> <object_name>`
	Example:
	Lock the object *My_Service_Obj* in the table *services* in the database:
	`dbedit> lock services My_Service_Obj`

`addelement`	**Description:**
	Adds a specified multiple field / container (with specified value) to a specified object in specified table.
	Syntax:
	`dbedit> addelement <table_name> <object_name> <field_name> <value>`
	Examples:
	■ Add the element *BranchObjectClass* with the value *Organization* to a multiple field *Read* in the object *My_Obj* in the table *ldap*:
	`dbedit> addelement ldap My_Obj Read:BranchObjectClass Organization`
	■ Add the service *MyService* to the group of services *MyServicesGroup* in the table *services*:
	`dbedit> addelement services MyServicesGroup '' services:MyService`
	■ Add the network *MyNetwork* to the group of networks *MyNetworksGroup* in the table *network_objects*:
	`dbedit> addelement network_objects MyNetworksGroup '' network_objects:MyNetwork`

Command	Description, Syntax, Examples

`rmelement`	**Description:**
	Removes a specified multiple field / container (with specified value) from a specified object in specified table.
	Syntax:
	`dbedit> rmelement <table_name> <object_name> <field_name> <value>`
	Examples:
	■ Remove the service *MyService* from the group of services *MyServicesGroup* from the table *services*:
	`dbedit> rmelement services MyServicesGroup '' services:MyService`
	■ Remove the network *MyNetwork* from the group of networks *MyNetworksGroup* from the table *network_objects*:
	`dbedit> rmelement network_objects MyNetworksGroup '' network_objects:MyNetwork`
	■ Remove the element *BranchObjectClass* with the value *Organization* from the multiple field *Read* in the object *My_Obj* in the table *ldap*:
	`dbedit> rmelement ldap my_obj Read:BranchObjectClass Organization`

`rename`	**Description:**
	Renames the specified object in specified table.
	Syntax:
	`dbedit> rename <table_name> <object_name> <new_object_name>`
	Example:
	Rename the network object *london* to *chicago* in the table *network_objects*:
	`dbedit> rename network_objects london chicago`

Command	Description, Syntax, Examples

`rmbyindex`	**Description:**
	Removes an element from a container by element's index.
	Syntax:
	`dbedit> rmbyindex <table_name> <object_name> <field_name> <index_number>`
	Example:
	Remove the element *backup_log_servers* from the container *log_servers* by element index *1* in the table *network_objects*:
	`dbedit> rmbyindex network_objects g log_servers:backup_log_servers 1`

`add_owned_remove_name`	**Description:**
	Adds an owned object (and removes its name) to a specified owned object field (or container).
	Syntax:
	`dbedit> add_owned_remove_name <table_name> <object_name> <field_name> <value>`
	Example:
	Add the owned object *My_Gateway* (and remove its name) to the owned object field (or container) *my_external_products*:
	`dbedit> add_owned_remove_name network_objects My_Gateway additional_products owned:my_external_products`

`is_delete_allowed`	**Description:**
	Checks if the specified object can be deleted from the specified table (object cannot be deleted if it is used by other objects).
	Syntax:
	`dbedit> is_delete_allowed <table_name> <object_name>`
	Example:
	`dbedit> is_delete_allowed network_objects MyObj`
	Check if the object *MyObj* can be deleted from the table *network_objects*:

Command	Description, Syntax, Examples

`set_pass`	**Description:**
	Sets specified password for specified user.
	Notes:
	■ The password must contain at least 4 characters and no more than 50 characters.
	■ This command cannot change the administrator's password.
	Syntax:
	`dbedit> set_pass <Username> <Password>`
	Example:
	Set the password *1234* for the user *abcd*:
	`dbedit> set_pass abcd 1234`

`savedb`	**Description:** Saves the database. You can run this command only when the database is locked globally (when you start the dbedit utility with the "`dbedit -globallock`" command). **Syntax:** `dbedit> savedb`
`savesession`	**Description:** Saves the session. You can run this command only when you start the dbedit utility in session mode (with the "`dbedit -session`" command). **Syntax:** `dbedit> savesession`

evstart

Description

On a Multi-Domain Security Management Server, this command:

- Starts the SmartEvent Server and the SmartEvent Correlation Unit services, if you stopped them with the "`evstop`" command (see *"evstop" on page 631*).
- Starts only the SmartEvent Correlation Unit service, if you stopped it with the "`evstop`" command (see *"evstop" on page 631*).
- Can apply only to the **MDS** context.
- Can apply only to the specified Domain Management Server with the enabled SmartEvent Server and SmartEvent Correlation Unit Software Blades.

On a Multi-Domain Log Server, this command:

- Starts the SmartEvent Server and the SmartEvent Correlation Unit services, if you stopped them with the "`evstop`" command (see *"evstop" on page 631*).
- Starts only the SmartEvent Correlation Unit service, if you stopped it with the "`evstop`" command (see *"evstop" on page 631*).
- Can apply only to the **MDS** context.
- Can apply only to the specified Domain Log Server with the enabled SmartEvent Server and SmartEvent Correlation Unit Software Blades.

Important:

- You can run this command only in the Expert mode.
- Multi-Domain Security Management Server / Multi-Domain Log Server runs this command automatically:
  - During boot.
  - When you run the "`mdsstart`" command (see *"mdsstart" on page 770*).
- Domain Management Server / Domain Log Server runs this command automatically when you run the "`mdsstart_customer`" command (see *"mdsstart_customer" on page 774*).

Related command

"evstop" on page 631

Syntax

```
evstart [-analyzer]
      -m
      <IP Address or Name of Domain Management Server / Domain Log
Server>
```

Parameters

Parameter	Description
No Parameters	Starts the SmartEvent Server and the SmartEvent Correlation Unit services.
`-analyzer`	Starts only the SmartEvent Correlation Unit service.
`-m`	Starts the service(s) only in the **MDS** context.
<IP Address or Name>	Starts the service(s) only in the context of the specified Domain Management Server / Domain Log Server. If you first go to this context with the "`mdsenv <IP Address or Name>`" command (see *"mdsenv" on page 766*), then you do not have to specify the IP Address or Name in the "`evstart`" syntax.

evstop

Description

On a Multi-Domain Security Management Server, this command:

- Stops the SmartEvent Server and the SmartEvent Correlation Unit services.
- Stops only the SmartEvent Correlation Unit service.
- Can apply only to the **MDS** context.
- Can apply only to the specified Domain Management Server with the enabled SmartEvent Server and SmartEvent Correlation Unit Software Blades.

On a Multi-Domain Log Server, this command:

- Stops the SmartEvent Server and the SmartEvent Correlation Unit services.
- Stops only the SmartEvent Correlation Unit service.
- Can apply only to the **MDS** context.
- Can apply only to the specified Domain Log Server with the enabled SmartEvent Server and SmartEvent Correlation Unit Software Blades.

Important:

- You can run this command only in the Expert mode.
- Multi-Domain Security Management Server / Multi-Domain Log Server runs this command automatically:
  - When you run the "`mdsstop`" command (see *"mdsstop" on page 777*).
  - During reboot or shutdown.
- Domain Management Server / Domain Log Server runs this command automatically when you run the "`mdsstop_customer`" command (see *"mdsstop_customer" on page 781*).

Related command

"evstart" on page 629

Syntax

```
evstop [-analyzer]
      -m
      <IP Address or Name of Domain Management Server / Domain Log
Server>
```

Parameters

Parameter	Description
No Parameters	Stops the SmartEvent Server and the SmartEvent Correlation Unit services.
`-analyzer`	Stops only the SmartEvent Correlation Unit service.
`-m`	Stops the service(s) only in the **MDS** context.
<IP Address or Name>	Stops the service(s) only in the context of the specified Domain Management Server / Domain Log Server. If you first go to this context with the "`mdsenv <IP Address or Name>`" command (see *"mdsenv" on page 766*), then you do not have to specify the IP Address or Name in the "`evstop`" syntax.

fw

Description

- Performs various operations on Security or Audit log files.
- Kills the specified Check Point processes.
- Manages the Suspicious Activity Monitoring (SAM) rules.
- Manages the Suspicious Activity Policy editor.

Syntax

```
fw [-d]
      fetchlogs <options>
      hastat <options>
      kill <options>
      log <options>
      logswitch <options>
      lslogs <options>
      mergefiles <options>
      repairlog <options>
      sam <options>
      sam_policy <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`fetchlogs <options>`	Fetches the specified Check Point log files - Security (`$FWDIR/log/*.log*`) or Audit (`$FWDIR/log/*.adtlog*`), from the specified Check Point server. See *"fw fetchlogs" on page 268*.
`hastat <options>`	Shows information about Check Point servers in High Availability configuration and their states. See *"fw hastat" on page 272*.

Parameter	Description
`kill` *<options>*	Kills the specified Check Point process. See *"fw kill" on page 273*.
`log` *<options>*	Shows the content of Check Point log files - Security (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`). See *"fw log" on page 274*.
`logswitch` *<options>*	Switches the current active Check Point log file - Security (`$FWDIR/log/fw.log`) or Audit (`$FWDIR/log/fw.adtlog`). See *"fw logswitch" on page 284*.
`lslogs` *<options>*	Shows a list of Check Point log files - Security (`$FWDIR/log/*.log*`) or Audit (`$FWDIR/log/*.adtlog*`), located on the local server or a remote server. See *"fw lslogs" on page 288*.
`mergefiles` *<options>*	Merges several Check Point log files - Security (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`), into a single log file. See *"fw mergefiles" on page 291*.
`repairlog` *<options>*	Rebuilds pointer files for Check Point log files - Security (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`). See *"fw repairlog" on page 294*.
`sam` *<options>*	Manages the Suspicious Activity Monitoring (SAM) rules. See *"fw sam" on page 295*.
`sam_policy` *<options>* or `samp` *<options>*	Manages the Suspicious Activity Policy editor that works with these type of rules: ■ Suspicious Activity Monitoring (SAM) rules. ■ Rate Limiting rules. See *"fw sam_policy" on page 303*.

fw fetchlogs

Description

Fetches the specified Security log files (`$FWDIR/log/*.log*`) or Audit log files (`$FWDIR/log/*.adtlog*`) from the specified Check Point server.

Important - You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).

Syntax

```
fw [-d] fetchlogs [-f <Name of Log File 1>] [-f <Name of Log File 2>]... [-f <Name of Log File N>] <Target>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-f <Name of Log File N>`	Specifies the name of the log file to fetch. Need to specify name only. **Notes:** ■ If you do not specify the log file name explicitly, the command transfers all Security log files (`$FWDIR/log/*.log*`) and all Audit log files (`$FWDIR/log/*.adtlog*`). ■ The specified log file name can include wildcards * and ? (for example, `2017-0?-*.log`). If you enter a wildcard, you must enclose it in double quotes or single quotes. ■ You can specify multiple log files in one command. You must use the `-f` parameter for each log file name pattern. ■ This command also transfers the applicable log pointer files.
`<Target>`	Specifies the remote Check Point server, with which this local Check Point server has established SIC trust. **Notes:** ■ The local and the remote servers must have established SIC trust. ■ The local server can be a Security Management Server, a Log Server, a Cluster Member. ■ The remote server can be a Security Gateway, a Cluster Member, a Log Server, or a Security Management Server in High Availability deployment. ■ You can specify the remote managed server by its main IP address or Object Name as configured in SmartConsole.

Notes:

- This command moves the specified log files from the `$FWDIR/log/` directory on the specified Check Point server.

  Meaning, it deletes the specified log files on the specified Check Point server after it copies them successfully.

- This command moves the specified log files to the `$FWDIR/log/` directory on the local Check Point server, on which you run this command.

- This command cannot fetch the *active* log files `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`.

  To fetch these active log files:

  1. Perform the log switch on the applicable Check Point server:

     See *"fw logswitch" on page 284*.

     ```
     fw logswitch [-audit] [-h <IP Address or Hostname>]
     ```

  2. Fetch the rotated log file from the applicable Check Point server:

     ```
     fw fetchlogs -f <Log File Name> <IP Address or Hostname>
     ```

- This command renames the log files it fetched from the specified Check Point server.

  The new log file name is the concatenation of these:

  - The Check Point server's name (as configured in SmartConsole).
  - Two underscore (_) characters.
  - The original log file name

  Example: `MyGW__2019-06-01_000000.log`

Example - Fetching log files from a Management Server

```
[Expert@HostName:0]# fw lslogs MyGW
     Size Log file name
        23KB 2019-05-16_000000.log
         9KB 2019-05-17_000000.log
        11KB 2019-05-18_000000.log
      5796KB 2019-06-01_000000.log
      4610KB fw.log
[Expert@HostName:0]#

[Expert@HostName:0]# fw fetchlogs -f 2019-06-01_000000 MyGW
File fetching in process. It may take some time...
File MyGW__2019-06-01_000000.log was fetched successfully
[Expert@HostName:0]#

[Expert@HostName:0]# ls $FWDIR/log/MyGW*
/opt/CPsuite-R81.20/fw1/log/MyGW__2019-06-01_000000.log
/opt/CPsuite-R81.20/fw1/log/MyGW__2019-06-01_000000.logaccount_ptr
/opt/CPsuite-R81.20/fw1/log/MyGW__2019-06-01_000000.loginitial_ptr
/opt/CPsuite-R81.20/fw1/log/MyGW__2019-06-01_000000.logptr
[Expert@HostName:0]#

[Expert@HostName:0]# fw lslogs MyGW
     Size Log file name
        23KB 2019-05-16_000000.log
         9KB 2019-05-17_000000.log
        11KB 2019-05-18_000000.log
      4610KB fw.log
[Expert@HostName:0]#
```

fw hastat

Description

Shows information about Check Point computers in High Availability configuration and their states.

Note - This command is outdated. On cluster members, run the Gaia Clish command "`show cluster state`", or the Expert mode command "`cphaprob state`".

Note - This command is outdated. On Management Servers, run the *"cpstat" on page 209* command.

Syntax

```
fw hastat [<Target1>] [<Target2>] ... [<TargetN>]
```

Parameters

Parameter	Description
<Target1> *<Target2>* ... *<TargetN>*	Specifies the Check Point computers to query. If you run this command on the Management Server, you can enter the applicable IP address, or the resolvable HostName of the managed Security Gateway or Cluster Member. If you do not specify the target, the command queries the local computer.

Example - Querying the cluster members from the Management Server

```
[Expert@MGMT:0]# fw hastat 192.168.3.52
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.52 1 active OK
[Expert@MGMT:0]#

[Expert@MGMT:0]# fw hastat 192.168.3.53
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.53 2 stand-by OK
[Expert@MGMT:0]#

[Expert@MGMT:0]# fw hastat 192.168.3.52 192.168.3.53
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.52 1 active OK
192.168.3.53 2 stand-by OK
[Expert@MGMT:0]#
```

Example - Querying the local Cluster Member

```
[Expert@Member1:0]# fw hastat
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.52 1 active OK
[Expert@Member1:0]#
```

fw kill

Description

Kills the specified Check Point processes.

Important:

- Make sure the killed process is restarted, or restart it manually. See sk97638.
- You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).

Syntax

```
fw [-d] kill [-t <Signal Number>] <Name of Process>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-t <Signal Number>`	Specifies which signal to send to the Check Point process. For the list of available signals and their numbers, run the `kill -l` command. For information about the signals, see the manual pages for the `kill` and `signal`. If you do not specify the signal explicitly, the command sends Signal 15 (`SIGTERM`). **Note** - Processes can ignore some signals.
`<Name of Process>`	Specifies the name of the Check Point process to kill. To see the names of the processes, run the `ps auxwf` command.

Example

```
fw kill fwd
```

fw log

Description

Shows the content of Check Point log files - Security (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`).

Important - You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).

Syntax

```
fw log {-h | -help}
```

```
fw [-d] log [-a] [-b "<Start Timestamp>" "<End Timestamp>"] [-c
<Action>] [{-f | -t}] [-g] [-H] [-h <Origin>] [-i] [-k {<Alert
Name> | all}] [-l] [-m {initial | semi | raw}] [-n] [-o] [-p] [-q]
[-S] [-s "<Start Timestamp>"] [-e "<End Timestamp>"] [-u
<Unification Scheme File>] [-w] [-x <Start Entry Number>] [-y <End
Entry Number>] [-z] [-#] [<Log File>]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the built-in usage. **Note** - The built-in usage does not show some of the parameters described in this table.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-a`	Shows only Account log entries.

Parameter	Description
`-b "<Start Timestamp>" "<End Timestamp>"`	Shows only entries that were logged between the specified start and end times. ■ The *<Start Timestamp>* and *<End Timestamp>* may be a date, a time, or both. ■ If date is omitted, then the command assumes the current date. ■ Enclose the "*<Start Timestamp>*" and "*<End Timestamp>* in single or double quotes (`-b 'XX' 'YY'`", or `-b "XX" "YY`). ■ You cannot use the "`-b`" parameter together with the "`-s`" or "`-e`" parameters. ■ See the date and time format below.
`-c <Action>`	Shows only events with the specified action. One of these: ■ `accept` ■ `drop` ■ `reject` ■ `encrypt` ■ `decrypt` ■ `vpnroute` ■ `keyinst` ■ `authorize` ■ `deauthorize` ■ `authcrypt` ■ `ctl` **Notes:** ■ The `fw log` command always shows the **Control** (`ctl`) actions. ■ For *login* action, use the `authcrypt`.
`-e "<End Timestamp>"`	Shows only entries that were logged before the specified time. **Notes:** ■ The *<End Timestamp>* may be a date, a time, or both. ■ Enclose the *<End Timestamp>* in single or double quotes (`-e '...'`, or `-e "..."`). ■ You cannot use the "`-e`" parameter together with the "`-b`" parameter. ■ See the date and time format below.

Parameter	Description
`-f`	This parameter: 1. Shows the saved entries that match the specified conditions. 2. After the command reaches the end of the currently opened log file, it continues to monitor the log file indefinitely and shows the new entries that match the specified conditions. **Note** - Applies only to the *active* log file `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`
`-g`	Does not show delimiters. The default behavior is: ■ Show a colon (`:`) after a field name ■ Show a semi-colon (`;`) after a field value
`-H`	Shows the High Level Log key.
`-h <Origin>`	Shows only logs that were generated by the Security Gateway with the specified IP address or object name (as configured in SmartConsole).
`-i`	Shows log UID.
`-k {<Alert Name> | all}`	Shows entries that match a specific alert type: ■ *<Alert Name>* - Show only entries that match a specific alert type: • `alert` • `mail` • `snmp_trap` • `spoof` • `user_alert` • `user_auth` ■ `all` - Show entries that match all alert types (this is the default).
`-l`	Shows both the date and the time for each log entry. The default is to show the date only once above the relevant entries, and then specify the time for each log entry.

Parameter	Description
`-m`	Specifies the log unification mode: ■ `initial` - Complete unification of log entries. The command shows one unified log entry for each ID. This is the default. If you also specify the `-f` parameter, then the output does not show any updates, but shows only entries that relate to the start of new connections. To shows updates, use the `semi` parameter. ■ `semi` - Step-by-step unification of log entries. For each log entry, the output shows an entry that unifies this entry with all previously encountered entries with the same ID. ■ `raw` - No log unification. The output shows all log entries.
`-n`	Does not perform DNS resolution of the IP addresses in the log file (this is the default behavior). This significantly speeds up the log processing.
`-o`	Shows detailed log chains - shows all the log segments in the log entry.
`-p`	Does not perform resolution of the port numbers in the log file (this is the default behavior). This significantly speeds up the log processing.
`-q`	Shows the names of log header fields.
`-S`	Shows the Sequence Number.
`-s "<Start Timestamp>"`	Shows only entries that were logged after the specified time. **Notes:** ■ The *<Start Timestamp>* may be a date, a time, or both. ■ If the date is omitted, then the command assumed the current date. ■ Enclose the *<Start Timestamp>* in single or double quotes (`-s '...'`, or `-s "..."`). ■ You cannot use the "`-s`" parameter together with the "`-b`" parameter. ■ See the date and time format below.

Parameter	Description
`-t`	This parameter: 1. Does not show the saved entries that match the specified conditions. 2. After the command reaches the end of the currently opened log file, it continues to monitor the log file indefinitely and shows the new entries that match the specified conditions. **Note** - Applies only to the *active* log file `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`
`-u <Unification Scheme File>`	Specifies the path and name of the log unification scheme file. The default log unification scheme file is: `$FWDIR/conf/log_unification_scheme.C`
`-w`	Shows the flags of each log entry (different bits used to specify the "nature" of the log - for example, control, audit, accounting, complementary, and so on).
`-x <Start Entry Number>`	Shows only entries from the specified log entry number and below, counting from the beginning of the log file.
`-y <End Entry Number>`	Shows only entries until the specified log entry number, counting from the beginning of the log file.
`-z`	In case of an error (for example, wrong field value), continues to show log entries. The default behavior is to stop.
`-#`	Show confidential logs in clear text.
`<Log File>`	Specifies the log file to read. If you do not specify the log file explicitly, the command opens the `$FWDIR/log/fw.log` log file. You can specify a switched log file.

Date and Time format

Part of timestamp	Format	Example
Date only	`MMM DD, YYYY`	`June 11, 2018`
Time only Note - In this case, the command assumes the current date.	`HH:MM:SS`	`14:20:00`
Date and Time	`MMM DD, YYYY HH:MM:SS`	`June 11, 2018 14:20:00`

Output

Each output line consists of a single log entry, whose fields appear in this format:

Note - The fields that show depends on the connection type.

```
HeaderDateHour ContentVersion HighLevelLogKey Uuid SequenceNum
Flags Action Origin IfDir InterfaceName LogId ...
```

This table describes some of the fields.

Field Header	Description	Example
`HeaderDateHour`	Date and Time	`12Jun2018 12:56:42`
`ContentVersion`	Version	`5`
`HighLevelLogKey`	High Level Log Key	`<max_null>`, or empty
`Uuid`	Log UUID	`(0x5b1f99cb,0x0,0x3403a8c0,0xc0000000)`
`SequenceNum`	Log Sequence Number	`1`

Field Header	Description	Example
`Flags`	Internal flags that specify the "nature" of the log - for example, control, audit, accounting, complementary, and so on	`428292`
`Action`	Action performed on this connection	■ `accept` ■ `dropreject` ■ `encrypt` ■ `decrypt` ■ `vpnroute` ■ `keyinst` ■ `authorize` ■ `deauthorize` ■ `authcrypt` ■ `ctl`
`Origin`	Object name of the Security Gateway that generated this log	`MyGW`
`IfDir`	Traffic direction through interface: ■ `<` - Outbound (sent by a Security Gateway) ■ `>` - Inbound (received by a Security Gateway)	■ `<` ■ `>`

Field Header	Description	Example
`InterfaceName`	Name of the Security Gateway interface, on which this traffic was logged If a Security Gateway performed some internal action (for example, log switch), then the log entry shows `daemon`	■ `eth0` ■ `daemon` ■ `N/A`
`LogId`	Log ID	`0`
`Alert`	Alert Type	■ `alert` ■ `mail` ■ `snmp_trap` ■ `spoof` ■ `user_alert` ■ `user_auth`
`OriginSicName`	SIC name of the Security Gateway that generated this log	`CN=MyGW,O=MyDomain_ Server.checkpoint.com.s6t98x`
`inzone`	Inbound Security Zone	`Local`
`outzone`	Outbound Security Zone	`External`
`service_id`	Name of the service used to inspect this connection	`ftp`
`src`	Object name or IP address of the connection's source server	`MyHost`

Field Header	Description	Example
`dst`	Object name or IP address of the connection's destination server	`MyFTPServer`
`proto`	Name of the connection's protocol	`tcp`
`sport_svc`	Source port of the connection	`64933`
`ProductName`	Name of the Check Point product that generated this log	■ `VPN-1 & FireWall-1` ■ `Application Control` ■ `FloodGate-1`
`ProductFamily`	Name of the Check Point product family that generated this log	`Network`

Examples

Example 1 - Show all log entries with both the date and the time for each log entry

```
fw log -l
```

Example 2 - Show all log entries that start after the specified timestamp

```
[Expert@MyGW:0]# fw log -l -s "June 12, 2018 12:33:00"
 12Jun2018 12:33:00 5 N/A 1 accept MyGW > N/A LogId: <max_null>; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; fg-1_client_in_rule_name: Default; fg-1_client_out_rule_name: Default; fg-1_server_in_rule_name: Host
Redirect; fg-1_server_out_rule_name: ; ProductName: FG; ProductFamily: Network;

 12Jun2018 12:33:39 5 N/A 1 drop MyGW < eth0 LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; inzone: Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_
table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid: 4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_
uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_table: TABLE_END; UP_action_table: TABLE_START; ROW_
START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc: ftp; sport_svc: 64933;
ProductFamily: Network;

... ... ...

[Expert@MyGW:0]#
```

Example 3 - Show all log entries between the specified timestamps

```
[Expert@MyGW:0]# fw log -l -b "June 12, 2018 12:33:00" 'June 12, 2018 12:34:00'
 12Jun2018 12:33:00 5 N/A 1 accept MyGW > N/A LogId: <max_null>; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; fg-1_client_in_rule_name: Default; fg-1_client_out_rule_name: Default; fg-1_server_in_rule_name: Host
Redirect; fg-1_server_out_rule_name: ; ProductName: FG; ProductFamily: Network;

 12Jun2018 12:33:39 5 N/A 1 drop MyGW < eth0 LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; inzone: Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_
table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid: 4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_
uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_table: TABLE_END; UP_action_table: TABLE_START; ROW_
START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc: ftp; sport_svc: 64933;
ProductFamily: Network;

 12Jun2018 12:33:45 5 N/A 1 ctl MyGW > LogId: <max_null>; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; description: Contracts; reason: Could not reach
"https://productcoverage.checkpoint.com/ProductCoverageService". Check DNS and Proxy configuration on the gateway.; Severity: 2;
status: Failed; version: 1.0; failure_impact: Contracts may be out-of-date; update_service: 1; ProductName: Security
Gateway/Management; ProductFamily: Network;
[Expert@MyGW:0]#
```

Example 4 - Show all log entries with action "drop"

```
[Expert@MyGW:0]# fw log -l -c drop
 12Jun2018 12:33:39 5 N/A 1 drop MyGW < eth0 LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; inzone: Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_
table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid: 4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_
uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_table: TABLE_END; UP_action_table: TABLE_START; ROW_
START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc: ftp; sport_svc: 64933;
ProductFamily: Network;
[Expert@MyGW:0]#
```

Example 5 - Show all log entries with action "drop", show all field headers, and show log flags

```
[Expert@MyGW:0]# fw log -l -q -w -c drop
 HeaderDateHour: 12Jun2018 12:33:39; ContentVersion: 5; HighLevelLogKey: <max_null>; LogUid: ; SequenceNum: 1; Flags: 428292; Action:
drop; Origin: MyGW; IfDir: <; InterfaceName: eth0; Alert: ; LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; inzone: Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_
table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid: 4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_
uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_table: TABLE_END; UP_action_table: TABLE_START; ROW_
START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc: ftp; sport_svc: 64933;
ProductFamily: Network;
[Expert@MyGW:0]#
```

Example 6 - Show only log entries from 0 to 10 (counting from the beginning of the log file)

```
[Expert@MyGW:0]# fw log -l -x 0 -y 10
... ...
[Expert@MyGW:0]#
```

fw logswitch

Description

Switches the current active log file:

1. Closes the current active log file.
2. Renames the current active log file.
3. Creates a new active log file with the default name.

Notes:

- By default, this command switches the active Security log file - `$FWDIR/log/fw.log`
- You can specify to switch the active Audit log file - `$FWDIR/log/fw.adtlog`

Important You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).

Syntax

```
fw [-d] logswitch
      [-audit] [<Name of Switched Log>]
      -h <Target> [[+ | -]<Name of Switched Log>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-audit`	Specifies to switch the active Audit log file (`$FWDIR/log/fw.adtlog`). You can use this parameter only on a Management Server.

Parameter	Description
`-h <Target>`	Specifies the remote server, on which to switch the log. **Notes:** ■ The local and the remote servers must have established SIC trust. ■ The local server can be a Security Management Server, a Log Server. ■ The remote server can be a Security Gateway, a Log Server, or a Security Management Server in High Availability deployment. ■ You can specify the remote managed server by its main IP address or Object Name as configured in SmartConsole.

`<Name of Switched Log>`	Specifies the name of the switched log file.
	Notes:
	■ If you do not specify this parameter, then a default name is:
	`<YYYY-MM-DD_HHMMSS>.log`
	`<YYYY-MM-DD_HHMMSS>.adtlog`
	For example, *2018-03-26_174455.log*
	■ If you specify the name of the switched log file, then the name of the switch log file is:
	`<Specified_Log_Name>.log`
	`<Specified_Log_Name>.adtlog`
	■ The log switch operation fails if the specified name for the switched log matches the name of an existing log file.
	■ The maximum length of the specified name of the switched log file is 230 characters.

`+`	Specifies to *copy* the active log from the remote server to the local server.
	Notes:
	■ If you specify the name of the switched log file, you must write it immediately after *this* + (plus) parameter.
	■ The command copies the active log from the remote server and saves it in the `$FWDIR/log/` directory on the local server.
	■ The default name of the saved log file is:
	`<Gateway_Object_Name>__<YYYY-MM-DD_HHMMSS>.log`
	For example, *MyGW__2018-03-26_174455.log*
	■ If you specify the name of the switched log file, then the name of the saved log file is:
	`<Gateway_Object_Name>__<Specified_Log_Name>.log`
	■ When this command copies the log file from the remote server, it compresses the file.

Parameter	Description
-	Specifies to *transfer* the active log from the remote server to the local server. **Notes:** ■ The command saves the copied active log file in the `$FWDIR/log/` directory on the local server and then deletes the switched log file on the remote server. ■ If you specify the name of the switched log file, you must write it immediately after this - (minus) parameter. ■ The default name of the saved log file is: `<Gateway_Object_Name>__<YYYY-MM-DD_HHMMSS>.log` For example, *MyGW__2018-03-26_174455.log* ■ If you specify the name of the switched log file, then the name of the saved log file is: `<Gateway_Object_Name>__<Specified_Log_Name>.log` ■ When this command transfers the log file from the remote server, it compresses the file. ■ As an alternative, you can use the *"fw fetchlogs" on page 268* command.

Compression

When this command transfers the log files from the remote server, it compresses the file with the `gzip` command (see RFC 1950 to RFC 1952 for details). The algorithm is a variation of LZ77 method. The compression ratio varies with the content of the log file and is difficult to predict. Binary data are not compressed. Text data, such as user names and URLs, are compressed.

Example - Switching the active Security log on a Security Management Server or Security Gateway

```
[Expert@MGMT:0]# fw logswitch
Log file has been switched to: 2018-06-13_182359.log
[Expert@MGMT:0]#
```

Example - Switching the active Audit log on a Security Management Server

```
[Expert@MGMT:0]# fw logswitch -audit
Log file has been switched to: 2018-06-13_185711.adtlog
[Expert@MGMT:0]#
```

Example - Switching the active Security log on a managed Security Gateway and copying the switched log

```
[Expert@MGMT:0]# fw logswitch -h MyGW +
Log file has been switched to: 2018-06-13_185451.log
[Expert@MGMT:0]#
[Expert@MGMT:0]# ls $FWDIR/log/*.log
/opt/CPsuite-R81.20/fw1/log/fw.log
/opt/CPsuite-R81.20/fw1/log/MyGW__2018-06-13_185451.log
[Expert@MGMT:0]#

[Expert@MyGW:0]# ls $FWDIR/log/*.log
/opt/CPsuite-R81.20/fw1/log/fw.log
/opt/CPsuite-R81.20/fw1/log/2018-06-13_185451.log
[Expert@MyGW:0]#
```

fw lslogs

Description

Shows a list of Security log files (`$FWDIR/log/*.log`) and Audit log files (`$FWDIR/log/*.adtlog`) residing on the local server or a remote server.

Important - You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).

Syntax

```
fw [-d] lslogs [-f <Name of Log File 1>] [-f <Name of Log File 2>]
... [-f <Name of Log File N>] [-e] [-r] [-s {name | size | stime |
etime}] [<Target>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-f <Name of Log File>`	Specifies the name of the log file to show. Need to specify only the name. **Notes:** ■ If the log file name is not specified explicitly, the command shows all Security log files (`$FWDIR/log/*.log`). ■ File names may include `*` and `?` as wildcards (for example, `2019-0?-*`). If you enter a wildcard, you must enclose it in double quotes or single quotes. ■ You can specify multiple log files in one command. You must use the "`-f`" parameter for each log file name pattern: `-f <Name of Log File 1> -f <Name of Log File 2> ... -f <Name of Log File N>`

Parameter	Description
`-e`	Shows an extended file list. It includes the following information for each log file: ■ `Size` - The total size of the log file and its related pointer files ■ `Creation Time` - The time the log file was created ■ `Closing Time` - The time the log file was closed ■ `Log File Name` - The file name
`-r`	Reverses the sort order (descending order).
`-s {name | size | stime | etime}`	Specifies the sort order of the log files using one of the following sort options: ■ `name` - The file name ■ `size` - The file size ■ `stime` - The time the log file was created (this is the default option) ■ `etime` - The time the log file was closed
<Target>	Specifies the remote Check Point server, with which this local Check Point server has established SIC trust. **Notes:** ■ The local and the remote servers must have established SIC trust. ■ The local server can be a Security Management Server, a Log Server, a Security Gateway, a Cluster Member. ■ The remote server can be a Security Gateway, a Cluster Member, a Log Server, or a Security Management Server in High Availability deployment. ■ You can specify the remote managed server by its main IP address or Object Name as configured in SmartConsole.

Example 1 - Default output

```
[Expert@HostName:0]# fw lslogs
     Size Log file name
         9KB 2019-06-14_000000.log
        11KB 2019-06-15_000000.log
         9KB 2019-06-16_000000.log
        10KB 2019-06-17_000000.log
         9KB fw.log
[Expert@HostName:0]#
```

Example 2 - Showing all log files

```
[Expert@HostName:0]# fw lslogs -f "*"
     Size Log file name
          9KB fw.adtlog
          9KB fw.log
          9KB 2019-05-29_000000.adtlog
          9KB 2019-05-29_000000.log
          9KB 2019-05-20_000000.adtlog
          9KB 2019-05-20_000000.log
[Expert@HostName:0]#
```

Example 3 - Showing only log files specified by the patterns

```
[Expert@HostName:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*'
     Size Log file name
          9KB 2019-06-14_000000.adtlog
          9KB 2019-06-14_000000.log
         11KB 2019-06-15_000000.adtlog
         11KB 2019-06-15_000000.log
[Expert@HostName:0]#
```

Example 4 - Showing only log files specified by the patterns and their extended information

```
[Expert@HostName:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*'
     Size Log file name
          9KB 2019-06-14_000000.adtlog
          9KB 2019-06-14_000000.log
         11KB 2019-06-15_000000.adtlog
         11KB 2019-06-15_000000.log
[Expert@HostName:0]#
```

Example 5 - Showing only log files specified by the patterns, sorting by name in reverse order

```
[Expert@HostName:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*' -e -s name -r
     Size Creation Time Closing Time Log file name
        11KB 14Jun2018 0:00:00 15Jun2018 0:00:00 2019-06-15_000000.log
        11KB 14Jun2018 0:00:00 15Jun2018 0:00:00 2019-06-15_000000.adtlog
         9KB 13Jun2018 18:23:59 14Jun2018 0:00:00 2019-06-14_000000.log
         9KB 13Jun2018 0:00:00 14Jun2018 0:00:00 2019-06-14_000000.adtlog
[Expert@HostName:0]#
```

Example 6 - Showing only log files specified by the patterns, from a managed Security Gateway with main IP address 192.168.3.53

```
[Expert@MGMT:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*' 192.168.3.53
     Size Log file name
        11KB 2019-06-15_000000.adtlog
        11KB 2019-06-15_000000.log
         9KB 2019-06-14_000000.log
         9KB 2019-06-14_000000.adtlog
[Expert@MGMT:0]#
```

fw mergefiles

Description

Merges several Security log files (`$FWDIR/log/*.log`) into a single log file.

Merges several Audit log files (`$FWDIR/log/*.adtlog`) into a single log file.

Important:

- Do **not** merge the *active* Security file `$FWDIR/log/fw.log` with other Security switched log files.
  Switch the active Security file `$FWDIR/log/fw.log` (with the *"fw logswitch" on page 1141* command) and only then merge it with other Security switched log files.
- Do **not** merge the *active* Audit file `$FWDIR/log/fw.adtlog` with other Audit switched log files.
  Switch the active Audit file `$FWDIR/log/fw.adtlog` (with the *"fw logswitch" on page 1141* command) and only then merge it with other Audit switched log files.
- This command unifies logs entries with the same Unique-ID (UID). If you rotate the current active log file before all the segments of a specific log arrive, this command merges the records with the same Unique ID from two different files, into one fully detailed record.
- If the size of the final merged log file exceeds 2GB, this command creates a list of merged files, where the size of each merged file size is not more than 2GB.
  The user receives this warning:

  ```
  Warning: The size of the files you have chosen to merge
  is greater than 2GB. The merge will produce two or more
  files.
  ```

  The names of merged files are:
  - *<Name of Merged Log File>*.log
  - *<Name of Merged Log File>*_1.log
  - *<Name of Merged Log File>*_2.log
  - ... ...
  - *<Name of Merged Log File>*_N.log

Important - You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).

Syntax

```
fw [-d] mergefiles {-h | -help}
```

```
fw [-d] mergefiles [-r] [-s] [-t <Time Conversion File>] <Name of Log File 1> <Name of Log File 2> ... <Name of Log File N> <Name of Merged Log File>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{-h | -help}`	Shows the built-in usage.
`-r`	Removes duplicate entries.
`-s`	Sorts the merged file by the **Time** field in log records.

`-t <Time Conversion File>`	Specifies a full path and name of a file that instructs this command how to adjust the times during the merge.
	This is required if you merge log files from Log Servers configured with different time zones.
	The file format is:
	`<IP Address of Log Server #1> <Signed Date Time #1 in Seconds>`
	`<IP Address of Log Server #2> <Signed Date Time #2 in Seconds>`
	`... ...`
	Notes
	■ You must specify the absolute path and the file name.
	■ The name of the time conversion file cannot exceed 230 characters.

Parameter	Description
<Name of Log File 1> ... <Name of Log File N>	Specifies the log files to merge. **Notes:** ■ You must specify the absolute path and the name of the input log files. ■ The name of the input log file cannot exceed 230 characters.
<Name of Merged Log File>	Specifies the output merged log file. **Notes:** ■ The name of the merged log file cannot exceed 230 characters. ■ If a file with the specified name already exists, the command stops and asks you to remove the existing file, or to specify another name. ■ The size of the merged log file cannot exceed 2 GB. In such scenario, the command creates several merged log files, each not exceeding the size limit.

Example - Merging Security log files

```
[Expert@HostName:0]# ls -l $FWDIR/*.log
-rw-rw-r-- 1 admin root 189497 Sep  7 00:00 2019-09-07_000000.log
-rw-rw-r-- 1 admin root  14490 Sep  9 09:52 2019-09-09_000000.log
-rw-rw-r-- 1 admin root  30796 Sep 10 10:56 2019-09-10_000000.log
-rw-rw-r-- 1 admin root  24503 Sep 10 13:08 fw.log
[Expert@HostName:0]#
[Expert@HostName:0]# fw mergefiles -s $FWDIR/2019-09-07_000000.log $FWDIR/2019-09-09_000000.log
$FWDIR/2019-09-10_000000.log /var/log/2019-Sep-Merged.log
[Expert@HostName:0]#
[Expert@HostName:0]# ls -l /var/log/2019-Sep-Merged.log*
-rw-rw---- 1 admin root 213688 Sep 10 13:18 /var/log/2019-Sep-Merged.log
-rw-rw---- 1 admin root   8192 Sep 10 13:18 /var/log/2019-Sep-Merged.logLuuidDB
-rw-rw---- 1 admin root     80 Sep 10 13:18 /var/log/2019-Sep-Merged.logaccount_ptr
-rw-rw---- 1 admin root   2264 Sep 10 13:18 /var/log/2019-Sep-Merged.loginitial_ptr
-rw-rw---- 1 admin root   4448 Sep 10 13:18 /var/log/2019-Sep-Merged.logptr
[Expert@HostName:0]#
```

fw repairlog

Description

Check Point Security log file (`$FWDIR/log/*.log`) and Audit log files (`$FWDIR/log/*.adtlog`) are databases, with special pointer files.

If these log pointer files become corrupted (which causes the inability to read the log file), this command can rebuild them.

Log File Type	Log File Location	Log Pointer Files

Security log	`$FWDIR/log/*.log`	`*.logptr`
		`*.logaccount_ptr`
		`*.loginitial_ptr`
		`*.logLuuidDB`

Audit log	`$FWDIR/log/*.adtlog`	`*.adtlogptr`
		`*.adtlogaccount_ptr`
		`*.adtloginitial_ptr`
		`*.adtlogLuuidDB`

Important - You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).

Syntax

```
fw [-d] repairlog [-u] <Name of Log File>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-u`	Specifies to rebuild the unification chains in the log file.
<Name of Log File>	The name of the log file to repair.

Example - Repairing the Audit log file

```
fw repairlog -u 2019-06-17_000000.adtlog
```

fw sam

Description

Manages the Suspicious Activity Monitoring (SAM) rules. You can use the SAM rules to block connections to and from IP addresses without the need to change or reinstall the Security Policy. For more information, see sk112061.

You can create the Suspicious Activity Rules in two ways:

- In SmartConsole from Monitoring Results
- In CLI with the `fw sam` command

Notes:

- VSX Gateways and VSX Cluster Members do not support Suspicious Activity Monitoring (SAM) Rules. See sk79700.
- See the "`fw sam_policy`" and "`sam_alert`" commands.
- SAM rules consume some CPU resources on Security Gateway.

  Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.
- Logs for enforced SAM rules (configured with the `fw sam` command) are stored in the `$FWDIR/log/sam.dat` file.
  By design, the file is purged when the number of stored entries reaches 100,000.
  This data log file contains the records in one of these formats:

`<type>,<actions>,<expire>,<ipaddr>`
`<type>,<actions>,<expire>,<src>,<dst>,<dport>,<ip_p>`

- SAM Requests are stored on the Security Gateway in the kernel table `sam_requests`.
- IP Addresses that are blocked by SAM rules, are stored on the Security Gateway in the kernel table `sam_blocked_ips`.

Note - To configure SAM Server settings for a Security Gateway or Cluster:

1. Connect with SmartConsole to the applicable Security Management Server or Domain Management Server.
2. From the left navigation panel, click Gateways & Servers.
3. Open the Security Gateway or Cluster object.
4. From the left tree, click **Other > SAM**.
5. Configure the settings.
6. Click **OK**.
7. Install the Access Control Policy on this Security Gateway or Cluster object.

Syntax

- **To add or cancel a SAM rule according to criteria:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM
Server>] [-f <Security Gateway>] [-t <Timeout>] [-l <Log
Type>] [-C] [-e <key=val>]+ [-r] -{n|i|I|j|J} <Criteria>
```

- **To delete all SAM rules:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM
Server>] [-f <Security Gateway>] -D
```

- **To monitor all SAM rules:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM
Server>] [-f <Security Gateway>] [-r] -M -{i|j|n|b|q} all
```

- **To monitor SAM rules according to criteria:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM
Server>] [-f <Security Gateway>] [-r] -M -{i|j|n|b|q}
<Criteria>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-v`	Enables verbose mode. In this mode, the command writes one message to *stderr* for each Security Gateway, on which the command is enforced. These messages show whether the command was successful or not.
`-s <SAM Server>`	Specifies the IP address (in the X.X.X.X format) or resolvable HostName of the Security Gateway that enforces the command. The default is `localhost`.

Parameter	Description
`-S <SIC Name of SAM Server>`	Specifies the SIC name for the SAM server to be contacted. It is expected that the SAM server has this SIC name, otherwise the connection fails. **Notes:** ■ If you do not explicitly specify the SIC name, the connection continues without SIC names comparison. ■ For more information about enabling SIC, refer to the OPSEC API Specification. ■ On VSX Gateway, run the *fw vsx showncs -vs <VSID>* command to show the SIC name for the applicable Virtual System.
`-f <Security Gateway>`	Specifies the Security Gateway, on which to enforce the action. `<Security Gateway>` can be one of these: ■ *All* - Default. Specifies to enforce the action on all managed Security Gateways, where SAM Server runs. You can use this syntax only on Security Management Server or Domain Management Server. ■ *localhost* - Specifies to enforce the action on this local Check Point server (on which the `fw sam` command is executed). You can use this syntax only on Security Gateway or StandAlone. ■ *Gateways* - Specifies to enforce the action on all objects defined as Security Gateways, on which SAM Server runs. You can use this syntax only on Security Management Server or Domain Management Server. ■ *Name of Security Gateway object* - Specifies to enforce the action on this specific Security Gateway object. You can use this syntax only on Security Management Server or Domain Management Server. ■ *Name of Group object* - Specifies to enforce the action on all specific Security Gateways in this Group object. **Notes:** ■ You can use this syntax only on Security Management Server or Domain Management Server. ■ VSX Gateways and VSX Cluster Members do not support Suspicious Activity Monitoring (SAM) Rules. See sk79700.
`-D`	Cancels all inhibit ("`-i`", "`-j`", "`-I`", "`-J`") and notify ("`-n`") parameters. **Notes:** ■ To "uninhibit" the inhibited connections, run the `fw sam` command with the "`-C`" or "`-D`" parameters. ■ It is also possible to use this command for active SAM requests.

Parameter	Description
`-C`	Cancels the `fw sam` command to inhibit connections with the specified parameters. **Notes:** ■ These connections are no longer inhibited (no longer rejected or dropped). ■ The command parameters must match the parameters in the original `fw sam` command, except for the `-t <Timeout>` parameter.
`-t <Timeout>`	Specifies the time period (in seconds), during which the action is enforced. The default is forever, or until you cancel the `fw sam` command.
`-l <Log Type>`	Specifies the type of the log for enforced action: ■ `nolog` - Does not generate Log / Alert at all ■ `short_noalert` - Generates a Log ■ `short_alert` - Generates an Alert ■ `long_noalert` - Generates a Log ■ `long_alert` - Generates an Alert (this is the default)
`-e <key=val>+`	Specifies rule information based on the keys and the provided values. Multiple keys are separated by the plus sign (+). Available keys are (each is limited to 100 characters): ■ `name` - Security rule name ■ `comment` - Security rule comment ■ `originator` - Security rule originator's username
`-r`	Specifies not to resolve IP addresses.
`-n`	Specifies to generate a "Notify" long-format log entry. **Notes:** ■ This parameter generates an alert when connections that match the specified services or IP addresses pass through the Security Gateway. ■ This action does not inhibit / close connections.
`-i`	Inhibits (drops or rejects) new connections with the specified parameters. **Notes:** ■ Each inhibited connection is logged according to the log type. ■ Matching connections are rejected.

Parameter	Description
`-I`	Inhibits (drops or rejects) new connections with the specified parameters, and closes all existing connections with the specified parameters. **Notes:** ■ Matching connections are rejected. ■ Each inhibited connection is logged according to the log type.
`-j`	Inhibits (drops or rejects) new connections with the specified parameters. **Notes:** ■ Matching connections are dropped. ■ Each inhibited connection is logged according to the log type.
`-J`	Inhibits new connections with the specified parameters, and closes all existing connections with the specified parameters. **Notes:** ■ Matching connections are dropped. ■ Each inhibited connection is logged according to the log type.
`-b`	Bypasses new connections with the specified parameters.
`-q`	Quarantines new connections with the specified parameters.
`-M`	Monitors the active SAM requests with the specified actions and criteria.
`all`	Gets all active SAM requests. This is used for monitoring purposes only.
`<Criteria>`	Criteria are used to match connections. The criteria and are composed of various combinations of the following parameters: ■ Source IP Address ■ Source Netmask ■ Destination IP Address ■ Destination Netmask ■ Port (see *IANA Service Name and Port Number Registry*) ■ Protocol Number (see *IANA Protocol Numbers*)

Parameter	Description
	Possible combinations are (see the explanations below this table): ■ src *<IP>* ■ dst *<IP>* ■ any *<IP>* ■ subsrc *<IP> <Netmask>* ■ subdst *<IP> <Netmask>* ■ subany *<IP> <Netmask>* ■ srv *<Src IP> <Dest IP> <Port> <Protocol>* ■ subsrv *<Src IP> <Src Netmask> <Dest IP> <Dest Netmask> <Port> <Protocol>* ■ subsrvs *<Src IP> <Src Netmask> <Dest IP> <Port> <Protocol>* ■ subsrvd *<Src IP> <Dest IP> <Dest Netmask> <Port> <Protocol>* ■ dstsrv *<Dest IP> <Port> <Protocol>* ■ subdstsrv *<Dest IP> <Dest Netmask> <Port> <Protocol>* ■ srcpr *<IP> <Protocol>* ■ dstpr *<IP> <Protocol>* ■ subsrcpr *<IP> <Netmask> <Protocol>* ■ subdstpr *<IP> <Netmask> <Protocol>* ■ generic *<key=val>*

Explanation for the *<Criteria>* syntax

Parameter	Description
src *<IP>*	Matches the Source IP address of the connection.
dst <IP>	Matches the Destination IP address of the connection.
any *<IP>*	Matches either the Source IP address or the Destination IP address of the connection.
subsrc *<IP> <Netmask>*	Matches the Source IP address of the connections according to the netmask.
subdst *<IP> <Netmask>*	Matches the Destination IP address of the connections according to the netmask.

Parameter	Description
`subany <IP> <Netmask>`	Matches either the Source IP address or Destination IP address of connections according to the netmask.
`srv <Src IP> <Dest IP> <Port> <Protocol>`	Matches the specific Source IP address, Destination IP address, Service (port number) and Protocol.
`subsrv <Src IP> <Netmask> <Dest IP> <Netmask> <Port> <Protocol>`	Matches the specific Source IP address, Destination IP address, Service (port number) and Protocol. Source and Destination IP addresses are assigned according to the netmask.
`subsrvs <Src IP> <Src Netmask> <Dest IP> <Port> <Protocol>`	Matches the specific Source IP address, source netmask, destination netmask, Service (port number) and Protocol.
`subsrvd <Src IP> <Dest IP> <Dest Netmask> <Port> <Protocol>`	Matches specific Source IP address, Destination IP, destination netmask, Service (port number) and Protocol.
`dstsrv <Dest IP> <Service> <Protocol>`	Matches specific Destination IP address, Service (port number) and Protocol.
`subdstsrv <Dest IP> <Netmask> <Port> <Protocol>`	Matches specific Destination IP address, Service (port number) and Protocol. Destination IP address is assigned according to the netmask.
`srcpr <IP> <Protocol>`	Matches the Source IP address and protocol.
`dstpr <IP> <Protocol>`	Matches the Destination IP address and protocol.
`subsrcpr <IP> <Netmask> <Protocol>`	Matches the Source IP address and protocol of connections. Source IP address is assigned according to the netmask.
`subdstpr <IP> <Netmask> <Protocol>`	Matches the Destination IP address and protocol of connections. Destination IP address is assigned according to the netmask.

Parameter	Description
`generic <key=val>+`	Matches the GTP connections based on the specified keys and provided values. Multiple keys are separated by the plus sign (+). Available keys are: ■ `service=gtp` ■ `imsi` ■ `msisdn` ■ `apn` ■ `tunl_dst` ■ `tunl_dport` ■ `tunl_proto`

fw sam_policy

Description

Manages the Suspicious Activity Policy editor that works with these types of rules:

- Suspicious Activity Monitoring (SAM) rules.

  See sk112061: How to create and view Suspicious Activity Monitoring (SAM) Rules.

- Rate Limiting rules.

  See sk112454: How to configure Rate Limiting rules for DoS Mitigation.

Also, see these commands:

- *"fw sam" on page 295*
- *"sam_alert" on page 405*

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax for IPv4

```
fw [-d] sam_policy
      add <options>
      batch
      del <options>
      get <options>
```

```
fw [-d] samp
      add <options>
      batch
      del <options>
      get <options>
```

Syntax for IPv6

```
fw6 [-d] sam_policy
      add <options>
      batch
      del <options>
      get <options>
```

```
fw6 [-d] samp
      add <options>
      batch
      del <options>
      get <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`add <options>`	Adds one Rate Limiting rule one at a time. See *"fw sam_policy add" on page 306*.
`batch`	Adds or deletes many Rate Limiting rules at a time. See *"fw sam_policy batch" on page 319*.
`del <options>`	Deletes one configured Rate Limiting rule one at a time. See *"fw sam_policy del" on page 321*.
`get <options>`	Shows all the configured Rate Limiting rules. See *"fw sam_policy get" on page 324*.

fw sam_policy add

Description

The "*fw sam_policy add*" and "*fw6 sam_policy add*" commands:

- Add one Suspicious Activity Monitoring (SAM) rule at a time.
- Add one Rate Limiting rule at a time.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax to configure a Suspicious Activity Monitoring (SAM) rule for IPv4

```
fw [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] ip <IP Filter Arguments>
```

Syntax to configure a Suspicious Activity Monitoring (SAM) rule for IPv6

```
fw6 [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] ip <IP Filter Arguments>
```

Syntax to configure a Rate Limiting rule for IPv4

```
fw [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] quota <Quota Filter Arguments>
```

Syntax to configure a Rate Limiting rule for IPv6

```
fw6 [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] quota <Quota Filter Arguments
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-u`	Optional. Specifies that the rule category is `User-defined`. Default rule category is `Auto`.
`-a {d | n | b}`	Mandatory. Specifies the rule action if the traffic matches the rule conditions: ■ `d` - Drop the connection. ■ `n` - Notify (generate a log) about the connection and let it through. ■ `b` - Bypass the connection - let it through without checking it against the policy rules. **Note** - Rules with action set to *Bypass* cannot have a log or limit specification. Bypassed packets and connections do not count towards overall number of packets and connection for limit enforcement of type ratio.
`-l {r | a}`	Optional. Specifies which type of log to generate for this rule for all traffic that matches: ■ `-r` - Generate a regular log ■ `-a` - Generate an alert log

Parameter	Description
`-t <Timeout>`	Optional. Specifies the time period (in seconds), during which the rule will be enforced. Default timeout is indefinite.
`-f <Target>`	Optional. Specifies the target Security Gateways, on which to enforce the Rate Limiting rule. *<Target>* can be one of these: ■ `all` - This is the default option. Specifies that the rule should be enforced on all managed Security Gateways. ■ Name of the Security Gateway or Cluster object - Specifies that the rule should be enforced only on this Security Gateway or Cluster object (the object name must be as defined in the SmartConsole). ■ Name of the Group object - Specifies that the rule should be enforced on all Security Gateways that are members of this Group object (the object name must be as defined in the SmartConsole).
`-n "<Rule Name>"`	Optional. Specifies the name (label) for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters. ■ Before each space or a backslash character in this string, you must write a backslash (\) character. Example: `"This\ is\ a\ rule\ name\ with\ a\ backslash\ \\"`
`-c "<Rule Comment>"`	Optional. Specifies the comment for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters. ■ Before each space or a backslash character in this string, you must write a backslash (\) character. Example: `"This\ is\ a\ comment\ with\ a\ backslash\ \\"`

Parameter	Description
`-o "<Rule Originator>"`	Optional. Specifies the name of the originator for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters. ■ Before each space or a backslash character in this string, you must write a backslash (\) character. Example: `"Created\ by\ John\ Doe"`
`-z "<Zone>"`	Optional. Specifies the name of the Security Zone for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters.
`ip <IP Filter Arguments>`	Mandatory (use this `ip` parameter, or the `quota` parameter). Configures the *Suspicious Activity Monitoring (SAM)* rule. Specifies the IP Filter Arguments for the SAM rule (you must use at least one of these options): `[-C] [-s <Source IP>] [-m <Source Mask>] [-d <Destination IP>] [-M <Destination Mask>] [-p <Port>] [-r <Protocol>]` See the explanations below.

Parameter	Description
`quota <Quota Filter Arguments>`	Mandatory (use this `quota` parameter, or the `ip` parameter). Configures the *Rate Limiting* rule. Specifies the Quota Filter Arguments for the Rate Limiting rule (see the explanations below): ■ `[flush true]` ■ `[source-negated {true | false}] source <Source>` ■ `[destination-negated {true | false}] destination <Destination>` ■ `[service-negated {true | false}] service <Protocol and Port numbers>` ■ `[<Limit1 Name> <Limit1 Value>] [<Limit2 Name> <Limit2 Value>] ...[<LimitN Name> <LimitN Value>]` ■ `[track <Track>]` **Important:** ■ The Quota rules are not applied immediately to the Security Gateway. They are only registered in the Suspicious Activity Monitoring (SAM) policy database. To apply all the rules from the SAM policy database immediately, add "`flush true`" in the `fw samp add` command syntax. ■ Explanation: For new connections rate (and for any rate limiting in general), when a rule's limit is violated, the Security Gateway also drops all packets that match the rule. The Security Gateway computes new connection rates on a per-second basis. At the start of the 1-second timer, the Security Gateway allows all packets, including packets for existing connections. If, at some point, during that 1 second period, there are too many new connections, then the Security Gateway blocks all remaining packets for the remainder of that 1-second interval. At the start of the next 1-second interval, the counters are reset, and the process starts over - the Security Gateway allows packets to pass again up to the point, where the rule's limit is violated.

Explanation for the *IP Filter Arguments* syntax for Suspicious Activity Monitoring (SAM) rules

Argument	Description
`-C`	Specifies that open connections should be closed.
`-s <Source IP>`	Specifies the Source IP address.
`-m <Source Mask>`	Specifies the Source subnet mask (in dotted decimal format - x.y.z.w).
`-d <Destination IP>`	Specifies the Destination IP address.
`-M <Destination Mask>`	Specifies the Destination subnet mask (in dotted decimal format - x.y.z.w).
`-p <Port>`	Specifies the port number (see *IANA Service Name and Port Number Registry*).
`-r <Protocol>`	Specifies the protocol number (see *IANA Protocol Numbers*).

Explanation for the *Quota Filter Arguments* syntax for Rate Limiting rules

Argument	Description
`flush true`	Specifies to compile and load the quota rule to the SecureXL immediately.
`[source-negated {true | false}] source <Source>`	Specifies the source type and its value: ■ `any` The rule is applied to packets sent from all sources. ■ `range:<IP Address>` or `range:<IP Address Start>-<IP Address End>` The rule is applied to packets sent from: • Specified IPv4 addresses (x.y.z.w) • Specified IPv6 addresses (xxxx:yyyy:....:zzzz) ■ `cidr:<IP Address>/<Prefix>` The rule is applied to packets sent from: • IPv4 address with Prefix from 0 to 32 • IPv6 address with Prefix from 0 to 128 ■ `cc:<Country Code>` The rule matches the country code to the source IP addresses assigned to this country, based on the Geo IP database. The two-letter codes are defined in ISO 3166-1 alpha-2. ■ `asn:<Autonomous System Number>` The rule matches the AS number of the organization to the source IP addresses that are assigned to this organization, based on the Geo IP database. The valid syntax is *ASnnnn*, where *nnnn* is a number unique to the specific organization. **Notes:** ■ Default is: `source-negated false` ■ The `source-negated true` processes all source types, *except* the specified type.

Argument	Description
`[destination-negated {true | false}] destination <Destination>`	Specifies the destination type and its value: ■ `any` The rule is applied to packets sent to all destinations. ■ `range:<IP Address>` or `range:<IP Address Start>-<IP Address End>` The rule is applied to packets sent to: • Specified IPv4 addresses (x.y.z.w) • Specified IPv6 addresses (xxxx:yyyy:...:zzzz) ■ `cidr:<IP Address>/<Prefix>` The rule is applied to packets sent to: • IPv4 address with Prefix from 0 to 32 • IPv6 address with Prefix from 0 to 128 ■ `cc:<Country Code>` The rule matches the country code to the destination IP addresses assigned to this country, based on the Geo IP database. The two-letter codes are defined in ISO 3166-1 alpha-2. ■ `asn:<Autonomous System Number>` The rule matches the AS number of the organization to the destination IP addresses that are assigned to this organization, based on the Geo IP database. The valid syntax is *ASnnnn*, where *nnnn* is a number unique to the specific organization. **Notes:** ■ Default is: `destination-negated false` ■ The `destination-negated true` will process all destination types except the specified type

Argument	Description
`[service-negated {true | false}] service <Protocol and Port numbers>`	Specifies the Protocol number (see *IANA Protocol Numbers*) and Port number (see *IANA Service Name and Port Number Registry*): ■ `<Protocol>` IP protocol number in the range 1-255 ■ `<Protocol Start>-<Protocol End>` Range of IP protocol numbers ■ `<Protocol>/<Port>` IP protocol number in the range 1-255 and TCP/UDP port number in the range 1-65535 ■ `<Protocol>/<Port Start>-<Port End>` IP protocol number and range of TCP/UDP port numbers from 1 to 65535 **Notes:** ■ Default is: `service-negated false` ■ The `service-negated true` will process all traffic except the traffic with the specified protocols and ports

Argument	Description
`[<Limit 1 Name> <Limit 1 Value>] [<Limit 2 Name> <Limit 2 Value>] ... [<Limit N Name> <Limit N Value>]`	Specifies quota limits and their values. **Note** - Separate multiple quota limits with spaces. ■ `concurrent-conns <Value>` Specifies the maximal number of concurrent active connections that match this rule. ■ `concurrent-conns-ratio <Value>` Specifies the maximal ratio of the *concurrent-conns* value to the total number of active connections through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`). ■ `pkt-rate <Value>` Specifies the maximum number of packets per second that match this rule. ■ `pkt-rate-ratio <Value>` Specifies the maximal ratio of the *pkt-rate* value to the rate of all connections through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`). ■ `byte-rate <Value>` Specifies the maximal total number of bytes per second in packets that match this rule. ■ `byte-rate-ratio <Value>` Specifies the maximal ratio of the *byte-rate* value to the bytes per second rate of all connections through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`). ■ `new-conn-rate <Value>` Specifies the maximal number of connections per second that match the rule. ■ `new-conn-rate-ratio <Value>` Specifies the maximal ratio of the *new-conn-rate* value to the rate of all connections per second through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`).

Argument	Description
`[track <Track>]`	Specifies the tracking option: ■ `source` Counts connections, packets, and bytes for specific source IP address, and not cumulatively for this rule. ■ `source-service` Counts connections, packets, and bytes for specific source IP address, and for specific IP protocol and destination port, and not cumulatively for this rule.

Examples

Example 1 - Rate Limiting rule with a range

```
fw sam_policy add -a d -l r -t 3600 quota service any source range:172.16.7.11-172.16.7.13 new-conn-rate 5 flush true
```

Explanations:

- This rule drops packets for all connections (`-a d`) that exceed the quota set by this rule, including packets for existing connections.
- This rule logs packets (`-l r`) that exceed the quota set by this rule.
- This rule will expire in 3600 seconds (`-t 3600`).
- This rule limits the rate of creation of new connections to 5 connections per second (`new-conn-rate 5`) for any traffic (`service any`) from the source IP addresses in the range 172.16.7.11 - 172.16.7.13 (`source range:172.16.7.11-172.16.7.13`).

  Note - The limit of the total number of log entries per second is configured with the *fwaccel dos config set -n <rate>* command.
- This rule will be compiled and loaded on the SecureXL, together with other rules in the Suspicious Activity Monitoring (SAM) policy database immediately, because this rule includes the "`flush true`" parameter.

Example 2 - Rate Limiting rule with a service specification

```
fw sam_policy add -a n -l r quota service 1,50-51,6/443,17/53 service-negated true source cc:QQ byte-rate 0
```

Explanations:

- This rule logs and lets through all packets (`-a n`) that exceed the quota set by this rule.
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to all packets except (`service-negated true`) the packets with IP protocol number 1, 50-51, 6 port 443 and 17 port 53 (`service 1,50-51,6/443,17/53`).
- This rule applies to all packets from source IP addresses that are assigned to the country with specified country code (`cc:QQ`).
- This rule does not let any traffic through (`byte-rate 0`) except the packets with IP protocol number 1, 50-51, 6 port 443 and 17 port 53.
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

Example 3 - Rate Limiting rule with ASN

```
fw sam_policy -a d quota source asn:AS64500,cidr:[::FFFF:C0A8:1100]/120 service any pkt-rate 0
```

Explanations:

- This rule drops (`-a d`) all packets that match this rule.
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to packets from the Autonomous System number 64500 (`asn:AS64500`).
- This rule applies to packets from source IPv6 addresses FFFF:C0A8:1100/120 (`cidr:[::FFFF:C0A8:1100]/120`).
- This rule applies to all traffic (`service any`).
- This rule does not let any traffic through (`pkt-rate 0`).
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

Example 4 - Rate Limiting rule with an Allow List

```
fw sam_policy add -a b quota source range:172.16.8.17-172.16.9.121 service 6/80
```

Explanations:

- This rule bypasses (`-a b`) all packets that match this rule.

  Note - The Access Control Policy and other types of security policy rules still apply.
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to packets from the source IP addresses in the range 172.16.8.17 - 172.16.9.121 (`range:172.16.8.17-172.16.9.121`).
- This rule applies to packets sent to TCP port 80 (`service 6/80`).
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

Example 5 - Rate Limiting rule with tracking

```
fw sam_policy add -a d quota service any source-negated true source cc:QQ concurrent-conns-ratio 655 track source
```

Explanations:

- This rule drops (`-a d`) all packets that match this rule.
- This rule does not log any packets (the `-l r` parameter is not specified).
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to all traffic (`service any`).
- This rule applies to all sources except (`source-negated true`) the source IP addresses that are assigned to the country with specified country code (`cc:QQ`).
- This rule limits the maximal number of concurrent active connections to 655/65536=~1% (`concurrent-conns-ratio 655`) for any traffic (`service any`) except (`service-negated true`) the connections from the source IP addresses that are assigned to the country with specified country code (`cc:QQ`).
- This rule counts connections, packets, and bytes for traffic only from sources that match this rule, and not cumulatively for this rule.
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

fw sam_policy batch

Description

The "*fw sam_policy batch*" and "*fw6 sam_policy batch*" commands:

- Add and delete many Suspicious Activity Monitoring (SAM) rules at a time.
- Add and delete many Rate Limiting rules at a time.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Procedure

1. **Start the batch mode**

   - For IPv4, run:

     ```
     fw sam_policy batch << EOF
     ```

   - For IPv6, run:

     ```
     fw6 sam_policy batch << EOF
     ```

2. **Enter the applicable commands**

   - Enter one "`add`" or "`del`" command on each line, on as many lines as necessary.

     Start each line with only "`add`" or "`del`" parameter (not with "`fw samp`").
   - Use the same set of parameters and values as described in these commands:
     - `fw sam_policy add`
     - `fw sam_policy del`
   - Terminate each line with a Return (ASCII 10 - Line Feed) character (press Enter).

3. **End the batch mode**

   Type `EOF` and press Enter.

Example of a Rate Limiting rule for IPv4

```
[Expert@HostName]# fw samp batch <<EOF

add -a d -l r -t 3600 -c "Limit\ conn\ rate\ to\ 5\ conn/sec from\ these\ sources" quota service
any source range:172.16.7.13-172.16.7.13 new-conn-rate 5

del <501f6ef0,00000000,cb38a8c0,0a0afffe>

add -a b quota source range:172.16.8.17-172.16.9.121 service 6/80

EOF
[Expert@HostName]#
```

fw sam_policy del

Description

The "*fw sam_policy del*" and "*fw6 sam_policy del*" commands:

- Delete one configured Suspicious Activity Monitoring (SAM) rule at a time.
- Delete one configured Rate Limiting rule at a time.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax for IPv4

```
fw [-d] sam_policy del '<Rule UID>'
```

Syntax for IPv6

```
fw6 [-d] sam_policy del '<Rule UID>'
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`'<Rule UID>'`	Specifies the UID of the rule you wish to delete. **Important:** ■ The quote marks and angle brackets (`'<...>'`) are mandatory. ■ To see the Rule UID, run the "`fw sam_policy get`" command.

Procedure

1. **List all the existing rules in the Suspicious Activity Monitoring policy database**

   List all the existing rules in the Suspicious Activity Monitoring policy database.

   - For IPv4, run:

     ```
     fw sam_policy get
     ```

   - For IPv6, run:

     ```
     fw6 sam_policy get
     ```

   The rules show in this format:

   ```
   operation=add uid=<Value1,Value2,Value3,Value4> target=...
   timeout=... action=... log= ... name= ... comment=...
   originator= ... src_ip_addr=... req_tpe=...
   ```

   Example for IPv4:

   ```
   operation=add uid=<5ac3965f,00000000,3403a8c0,0000264a>
   target=all timeout=300 action=notify log=log name=Test\ Rule
   comment=Notify\ about\ traffic\ from\ 1.1.1.1
   originator=John\ Doe src_ip_addr=1.1.1.1 req_tpe=ip
   ```

2. **Delete a rule from the list by its UID**

   - For IPv4, run:

     ```
     fw [-d] sam_policy del '<Rule UID>'
     ```

   - For IPv6, run:

     ```
     fw6 [-d] sam_policy del '<Rule UID>'
     ```

   Example for IPv4:

   ```
   fw samp del '<5ac3965f,00000000,3403a8c0,0000264a>'
   ```

3. **Add the flush-only rule**

   - For IPv4, run:

     ```
     fw samp add -t 2 quota flush true
     ```

   - For IPv6, run:

     ```
     fw6 samp add -t 2 quota flush true
     ```

   Explanation:

   The "`fw samp del`" and "`fw6 samp del`" commands only remove a rule from the persistent database. The Security Gateway continues to enforce the deleted rule until the next time you compiled and load a policy. To force the rule deletion immediately, you must enter a flush-only rule right after the "`fw samp del`" and "`fw6 samp del`" command. This flush-only rule immediately deletes the rule you specified in the previous step, and times out in 2 seconds.

   Best Practice - Specify a short timeout period for the flush-only rules. This prevents accumulation of rules that are obsolete in the database.

fw sam_policy get

Description

The "*fw sam_policy get*" and "*fw6 sam_policy get*" commands:

- Show all the configured Suspicious Activity Monitoring (SAM) rules.
- Show all the configured Rate Limiting rules.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax for IPv4

```
fw [-d] sam_policy get [-l] [-u '<Rule UID>'] [-k '<Key>' -t
<Type> [+{-v '<Value>'}] [-n]]
```

Syntax for IPv6

```
fw6 [-d] sam_policy get [-l] [-u '<Rule UID>'] [-k '<Key>' -t
<Type> [+{-v '<Value>'}] [-n]]
```

Parameters

Note - All these parameters are optional.

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-l`	Controls how to print the rules: ■ In the default format (without "`-l`"), the output shows each rule on a separate line. ■ In the list format (with "`-l`"), the output shows each parameter of a rule on a separate line. ■ See the "`fw sam_policy add`" command.
`-u '<`*`Rule UID`*`>'`	Prints the rule specified by its Rule UID or its zero-based rule index. The quote marks and angle brackets ('<...>') are mandatory.
`-k '<`*`Key`*`>'`	Prints the rules with the specified predicate key. The quote marks are mandatory.
`-t <`*`Type`*`>`	Prints the rules with the specified predicate type. For Rate Limiting rules, you must always use "`-t in`".
`+{-v '<`*`Value`*`>'}`	Prints the rules with the specified predicate values. The quote marks are mandatory.
`-n`	Negates the condition specified by these predicate parameters: ■ `-k` ■ `-t` ■ `+-v`

Examples

Example 1 - Output in the default format

```
[Expert@HostName:0]# fw samp get

operation=add uid=<5ac3965f,00000000,3403a8c0,0000264a> target=all timeout=300 action=notify
log=log name=Test\ Rule comment=Notify\ about\ traffic\ from\ 1.1.1.1 originator=John\ Doe
src_ip_addr=1.1.1.1 req_tpe=ip
```

Example 2 - Output in the list format

```
[Expert@HostName:0]# fw samp get -l

uid
<5ac3965f,00000000,3403a8c0,0000264a>
target
all
timeout
2147483647
action
notify
log
log
name
Test\ Rule
comment
Notify\ about\ traffic\ from\ 1.1.1.1
originator
John\ Doe
src_ip_addr
1.1.1.1
req_type
ip
```

Example 3 - Printing a rule by its Rule UID

```
[Expert@HostName:0]# fw samp get -u '<5ac3965f,00000000,3403a8c0,0000264a>'
0
operation=add uid=<5ac3965f,00000000,3403a8c0,0000264a> target=all timeout=300 action=notify
log=log name=Test\ Rule comment=Notify\ about\ traffic\ from\ 1.1.1.1 originator=John\ Doe
src_ip_addr=1.1.1.1 req_tpe=ip
```

Example 4 - Printing rules that match the specified filters

```
[Expert@HostName:0]# fw samp get
no corresponding SAM policy requests
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a d -l r -t 3600 quota service any source
range:172.16.7.11-172.16.7.13 new-conn-rate 5 flush true
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a n -l r quota service 1,50-51,6/443,17/53 service-negated
true source cc:QQ byte-rate 0
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a b quota source range:172.16.8.17-172.16.9.121 service
6/80
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a d quota service any source-negated true source cc:QQ
concurrent-conns-ratio 655 track source
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get
operation=add uid=<5bab3acf,00000000,3503a8c0,00003ddc> target=all timeout=indefinite
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
operation=add uid=<5bab3ac6,00000000,3503a8c0,00003dbf> target=all timeout=3586 action=drop
log=log service=any source=range:172.16.7.11-172.16.7.13 new-conn-rate=5 flush=true req_
type=quota
operation=add uid=<5bab3acc,00000000,3503a8c0,00003dd7> target=all timeout=indefinite
action=bypass source=range:172.16.8.17-172.16.9.121 service=6/80 req_type=quota
operation=add uid=<5bab3ac9,00000000,3503a8c0,00003dd5> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'service' -t in -v '6/80'
operation=add uid=<5bab3acc,00000000,3503a8c0,00003dd7> target=all timeout=indefinite
action=bypass source=range:172.16.8.17-172.16.9.121 service=6/80 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'service-negated' -t in -v 'true'
operation=add uid=<5bab3ac9,00000000,3503a8c0,00003dd5> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'source' -t in -v 'cc:QQ'
operation=add uid=<5bab3acf,00000000,3503a8c0,00003ddc> target=all timeout=indefinite
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
operation=add uid=<5bab3ac9,00000000,3503a8c0,00003dd5> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k source -t in -v 'cc:QQ' -n
operation=add uid=<5bab3ac6,00000000,3503a8c0,00003dbf> target=all timeout=3291 action=drop
log=log service=any source=range:172.16.7.11-172.16.7.13 new-conn-rate=5 flush=true req_
type=quota
operation=add uid=<5bab3acc,00000000,3503a8c0,00003dd7> target=all timeout=indefinite
action=bypass source=range:172.16.8.17-172.16.9.121 service=6/80 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'source-negated' -t in -v 'true'
operation=add uid=<5baa94e0,00000000,860318ac,00003016> target=all timeout=indefinite
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'byte-rate' -t in -v '0'
operation=add uid=<5baa9431,00000000,860318ac,00002efd> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'flush' -t in -v 'true'
operation=add uid=<5baa9422,00000000,860318ac,00002eea> target=all timeout=2841 action=drop
log=log service=any source=range:172.16.7.11-172.16.7.13 new-conn-rate=5 flush=true req_
type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'concurrent-conns-ratio' -t in -v '655'
operation=add uid=<5baa94e0,00000000,860318ac,00003016> target=all timeout=indefinite
```

```
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
[Expert@HostName:0]#
```

fwm

Description

Performs various management operations and shows various management information.

Notes:

- For debug instructions, see the description of the `fwm` process in sk97638.
- On a Multi-Domain Server, you must run these commands in the context of the applicable Domain Management Server.

Syntax

```
fwm [-d]
      dbload <options>
      exportcert <options>
      fetchfile <options>
      fingerprint <options>
      getpcap <options>
      ikecrypt <options>
      load [<options>]
      logexport <options>
      mds <options>
      printcert <options>
      sic_reset
      snmp_trap <options>
      unload [<options>]
      ver [<options>]
      verify <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.

Parameter	Description
`dbload <options>`	Downloads the user database and network objects information to the specified targets See *"fwm dbload" on page 333*.
`exportcert <options>`	Export a SIC certificate of the specified object to file. See *"fwm exportcert" on page 334*.
`fetchfile <options>`	Fetches a specified OPSEC configuration file from the specified source server. See *"fwm fetchfile" on page 335*.
`fingerprint <options>`	Shows the Check Point fingerprint. See *"fwm fingerprint" on page 337*.
`getpcap <options>`	Fetches the IPS packet capture data from the specified Security Gateway. See *"fwm getpcap" on page 339*.
`ikecrypt <options>`	Encrypts a secret with a key. See *"fwm ikecrypt" on page 341*.
`load <options>`	This command is obsolete for R80 and higher. Use the *"mgmt_cli" on page 386* command to load a policy to a managed Security Gateway. See *"fwm load" on page 342*.
`logexport <options>`	Exports a Security log file (`$FWDIR/log/*.log`) or Audit log file (`$FWDIR/log/*.adtlog`) to an ASCII file. See *"fwm logexport" on page 343*.
`mds <options>`	Shows information and performs various operations on Multi-Domain Server. See *"fwm mds" on page 348*.
`printcert <options>`	Shows a SIC certificate's details. See *"fwm printcert" on page 350*.
`sic_reset`	Resets SIC on the Management Server. See *"fwm sic_reset" on page 356*.
`snmp_trap <options>`	Sends an SNMP Trap to the specified host. See *"fwm snmp_trap" on page 357*.
`unload <options>`	Unloads the policy from the specified managed Security Gateways. See *"fwm unload" on page 360*.

Parameter	Description
`ver <options>`	Shows the Check Point version of the Management Server. See *"fwm ver" on page 364*.
`verify <options>`	This command is obsolete for R80 and higher. Use the *"mgmt_cli" on page 386* command to verify a policy. See *"fwm verify" on page 365*.

fwm dbload

Description

Copies the user database and network objects information to specified managed servers with one or more **Management** Software Blades enabled.

Important - This command is obsolete for R80 and higher.
Use the API command "`install-database`" to install the database on the applicable servers.
See the *Check Point Management API Reference* (at the top, select the correct version) .

fwm exportcert

Description

Export a SIC certificate of the specified managed object to a file.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] exportcert -obj <Name of Object> -cert <Name of CA> -file
<Output File> [-withroot] [-pem]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
<Name of Object>	Specifies the name of the managed object, whose certificate you wish to export.
<Name of CA>	Specifies the name of Certificate Authority, whose certificate you wish to export.
<Output File>	Specifies the name of the output file.
`-withroot`	Exports the certificate's root in addition to the certificate's content.
`-pem`	Save the exported information in a text file. Default is to save in a binary file.

fwm fetchfile

Description

Fetches a specified OPSEC configuration file from the specified source server.

This command supports only the `fwopsec.conf` or `fwopsec.v4x` files.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] fetchfile -r <File> [-d <Local Path>] <Source>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-r <File>`	Specifies the relative `fw1` directory. This command supports only these files: ■ `conf/fwopsec.conf` ■ `conf/fwopsec.v4x`
`-d <Local Path>`	Specifies the local directory to save the fetched file.
`<Source>`	Specifies the managed remote source server, from which to fetch the file. **Note** - The local and the remote source servers must have established SIC trust.

Example

```
[Expert@MGMT:0]# fwm fetchfile -r "conf/fwopsec.conf" -d /tmp 192.168.3.52
Fetching conf/fwopsec.conf from 192.168.3.52...
Done
[Expert@MGMT:0]#
```

fwm fingerprint

Description

Shows the Check Point fingerprint.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] fingerprint [-d]
      <IP address of Target> <SSL Port>
      localhost <SSL Port>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. The debug options are: ■ `fwm -d` Runs the complete debug of all `fwm` actions. For complete debug instructions, see the description of the `fwm` process in sk97638. ■ `fingerprint -d` Runs the debug only for the fingerprint actions.
<IP address of Target>	Specifies the IP address of a remote managed server.
<SSL Port>	Specifies the SSL port number. The default is 443.

Example 1 - Showing the fingerprint on the local Management Server

```
[Expert@MGMT:0]# fwm fingerprint localhost 443
#DN OID.1.2.840.113549.1.9.2=An optional company name,Email=Email
Address,CN=192.168.3.51,L=Locality Name (eg\, city)
#FINGER 11:A6:F7:1F:B9:F5:15:BC:F9:7B:5F:DC:28:FC:33:C5
##
[Expert@MGMT:0]#
```

Example 2 - Showing the fingerprint from a managed Security Gateway

```
[Expert@MGMT:0]# fwm fingerprint 192.168.3.52 443
#DN OID.1.2.840.113549.1.9.2=An optional company name,Email=Email
Address,CN=192.168.3.52,L=Locality Name (eg\, city)
#FINGER 5C:8E:4D:B9:B4:3A:58:F3:79:18:F1:70:99:8B:5F:2B
##
[Expert@MGMT:0]#
```

fwm getpcap

Description

Fetches the IPS packet capture data from the specified Security Gateway.

This command only works with IPS packet captures stored on the Security Gateway in the `$FWDIR/log/captures_repository/` directory.

This command does not work with other Software Blades, such as Anti-Bot and Anti-Virus that store packet captures in the `$FWDIR/log/blob/` directory on the Security Gateway.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] getpcap -g <Security Gateway> -u '{<Capture UID>}' -p
<Local Path>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`-g <Security Gateway>`	Specifies the main IP address or Name of Security Gateway object as configured in SmartConsole.
`-u '{<Capture UID>}'`	Specifies the Unique ID of the packet capture file. To see the Unique ID of the packet capture file, open the applicable log file in **SmartConsole > Logs & Monitor > Logs**.
`-p <Local Path>`	Specifies the local path to save the specified packet capture file. If you do not specify the local directory explicitly, the command saves the packet capture file in the current working directory.

Example

```
[Expert@MGMT:0]# fwm getpcap -g 192.168.162.1 -u '{0x4d79dc02,0x10000,0x220da8c0,0x1ffff}'
/var/log/
[Expert@MGMT:0]#
```

fwm ikecrypt

Description

Encrypts the password of an Endpoint VPN Client user using IKE. The resulting string must then be stored in the LDAP database.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] ikecrypt <Key> <Password>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
<Key>	Specifies the IKE Key as defined in the **LDAP Account Unit** properties window on the **Encryption** tab.
<Password>	Specifies the password for the Endpoint VPN Client user.

Example

```
[Expert@MGMT:0]# fwm ikecrypt MySecretKey MyPassword
OUQJHiNHCj6HJGH8ntnKQ7tg
[Expert@MGMT:0]#
```

fwm load

Description

Loads a policy on a managed Security Gateway.

Important - This command is obsolete for R80 and higher.
Use the API command "`install-policy`" to load a policy on a managed Security Gateway.
See the *Check Point Management API Reference* (at the top, select the correct version) .

fwm logexport

Description

Exports a Security log file (`$FWDIR/log/*.log`) or Audit log file (`$FWDIR/log/*.adtlog`) to an ASCII file.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm logexport -h
```

```
fwm [-d] logexport [{-d <Delimiter> | -s}] [-t <Table Delimiter>]
[-i <Input File>] [-o <Output File>] [{-f | -e}] [-x <Start Entry
Number>] [-y <End Entry Number>] [-z] [-n] [-p] [-a] [-u
<Unification Scheme File>] [-m {initial | semi | raw}]
```

Parameters

Parameter	Description
`-h`	Shows the built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`-d <Delimiter> | -s`	Specifies the output delimiter between fields of log entries: ■ `-d <Delimiter>` - Uses the specified delimiter. ■ `-s` - Uses the ASCII character #255 (non-breaking space) as the delimiter. **Note** - If you do not specify the delimiter explicitly, the default is a semicolon (`;`).

Parameter	Description
`-t <Table Delimiter>`	Specifies the output delimiter inside table field. Table field would look like: *ROWx:COL0,ROWx:COL1,ROWx:COL2*, and so on **Note** - If you do not specify the table delimiter explicitly, the default is a comma (`,`).
`-i <Input File>`	Specifies the name of the input log file. **Notes:** ■ This command supports only Security log file (`$FWDIR/log/*.log`) and Audit log file (`$FWDIR/log/*.adtlog`) ■ If you do not specify the input log file explicitly, the command processes the active Security log file `$FWDIR/log/fw.log`
`-o <Output File>`	Specifies the name of the output file. **Note** - If you do not specify the output log file explicitly, the command prints its output on the screen.
`-f`	After reaching the end of the currently opened log file, specifies to continue to monitor the log file indefinitely and export the new entries as well. **Note** - Applies only to the *active* log file: `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`
`-e`	After reaching the end of the currently opened log file, continue to monitor the log file indefinitely and export the new entries as well. **Note** - Applies only to the *active* log file: `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`
`-x <Start Entry Number>`	Starts exporting the log entries from the specified log entry number and below, counting from the beginning of the log file.
`-y <End Entry Number>`	Starts exporting the log entries until the specified log entry number, counting from the beginning of the log file.
`-z`	In case of an error (for example, wrong field value), specifies to continue the export of log entries. The default behavior is to stop.
`-n`	Specifies not to perform DNS resolution of the IP addresses in the log file (this is the default behavior). This significantly speeds up the log processing.

Parameter	Description
`-p`	Specifies to not to perform resolution of the port numbers in the log file (this is the default behavior). This significantly speeds up the log processing.
`-a`	Exports only Account log entries.
`-u <`*`Unification Scheme File`*`>`	Specifies the path and name of the log unification scheme file. The default log unification scheme file is: `$FWDIR/conf/log_unification_scheme.C`
`-m {initial | semi | raw}`	Specifies the log unification mode: ■ `initial` - Complete unification of log entries. The command exports one unified log entry for each ID. This is the default. If you also specify the "`-f`" parameter, then the output does not export any updates, but exports only entries that relate to the start of new connections. To export updates as well, use the "`semi`" parameter. ■ `semi` - Step-by-step unification of log entries. For each log entry, exports entry that unifies this entry with all previously encountered entries with the same ID. ■ `raw` - No log unification. Exports all log entries.

The output of the `fwm logexport` command appears in tabular format.

The first row lists the names of all log fields included in the log entries.

Each of the next rows consists of a single log entry, whose fields are sorted in the same order as the first row.

If a log entry has no information in a specific field, this field remains empty (as indicated by two successive semi-colons "`;;`").

You can control which log fields appear in the output of the command output:

Step	Instructions
1	Create the `$FWDIR/conf/logexport.ini` file: `[Expert@MGMT:0]# touch $FWDIR/conf/logexport.ini`
2	Edit the `$FWDIR/conf/logexport.ini` file: `[Expert@MGMT:0]# vi $FWDIR/conf/logexport.ini`

3	To include or exclude the log fields from the output, add these lines in the configuration file:
	`[Fields_Info]`
	`included_fields = field1,field2,field3,<REST_OF_FIELDS>,field100`
	`excluded_fields = field10,field11`
	Where:
	■ You can specify only the `included_fields` parameter, only the `excluded_fields` parameter, or both.
	■ The `num` field must always appear first. You cannot manipulate this field.
	■ The `<REST_OF_FIELDS>` is an optional reserved token that refers to a list of fields.
	• If you specify the "`-f`" parameter, then the `<REST_OF_FIELDS>` is based on a list of fields from the `$FWDIR/conf/logexport_default.C` file.
	• If you do not specify the "`-f`" parameter, then the `<REST_OF_FIELDS>` is based on the input log file.

4	Save the changes in the file and exit the Vi editor.
5	Export the logs: `fwm logexport <options>`

Example 1 - Exporting all log entries

```
[Expert@MGMT:0]# fwm logexport -i MySwitchedLog.log
Starting... There are 113 log records in the file
num;date;time;orig;type;action;alert;i/f_name;i/f_dir;product;LogId;ContextNum;origin_
id;ContentVersion;HighLevelLogKey;SequenceNum;log_sys_message;ProductFamily;fg-1_client_in_rule_
name;fg-1_client_out_rule_name;fg-1_server_in_rule_name;fg-1_server_out_rule_
name;description;status;version;comment;update_service;reason;Severity;failure_impact
0;13Jun2018;19:47:54;CXL1_192.168.3.52;control; ;;daemon;inbound;VPN-1 & FireWall-1;-1;-
1;CN=CXL1_192.168.3.52,O=MyDomain_Server.checkpoint.com.s6t98x;5;18446744073709551615;2;Log file
has been switched to: MyLog.log;Network;;;;;;;;;;;
1;13Jun2018;19:47:54;CXL1_192.168.3.52;account;accept;;;inbound;FG;-1;-1;CN=CXL1_
192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;Default;Default;;;;;;;;;
... ...
35;13Jun2018;19:55:59;CXL1_192.168.3.52;account;accept;;;inbound;FG;-1;-1;CN=CXL1_
192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;Default;Default;Host
Redirect;;;;;;;;;
36;13Jun2018;19:56:06;CXL1_192.168.3.52;control; ;;;inbound;Security Gateway/Management;-1;-
1;CN=CXL1_192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;;;;;Contracts;Started;1.0;<null>
;1;;;
... ...
47;13Jun2018;19:57:02;CXL1_192.168.3.52;control; ;;;inbound;Security Gateway/Management;-1;-
1;CN=CXL1_192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;;;;;Contracts;Failed;1.0;;1;Could
not reach "https://productcoverage.checkpoint.com/ProductCoverageService". Check DNS and Proxy
configuration on the gateway.;2;Contracts may be out-of-date
... ...
[Expert@MGMT:0]#
```

Example 2 - Exporting only log entries with specified numbers

```
[Expert@MGMT:0]# fwm logexport -i MySwitchedLog.log -x 36 -y 47
Starting... There are 113 log records in the file
num;date;time;orig;type;action;alert;i/f_name;i/f_dir;product;LogId;ContextNum;origin_
id;ContentVersion;HighLevelLogKey;SequenceNum;log_sys_message;ProductFamily;fg-1_client_in_rule_
name;fg-1_client_out_rule_name;fg-1_server_in_rule_name;fg-1_server_out_rule_
name;description;status;version;comment;update_service;reason;Severity;failure_impact
36;13Jun2018;19:56:06;CXL1_192.168.3.52;control; ;;;inbound;Security Gateway/Management;-1;-
1;CN=CXL1_192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;;;;;Contracts;Started;1.0;<null>
;1;;;
37;13Jun2018;19:56:06;CXL1_192.168.3.52;account;accept;;;inbound;FG;-1;-1;CN=CXL1_
192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;2;;Network;Default;Default;Host
Redirect;;;;;;;;;
... ...
46;13Jun2018;19:56:59;CXL1_192.168.3.52;account;accept;;;inbound;FG;-1;-1;CN=CXL1_
192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;Default;Default;Host
Redirect;;;;;;;;;
47;13Jun2018;19:57:02;CXL1_192.168.3.52;control; ;;;inbound;Security Gateway/Management;-1;-
1;CN=CXL1_192.168.3.52,O=MyDomain_
Server.checkpoint.com.s6t98x;5;18446744073709551615;1;;Network;;;;;Contracts;Failed;1.0;;1;Could
not reach "https://productcoverage.checkpoint.com/ProductCoverageService". Check DNS and Proxy
configuration on the gateway.;2;Contracts may be out-of-date
[Expert@MGMT:0]#
```

fwm mds

Description

- Shows the Check Point version of the Multi-Domain Server.
- Rebuilds status tree for Global VPN Communities.

Note - On a Multi-Domain Server, you can run this command:

- In the context of the MDS:

```
mdsenv
```

- In the context of a Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] mds
      ver
      rebuild_global_communities_status {all | missing}
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`ver`	Shows the Check Point version of the Multi-Domain Server.
`rebuild_global_communities_status`	Rebuilds status tree for Global VPN Communities: ■ `all` - Rebuilds status tree for all Global VPN Communities. ■ `missing` - Rebuild status tree only for Global VPN Communities that do not have status trees.

Example

```
[Expert@MDS:0]# fwm mds ver
This is Check Point Multi-Domain Security Management R81.20 -
Build 11
[Expert@MDS:0]#
```

fwm printcert

Description

Shows a SIC certificate's details.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] printcert
      -obj <Name of Object> [-cert <Certificate Nick Name>] [-
verbose]
      -ca <CA Name> [-x509 <Name of File> [-p]] [-verbose]
      -f <Name of Binary Certificate File> [-verbose]
```

Parameters

Item	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`-obj <Name of Object>`	Specifies the name of the managed object, for which to show the SIC certificate information.
`-cert <Certificate Nick Name>`	Specifies the certificate nick name.
`-ca <CA Name>`	Specifies the name of the Certificate Authority. **Note** - Check Point CA Name is `internal_ca`.
`-x509 <Name of File>`	Specifies the name of the X.509 file.
`-p`	Specifies to show the SIC certificate as a text file.
`-f <Name of Binary Certificate File>`	Specifies the binary SIC certificate file to show.
`-verbose`	Shows the information in verbose mode.

Examples

Example 1 - Showing the SIC certificate of a Management Server

```
[Expert@MGMT:0]# fwm printcert -ca internal_ca
Subject: O=MGMT.checkpoint.com.s6t98x
Issuer: O=MGMT.checkpoint.com.s6t98x
Not Valid Before: Sun Apr 8 13:41:00 2018 Local Time
Not Valid After: Fri Jan 1 05:14:07 2038 Local Time
Serial No.: 1
Public Key: RSA (2048 bits)
Signature: RSA with SHA256
Key Usage:
        digitalSignature
        keyCertSign
        cRLSign
Basic Constraint:
        is CA
MD5 Fingerprint:
   7B:F9:7B:4C:BD:40:B9:1C:AB:2C:AE:CF:66:2E:E7:06
SHA-1 Fingerprints:
1. A6:43:3A:2B:1A:04:7F:A6:36:A6:2C:78:BF:22:D9:BC:F7:7E:4D:73
2. KEYS HEM GERM PIT ABUT ROVE RAW PA IQ FAWN NUT SLAM
[Expert@MGMT:0]#
```

Example 2 - Showing the SIC certificate of a Management Server in verbose mode

```
[Expert@MGMT:0]# fwm printcert -ca internal_ca -verbose
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] fwa_db_init: called
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] fwa_db_init: closing existing database
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] do_links_getver: strncmp failed. Returning -2
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] db_fetchkey: entering
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] PubKey:
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] Modulus:
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] ae b3 75 36 64 e4 1a 40 fe c2 ad 2f 9b 83 0b 45
f1 00 04 bc
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 3f 77 77 76 d1 de 8a cf 9f 32 78 8b d4 b1 b4 be
db 75 cc c8
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] c2 6d ff 3e aa fe f1 2b c3 0a b0 a2 a5 e0 a8 ab
45 cd 87 32
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] ac c6 9f a4 a9 ba 30 79 08 fa 59 4c d2 dc 3d 36
ca 17 d7 c1
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] b2 a2 41 f5 89 0f 00 d4 2d f2 55 d2 30 a5 32 c7
46 7a 6b 32
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 29 0f 53 9f 35 42 91 e5 7d f7 30 6d bc b3 f2 ae
f3 f0 ed 88
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] c4 d7 7d 0c 2d f6 5f c8 ed 9f 9a 57 54 79 d0 0f
0b 2f 9c 0d
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 94 2e f0 f4 66 62 f7 ae 2e f8 8e 90 08 ba 63 85
b6 46 2f b7
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] a7 01 29 9a 14 58 a8 ef eb 07 17 4e 95 8b 2f 48
5f d3 18 10
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 3f 00 d5 03 d7 fd 45 45 ca 67 5b 34 be b8 00 ae
ea 9a cd 50
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] d6 e7 a2 81 86 78 11 d7 bf 04 9f 8b 43 3f f7 36
5f ed 31 a8
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] a3 9d 8b 0a de 05 fb 5c 44 2e 29 e3 3e f4 dd 50
01 0f 86 9d
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] 55 16 a3 4d f8 90 2d 13 c6 c1 28 57 f8 3e 7c 59
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] Exponent: 65537 (0x10001)
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52]
X509 Certificate Version 3
refCount: 1
Serial Number: 1
Issuer: O=MGMT.checkpoint.com.s6t98x
Subject: O=MGMT.checkpoint.com.s6t98x
Not valid before: Sun Apr 8 13:41:00 2018 Local Time
Not valid after: Fri Jan 1 05:14:07 2038 Local Time
Signature Algorithm: RSA with SHA-256 Public key: RSA (2048 bits)
Extensions:
        Key Usage:
                digitalSignature
                keyCertSign
                cRLSign
        Basic Constraint (Critical):
                is CA

[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] destroy_rand_mutex: destroy
[FWM 24304 4024166304]@MGMT[12 Jun 20:21:52] cpKeyTaskManager::~cpKeyTaskManager: called.
[Expert@MGMT:0]#
```

Example 3 - Showing the SIC certificate of a managed Cluster object

```
[Expert@MGMT:0]# fwm printcert -obj CXL_192.168.3.244

printing all certificates of CXL_192.168.3.244

defaultCert:
Host Certificate (level 0):
Subject: CN=CXL_192.168.3.244 VPN Certificate,O=MGMT.checkpoint.com.s6t98x
Issuer: O=MGMT.checkpoint.com.s6t98x
Not Valid Before: Sun Jun 3 19:58:19 2018 Local Time
Not Valid After: Sat Jun 3 19:58:19 2023 Local Time
Serial No.: 85021
Public Key: RSA (2048 bits)
Signature: RSA with SHA256
Subject Alternate Names:
        IP Address: 192.168.3.244
CRL distribution points:
        http://192.168.3.240:18264/ICA_CRL2.crl
        CN=ICA_CRL2,O=MGMT.checkpoint.com.s6t98x
Key Usage:
        digitalSignature
        keyEncipherment
Basic Constraint:
        not CA
MD5 Fingerprint:
   B1:15:C7:A8:2A:EE:D1:75:92:9F:C7:B4:B9:BE:42:1B
SHA-1 Fingerprints:
1. BC:7A:D9:E2:CD:29:D1:9E:F0:39:5A:CD:7E:A9:0B:F9:6A:A7:2B:85
2. MIRE SANK DUSK HOOD HURD RIDE TROY QUAD LOVE WOOD GRIT WITH


               *****
[Expert@MGMT:0]#
```

Example 4 - Showing the SIC certificate of a managed Cluster object in verbose mode

```
[Expert@MGMT:0]# fwm printcert -obj CXL_192.168.3.244 -verbose
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] fwa_db_init: called
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] fwa_db_init: closing existing database
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] do_links_getver: strncmp failed. Returning -2

printing all certificates of CXL_192.168.3.244

[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] db_fetchkey: entering
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] 1 certificates
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] PubKey:
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] Modulus:
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] df 35 c3 45 ca 42 16 6e 21 9e 31 af c1 fd 20 0a
3d 5b 6f 5d
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] e0 a2 0c 0e fa fa 5e e5 91 9d 4e 73 77 fa db 86
0b 5e 5d 0c
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] ce af 4a a4 7b 30 ed b0 43 7d d8 93 c5 4b 01 f4
3d b5 d8 f4
... ... ...
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] 34 b1 db ac 18 4f 11 bd d2 fb 26 7d 23 74 5c d9
00 a1 58 1e
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] 60 7c 83 44 fa 1e 1e 86 fa ad 98 f7 df 24 4a 21
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] Exponent: 65537 (0x10001)
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45]
X509 Certificate Version 3
refCount: 1
Serial Number: 85021
Issuer: O=MGMT.checkpoint.com.s6t98x
Subject: CN=CXL_192.168.3.244 VPN Certificate,O=MGMT.checkpoint.com.s6t98x
Not valid before: Sun Jun 3 19:58:19 2018 Local Time
Not valid after: Sat Jun 3 19:58:19 2023 Local Time
Signature Algorithm: RSA with SHA-256 Public key: RSA (2048 bits)
Extensions:
        Key Usage:
                digitalSignature
                keyEncipherment
        Subject Alternate names:
                IP: 192.168.3.244
        Basic Constraint:
                not CA
        CRL distribution Points:
                URI: http://192.168.3.240:18264/ICA_CRL2.crl
                DN: CN=ICA_CRL2,O=MGMT.checkpoint.com.s6t98x

defaultCert:

[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] destroy_rand_mutex: destroy
[FWM 24665 4023814048]@MGMT[12 Jun 20:26:45] cpKeyTaskManager::~cpKeyTaskManager: called.
                *****
[Expert@MGMT:0]#
```

fwm sic_reset

Description

Resets SIC on the Management Server.

For detailed procedure, see sk65764: How to reset SIC.

Warning:

- **Before you run this command, take a Gaia Snapshot and a full backup of the Management Server.**
  This command resets SIC between the Management Server and all its managed objects.
- **This operation breaks trust in all Internal CA certificates and SIC trust across the managed environment.**
  Therefore, we do not recommend it at all, except for real disaster recovery.

Note
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] sic_reset
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.

fwm snmp_trap

Description

Sends an SNMPv1 Trap to the specified host.

Notes:

- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

- On a Multi-Domain Server, the SNMP Trap packet is sent from the IP address of the Leading Interface.

Syntax

```
fwm [-d] snmp_trap [-v <SNMP OID>] [-g <Generic Trap Number>] [-s
<Specific Trap Number>] [-p <Source Port>] [-c <SNMP Community>]
<Target> ["<Message>"]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`-v <SNMP OID>`	Specifies an optional SNMP OID to bind with the message.
`-g <Generic Trap Number>`	Specifies the generic trap number. One of these values: ■ 0 - For `coldStart` trap ■ 1 - For `warmStart` trap ■ 2 - For `linkDown` trap ■ 3 - For `linkUp` trap ■ 4 - For `authenticationFailure` trap ■ 5 - For `egpNeighborLoss` trap ■ 6 - For `enterpriseSpecific` trap (this is the default value)
`-s <Specific Trap Number>`	Specifies the unique trap type. Valid only of generic trap value is 6 (for `enterpriseSpecific`). Default value is 0.
`-p <Source Port>`	Specifies the source port, from which to send the SNMP Trap packets.
`-c <SNMP Community>`	Specifies the SNMP community.
`<Target>`	Specifies the managed target host, to which to send the SNMP Trap packets. Enter an IP address of a resolvable hostname.
`"<Message>"`	Specifies the SNMP Trap text message.

Example - Sending an SNMP Trap from a Management Server and capturing the traffic on the Security Gateway

```
[Expert@MGMT:0]# fwm snmp_trap -g 2 -c public 192.168.3.52 "My Trap Message"
[Expert@MGMT:0]#

[Expert@MyGW_192.168.3.52:0]# tcpdump -s 1500 -vvvv -i eth0 udp and host 192.168.3.51
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 1500 bytes
22:49:43.891287 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto: UDP (17), length: 103)
192.168.3.51.53450 > MyGW_192.168.3.52.snmptrap: [udp sum ok] { SNMPv1 { Trap(58) E:2620.1.1
192.168.3.240 linkDown 1486440 E:2620.1.1.11.0="My Trap Message" } }
Pressed CTRL+C
[Expert@MyGW_192.168.3.52:0]#
```

fwm unload

Description

Unloads the policy from the specified managed Security Gateways or Cluster Members.

Warning:

1. The `fwm unload` command prevents all traffic from passing through the Security Gateway (Cluster Member), because it disables the IP Forwarding in the Linux kernel on the specified Security Gateway (Cluster Member).
2. The `fwm unload` command removes all policies from the specified Security Gateway (Cluster Member).
   This means that the Security Gateway (Cluster Member) accepts all incoming connections destined to all active interfaces without any filtering or protection enabled.

Notes:

- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:
  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```
- If it is necessary to remove the current policy, but keep the Security Gateway (Cluster Member) protected, then run the *"comp_init_policy" on page 965* command on the Security Gateway (Cluster Member).
- To load the policies on the Security Gateway (Cluster Member), run one of these commands on the Security Gateway (Cluster Member), or reboot:
  - *"fw fetch" on page 1119*
  - *"cpstart" on page 1018*
- In addition, see the *"fw unloadlocal" on page 1242* command.

Syntax

```
fwm [-d] unload <GW1> <GW2> ... <GWN>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
<GW1> <GW2> ... <GWN>	Specifies the managed Security Gateways by their main IP address or Object Name as configured in SmartConsole.

Example

```
[Expert@MyGW:0]# cpstat -f policy fw

Product name: Firewall
Policy name: CXL_Policy
Policy install time: Wed Oct 23 18:23:14 2019
... ... ...
[Expert@MyGW:0]#


[Expert@MyGW:0]# sysctl -a | grep forwarding | grep -v bridge
net.ipv6.conf.bond0.forwarding = 1
net.ipv6.conf.eth1.forwarding = 1
net.ipv6.conf.eth3.forwarding = 1
net.ipv6.conf.eth2.forwarding = 1
net.ipv6.conf.eth4.forwarding = 1
net.ipv6.conf.eth5.forwarding = 1
net.ipv6.conf.eth0.forwarding = 1
net.ipv6.conf.eth6.forwarding = 1
net.ipv6.conf.default.forwarding = 1
net.ipv6.conf.all.forwarding = 1
net.ipv6.conf.lo.forwarding = 1
net.ipv4.conf.bond0.mc_forwarding = 0
net.ipv4.conf.bond0.forwarding = 1
net.ipv4.conf.eth1.mc_forwarding = 0
net.ipv4.conf.eth1.forwarding = 1
net.ipv4.conf.eth2.mc_forwarding = 0
net.ipv4.conf.eth2.forwarding = 1
net.ipv4.conf.eth0.mc_forwarding = 0
net.ipv4.conf.eth0.forwarding = 1
net.ipv4.conf.lo.mc_forwarding = 0
net.ipv4.conf.lo.forwarding = 1
net.ipv4.conf.default.mc_forwarding = 0
net.ipv4.conf.default.forwarding = 1
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.all.forwarding = 1
[Expert@MyGW:0]#


[Expert@MGMT:0]# fwm unload MyGW

Uninstalling Policy From: MyGW

 Security Policy successfully uninstalled from MyGW...

Security Policy uninstall complete.

[Expert@MGMT:0]#
```

```
[Expert@MyGW:0]# cpstat -f policy fw

Product name: Firewall
Policy name:
Policy install time:
... ... ...
[Expert@MyGW:0]#


[Expert@MyGW:0]# sysctl -a | grep forwarding | grep -v bridge
net.ipv6.conf.bond0.forwarding = 0
net.ipv6.conf.eth1.forwarding = 0
net.ipv6.conf.eth3.forwarding = 0
net.ipv6.conf.eth2.forwarding = 0
net.ipv6.conf.eth4.forwarding = 0
net.ipv6.conf.eth5.forwarding = 0
net.ipv6.conf.eth0.forwarding = 0
net.ipv6.conf.eth6.forwarding = 0
net.ipv6.conf.default.forwarding = 0
net.ipv6.conf.all.forwarding = 0
net.ipv6.conf.lo.forwarding = 0
net.ipv4.conf.bond0.mc_forwarding = 0
net.ipv4.conf.bond0.forwarding = 0
net.ipv4.conf.eth1.mc_forwarding = 0
net.ipv4.conf.eth1.forwarding = 0
net.ipv4.conf.eth2.mc_forwarding = 0
net.ipv4.conf.eth2.forwarding = 0
net.ipv4.conf.eth0.mc_forwarding = 0
net.ipv4.conf.eth0.forwarding = 0
net.ipv4.conf.lo.mc_forwarding = 0
net.ipv4.conf.lo.forwarding = 0
net.ipv4.conf.default.mc_forwarding = 0
net.ipv4.conf.default.forwarding = 0
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.all.forwarding = 0
[Expert@MyGW:0]#
```

fwm ver

Description

Shows the Check Point version of the Security Management Server.

Note - On a Multi-Domain Server, you can run this command:

- In the context of the MDS:

```
mdsenv
```

- In the context of a Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] ver [-f <Output File>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
`-f <Output File>`	Specifies the name of the output file, in which to save this information.

Example

```
[Expert@MGMT:0]# fwm ver
This is Check Point Security Management Server R81.20 - Build 11
[Expert@MGMT:0]#
```

fwm verify

Important - This command is obsolete for R80 and higher. Use the *"mgmt_cli" on page 386* command to verify a policy on a managed Security Gateway.

Description

Verifies the specified policy package without installing it.

Note
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
fwm [-d] verify <Policy Name>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. For complete debug instructions, see the description of the `fwm` process in sk97638.
<Policy Name>	Specifies the name of the policy package as configured in SmartConsole.

Example

```
[Expert@MGMT:0]# fwm verify Standard
 Verifier messages:
Error: Rule 1 Hides rule 2 for Services & Applications: any .
[Expert@MGMT:0]#
```

inet_alert

Description

Notifies an Internet Service Provider (ISP) when a company's corporate network is under attack. This command forwards log messages generated by the alert daemon on your Check Point Security Gateway to an external Management Station. This external Management Station is usually located at the ISP site. The ISP can then analyze the alert and react accordingly.

This command uses the Event Logging API (ELA) protocol to send the alerts. The Management Station receiving the alert must be running the ELA Proxy.

If communication with the ELA Proxy is to be authenticated or encrypted, a key exchange must be performed between the external Management Station running the ELA Proxy at the ISP site and the Check Point Security Gateway generating the alert.

Procedure

Step	Instructions
1	Connect with SmartConsole to the applicable Security Management Server or Domain Management Server, which manages the applicable Security Gateway that should forward log messages to an external Management Station.
2	From the top left **Menu**, click **Global properties**.
3	Click on the **[+]** near the **Log and Alert** and click **Alerts**.
4	Clear the **Send user defined alert no. 1 to SmartView Monitor**.
5	Select the next option **Run UserDefined script under the above**.
6	Enter the applicable **inet_alert** syntax (see the *Syntax* section below).
7	Click **OK**.
8	Install the Access Control Policy on the applicable Security Gateway.

Syntax

```
inet_alert -s <IP Address> [-o] [-a <Auth Type>] [-p <Port>] [-f
<Token> <Value>] [-m <Alert Type>]
```

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

Parameters

Parameter	Description
`-s <IP Address>`	The IPv4 address of the ELA Proxy (usually located at the ISP site).
`-o`	Prints the alert log received to `stdout`. Use this option when `inet_alert` is part of a pipe syntax (`<some command> | inet_alert ...`).
`-a <Auth Type>`	Specifies the type of connection to the ELA Proxy. One of these values: ■ `ssl_opsec` - The connection is authenticated and encrypted (this is the default). ■ `auth_opsec` - The connection is authenticated. ■ `clear` - The connection is neither authenticated, nor encrypted.
`-p <Port>`	Specifies the port number on the ELA proxy. Default port is 18187.
`-f <Token> <Value>`	A field to be added to the log, represented by a `<Token> <Value>` pair as follows: ■ `<Token>` - The name of the field to be added to the log. Cannot contain spaces. ■ `<Value>` - The field's value. Cannot contain spaces. This option can be used multiple times to add multiple `<Token> <Value>` pairs to the log.

Parameter	Description
`-m <Alert Type>`	The alert to be triggered at the ISP site. This alert overrides the alert specified in the log message generated by the alert daemon. The response to the alert is handled according to the actions specified in the ISP Security Policy: These alerts execute the OS commands: ■ `alert` - Popup alert command ■ `mail` - Mail alert command ■ `snmptrap` - SNMP trap alert command ■ `spoofalert` - Anti-Spoof alert command These NetQuota and ServerQuota alerts execute the OS commands specified in the `$FWDIR/conf/objects.C`: file: `value=clientquotaalert. Parameter=clientquotaalertcmd`

Exist Status

Exit Status	Description
`0`	Execution was successful.
`102`	Undetermined error.
`103`	Unable to allocate memory.
`104`	Unable to obtain log information from `stdin`
`106`	Invalid command line arguments.
`107`	Failed to invoke the OPSEC API.

Example

```
inet_alert -s 10.0.2.4 -a clear -f product cads -m alert
```

This command specifies to perform these actions in the event of an attack:

- Establish a clear connection with the ELA Proxy located at IP address 10.0.2.4
- Send a log message to the specified ELA Proxy. Set the product field of this log message to `cads`
- Trigger the OS command specified in the SmartConsole > **Menu > Global properties > Log and Alert > Popup Alert Command** field.

ldapcmd

Description

This is an LDAP utility that controls these features:

Feature	Description
Cache	LDAP cache operations, such as emptying the cache, as well as providing debug information.
Statistics	LDAP search statistics, such as: ■ All user searches ■ Pending lookups (when two or more lookups are identical) ■ Total lookup time (the total search time for a specific lookup) ■ Cache statistics such as hits and misses These statistics are saved in the `$FWDIR/log/ldap_pid_<Process PID>.stats` file.
Logging	View the alert and warning logs.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
ldapcmd [-d <Debug Level>] -p {<Process Name> | all} <Command>
```

Parameters

Parameter	Description
`-d <Debug Level>`	Runs the command in debug mode with the specified TDERROR debug level. Valid values are from 0 (disabled) to 5 (maximal level, recommended).
`-p {<Process Name> | all}`	Runs on a specified Check Point process, or all supported Check Point processes.
`<Command>`	One of these commands: ■ `cacheclear {all | UserCacheObject | TemplateCacheObject | TemplateExtGrpCacheObject}` • `all` - Clears cache for all objects • `UserCacheObject` - Clears cache for user objects • `TemplateCacheObject` - Clears cache for template objects • `TemplateExtGrpCacheObject` - Clears cache for external template group objects ■ `cachetrace {all | UserCacheObject | TemplateCacheObject | TemplateExtGrpCacheObject}` • `all` - Traces cache for all objects • `UserCacheObject` - Traces cache for user objects • `TemplateCacheObject` - Traces cache for template objects • `TemplateExtGrpCacheObject` - Traces cache for external template group objects ■ `log {on | off}` • `on` - Creates LDAP logs • `off` - Does not create LDAP logs ■ `stat {<Print Interval in Sec> | 0}` • `<Print Interval in Sec>` - How frequently to collect the statistics • `0` - Stops collecting the statistics

ldapcompare

Description

This is an LDAP utility that performs compare queries and prints a message whether the result returned a match or not.

This utility opens a connection to an LDAP directory server, binds, and performs the comparison specified on the command line or from a specified file.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
ldapcompare [-d <Debug Level>] [<Options>] <DN> {<Attribute>
<Value> | <Attribute> <Base64 Value>}
```

Parameters

Parameter	Description
`-d <Debug Level>`	Runs the command in debug mode with the specified TDERROR debug level. Valid values are from 0 (disabled) to 5 (maximal level, recommended).
`<Options>`	See the tables below: ■ Compare options ■ Common options
`<DN>`	Specifies the Distinguished Name.
`<Attribute>`	Specifies the assertion attribute.
`<Value>`	Specifies the assertion value.
`<Base64 Value>`	Specifies the Base64 encoding of the assertion value.

Compare options

Option	Description
`-E [!]<Extension> [=<Extension Parameter>]`	Specifies the compare extensions. **Note** - The exclamation sign "!" indicates criticality. For example: `!dontUseCopy` = Do **not** use Copy
`-M`	Enables the Manage DSA IT control. Use the "`-MM`" option to make it critical.
`-P <LDAP Protocol Version>`	Specifies the LDAP protocol version. Default version is 3.
`-z`	Enables the quiet mode. The command does not print anything. You can use the command return values.

Common options

Option	Description
`-D <Bind DN>`	Specifies the LDAP Server administrator Distinguished Name.

Option	Description
`-e [!]<Extension> [=<Extension Parameter>]`	Specifies the general extensions: **Note** - The exclamation sign "!" indicates criticality. ■ `[!]assert=<Filter>` RFC 4528; an RFC 4515 filter string ■ `[!]authzid=<Authorization ID>` RFC 4370; either "`dn:<DN>`", or "`u:<Username>`" ■ `[!]chaining[=<Resolve Behavior>[/<Continuation Behavior>]]` One of these: • "chainingPreferred" • "chainingRequired" • "referralsPreferred" • "referralsRequired" ■ `[!]manageDSAit` RFC 3296 ■ `[!]noop` ■ `ppolicy` ■ `[!]postread[=<Attributes>]` RFC 4527; a comma-separated list of attributes ■ `[!]preread[=<Attributes>]` RFC 4527; a comma-separated list of attributes ■ `[!]relax` ■ `abandon` SIGINT sends the abandon signal; if critical, does not wait for SIGINT. Not really controls. ■ `cancel` SIGINT sends the cancel signal; if critical, does not wait for SIGINT. Not really controls. ■ `ignore` SIGINT ignores the response; if critical, does not wait for SIGINT. Not really controls.
`-h <LDAP Server>`	Specifies the LDAP Server server by its IP address or resolvable hostname.
`-H <LDAP URI>`	Specifies the LDAP Server Uniform Resource Identifier (s).
`-I`	Specifies to use the SASL Interactive mode.
`-n`	Dry run - shows what would be done, but does not actually do it.

Option	Description
`-N`	Specifies not to use the reverse DNS to canonicalize SASL host name.
`-o <Option>[=<Option Parameter>]`	Specifies the general options: `nettimeout={<Timeout in Sec> | none | max}`
`-O <Properties>`	Specifies the SASL security properties.
`-p <LDAP Server Port>`	Specifies the LDAP Server port. Default is 389.
`-Q`	Specifies to use the SASL Quiet mode.
`-R <Realm>`	Specifies the SASL realm.
`-U <Authentication Identity>`	Specifies the SASL authentication identity.
`-v`	Runs in verbose mode (prints the diagnostics to *stdout*).
`-V`	Prints version information (use the "`-VV`" option only).
`-w <LDAP Admin Password>`	Specifies the LDAP Server administrator password (for simple authentication).
`-W`	Specifies to prompt the user for the LDAP Server administrator password.
`-x`	Specifies to use simple authentication.
`-X <Authorization Identity>`	Specifies the SASL authorization identity (either "`dn:<DN>`", or "`u:<Username>`" option).
`-y <File>`	Specifies to read the LDAP Server administrator password from the `<File>`.
`-Y <SASL Mechanism>`	Specifies the SASL mechanism.
`-Z`	Specifies to start the TLS request. Use the "`-ZZ`" option to require successful response.

ldapmemberconvert

Description

This is an LDAP utility that ports from the "Member" attribute values in LDAP group entries to the "MemberOf" attribute values in LDAP member (User or Template) entries.

This utility converts the LDAP server data to work in either the "MemberOf" mode, or "Both" mode. The utility searches through all specified group or template entries that hold one or more "Member" attribute values and modifies each value. The utility searches through all specified group/template entries and fetches their "Member" attribute values.

Each value is the DN of a member entry. The entry identified by this DN is added to the "MemberOf" attribute value of the group/template DN at hand. In addition, the utility delete those "Member" attribute values from the group/template, unless you run the command in the "Both" mode.

When your run the command, it creates a log file `ldapmemberconvert.log` in the current working directory. The command logs all modifications done and errors encountered in that log file.

Important - Back up the LDAP server database *before* you run this conversion utility.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
ldapmemberconvert [-d <Debug Level>] -h <LDAP Server> -p <LDAP
Server Port> -D <LDAP Admin DN> -w <LDAP Admin Password> -m
<Member Attribute Name> -o <MemberOf Attribute Name> -c <Member
ObjectClass Value> [-B] [-f <File> | -g <Group DN>] [-L <LDAP
Server Timeout>] [-M <Number of Updates>] [-S <Size>] [-T <LDAP
Client Timeout>] [-Z]
```

Parameters

Parameter	Description
`-d <Debug Level>`	Runs the command in debug mode with the specified TDERROR debug level. Valid values are from 0 (disabled) to 5 (maximal level, recommended).
`-h <LDAP Server>`	Specifies the LDAP Server server by its IP address or resolvable hostname. If you do not specify the LDAP Server explicitly, the command connects to `localhost`.
`-p <LDAP Server Port>`	Specifies the LDAP Server port. Default is 389.
`-D <LDAP Admin DN>`	Specifies the LDAP Server administrator Distinguished Name.
`-w <LDAP Admin Password>`	Specifies the LDAP Server administrator password.
`-m <Member Attribute Name>`	Specifies the LDAP attribute name when fetching and (possibly) deleting a group `Member` attribute value.
`-o <MemberOf Attribute Name>`	Specifies the LDAP attribute name for adding an LDAP "`MemberOf`" attribute value.
`-c <Member ObjectClass Value>`	Specifies the LDAP "`ObjectClass`" attribute value that defines, which type of member to modify. You can specify multiple attribute values with this syntax: `-c <Member Object Class 1> -c <Member Object Class 2> ... -c <Member Object Class N>`
`-B`	Specifies to run in "`Both`" mode.

`-f <File>`	Specifies the file that contains a list of Group DNs separated by a new line:
	`<Group DN 1>`
	`<Group DN 2>`
	`...`
	`<Group DN N>`
	Length of each line is limited to 256 characters.

Parameter	Description
`-g <Group DN>`	Specifies the Group or Template Distinguished Name, on which to perform the conversion. You can specify multiple Group DNs with this syntax: `-g <Group DN 1> -g <Group DN 2> ... -g <Group DN N>`
`-L <LDAP Server Timeout>`	Specifies the Server side time limit for LDAP operations, in seconds. Default is "never".
`-M <Number of Updates>`	Specifies the maximal number of simultaneous member LDAP updates. Default is 20.
`-S <Size>`	Specifies the Server side size limit for LDAP operations, in number of entries. Default is "none".
`-T <LDAP Client Timeout>`	Specifies the Client side timeout for LDAP operations, in milliseconds. Default is "never".
`-Z`	Specifies to use SSL connection.

Notes

There are two "GroupMembership" modes. You must keep these modes consistent:

- template-to-groups
- user-to-groups

For example, if you apply conversion on LDAP users to include the "MemberOf" attributes for their groups, then this conversion has to be applied on LDAP defined templates for their groups.

Troubleshooting

Symptom:

A command fails with an error message stating the connection stopped unexpectedly when you run it with the parameter `-M <Number of Updates>`.

Root Cause:

The LDAP server could not handle that many LDAP requests simultaneously and closed the connection.

Solution:

Run the command again with a lower value for the "`-M`" parameter. The default value should be adequate, but can also cause a connection failure in extreme situations. Continue to reduce the value until the command runs normally. Each time you run the command with the same set of groups, the command continues from where it left off.

Examples

Example 1

A group is defined with the DN "`cn=cpGroup,ou=groups,ou=cp,c=us`" and these attributes:

```
...
cn=cpGroup
uniquemember="cn=member1,ou=people,ou=cp,c=us"
uniquemember="cn=member2,ou=people,ou=cp,c=us"
...
```

For the two member entries:

```
...
cn=member1
objectclass=fw1Person
...
```

and:

```
...
cn=member2
objectclass=fw1Person
...
```

Run:

```
[Expert@MGMT:0]# ldapconvert -g cn=cpGroup,ou=groups,ou=cp,c=us -h MyLdapServer -d cn=admin -w secret -m uniquemember -o memberof -c
fw1Person
```

The result for the group DN is:

```
...
cn=cpGroup
...
```

The result for the two member entries is:

```
...
cn=member1
objectclass=fw1Person
memberof="cn=cpGroup,ou=groups,ou=cp,c=us"
...
```

and:

```
...
cn=member2
objectclass=fw1Person
memberof="cn=cpGroup,ou=groups,ou=cp,c=us"
...
```

If you run the same command with the "`-B`" parameter, it produces the same result, but the group entry is not modified.

Example 2

If there is another member attribute value for the same group entry:

```
uniquemember="cn=template1,ou=people, ou=cp,c=us"
```

and the template is:

```
cn=member1
objectclass=fw1Template
```

Then after running the same command, the template entry stays intact, because of the parameter "`-c fw1Person`", but the object class of "`template1`" is "`fw1Template`".

ldapmodify

Description

This is an LDAP utility that imports users to an LDAP server. The input file must be in the LDIF format.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
ldapmodify [-d <Debug Level>] [-h <LDAP Server>] [-p <LDAP Server Port>] [-D <LDAP Admin DN>] [-w <LDAP Admin Password>] [-a] [-b] [-c] [-F] [-k] [-n] [-r] [-v] [-T <LDAP Client Timeout>] [-Z] [ -f <Input File> .ldif | < <Entry>]
```

Parameters

Parameter	Description
`-d <Debug Level>`	Runs the command in debug mode with the specified TDERROR debug level. Valid values are from 0 (disabled) to 5 (maximal level, recommended).
`-h <LDAP Server>`	Specifies the LDAP Server server by its IP address or resolvable hostname. If you do not specify the LDAP Server explicitly, the command connects to `localhost`.
`-p <LDAP Server Port>`	Specifies the LDAP Server port. Default is 389.
`-D <LDAP Admin DN>`	Specifies the LDAP Server administrator Distinguished Name.
`-w <LDAP Admin Password>`	Specifies the LDAP Server administrator password.

Parameter	Description
`-a`	Specifies that this is the LDAP "`add`" operation.
`-b`	Specifies to read values from files (for binary attributes).
`-c`	Specifies to ignore errors during continuous operation.
`-F`	Specifies to force changes on all records.
`-k`	Specifies the Kerberos bind.
`-K`	Specifies the Kerberos bind, part 1 only.
`-n`	Specifies to print the LDAP "`add`" operations, but do not actually perform them.
`-r`	Specifies to replace values, instead of adding values.
`-v`	Specifies to run in verbose mode.
`-T <`*`LDAP Client Timeout`*`>`	Specifies the Client side timeout for LDAP operations, in milliseconds. Default is "`never`".
`-Z`	Specifies to use SSL connection.
`-f <`*`Input File`*`>.ldif`	Specifies to read from the `<`*`Input File`*`>.ldif` file. The input file must be in the LDIF format.
`< <`*`Entry`*`>`	Specifies to read the entry from the *stdin*. The "`<`" character is mandatory part of the syntax. It specifies the input comes from the standard input (from the data you enter on the screen).

ldapsearch

Description

This is an LDAP utility that queries an LDAP directory and returns the results.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

```
ldapsearch [-d <Debug Level>] [-h <LDAP Server>] [-p <LDAP Port>]
[-D <LDAP Admin DN>] [-w <LDAP Admin Password>] [-A] [-B] [-b
<Base DN>] [-F <Separator>] [-l <LDAP Server Timeout>] [-s
<Scope>] [-S <Sort Attribute>] [-t] [-T <LDAP Client Timeout>] [-
u] [-z <Number of Search Entries>] [-Z] <Filter> [<Attributes>]
```

Parameters

Parameter	Description
`-d <Debug Level>`	Runs the command in debug mode with the specified TDERROR debug level. Valid values are from 0 (disabled) to 5 (maximal level, recommended).
`-h <LDAP Server>`	Specifies the LDAP Server server by its IP address or resolvable hostname. If you do not specify the LDAP Server explicitly, the command connects to `localhost`.
`-p <LDAP Port>`	Specifies the LDAP Server port. Default is 389.
`-D <LDAP Admin DN>`	Specifies the LDAP Server administrator Distinguished Name.
`-w <LDAP Admin Password>`	Specifies the LDAP Server administrator password.
`-A`	Specifies to retrieve attribute names only, without values.

Parameter	Description
`-B`	Specifies not to suppress the printing of non-ASCII values.
`-b <Base DN>`	Specifies the Base Distinguished Name (DN) for search.
`-F <Separator>`	Specifies the print separator character between attribute names and their values. The default separator is the equal sign (=).
`-l <LDAP Server Timeout>`	Specifies the Server side time limit for LDAP operations, in seconds. Default is "`never`".
`-s <Scope>`	Specifies the search scope. One of these: ■ `base` ■ `one` ■ `sub`
`-S <Sort Attribute>`	Specifies to sort the results by the values of this attribute.

`-t`	Specifies to write values to files in the `/tmp/` directory.
	Writes each *<attribute>-<value>* pair to a separate file named:
	`/tmp/ldapsearch-<Attribute>-<Value>`
	For example, for the `fw1color` attribute with the value `a00188`, the command writes to the file named:
	`/tmp/ldapsearch-fw1color-a00188`

`-T <LDAP Client Timeout>`	Specifies the Client side timeout for LDAP operations, in milliseconds. Default is `never`.
`-u`	Specifies to show user-friendly entry names in the output. For example: shows `cn=Babs Jensen, users, omi` instead of `cn=Babs Jensen, cn=users,cn=omi`
`-z <Number of Search Entries>`	Specifies the maximal number of entries to search on the LDAP Server.
`-Z`	Specifies to use SSL connection.
`<Filter>`	LDAP search filter compliant with RFC-1558. For example: `objectclass=fw1host`

Parameter	Description
<Attributes>	Specifies the list of attributes to retrieve. If you do not specify attributes explicitly, then the command retrieves all attributes.

Example

```
[Expert@MGMT:0]# ldapsearch -p 18185 -b cn=omi objectclass=fw1host objectclass
```

With this syntax, the command:

1. Connects to the LDAP Server to port 18185.
2. Connects to the LDAP Server with Base DN "`cn=omi`".
3. Queries the LDAP directory for "`fw1host`" objects.
4. For each object found, prints the value of its "`objectclass`" attribute.

mcd

Description

This command changes current working directory to the specified directory in the `$FWDIR` directory in the context of a Domain Management Server.

Syntax

```
mdsenv <IP Address or Name of Domain Management Server>
mcd <Name of Directory in $FWDIR>
```

Example

```
[Expert@MDS:0]# mdsstat
+-----------------------------------------------------------------------------------------------------
------+
|                                     Processes status checking
     |
+------+--------------------+----------------+-------------+-------------+-------------+-------
------+
| Type | Name               | IP address     | FWM         | FWD         | CPD         | CPCA
     |
+------+--------------------+----------------+-------------+-------------+-------------+-------
------+
| MDS  |          -         | 192.168.3.51   | up 15312    | up 15310    | up 10227    | up
15475    |
+------+--------------------+----------------+-------------+-------------+-------------+-------
------+
| CMA  | MyDomain_Server    | 192.168.3.240  | up 17225    | up 17208    | up 17101    | up
18402    |
+------+--------------------+----------------+-------------+-------------+-------------+-------
------+
| Total Domain Management Servers checked: 1     1 up   0 down
     |
| Tip: Run mdsstat -h for legend
     |
+-----------------------------------------------------------------------------------------------------
------+
[Expert@MDS:0]#
[Expert@MDS:0]#
[Expert@MDS:0]# mdsenv MyDomain_Server
[Expert@MDS:0]#
[Expert@MDS:0]# mcd
changing to /opt/CPmds-R81.20/customers/MyDomain_Server/CPsuite-R81.20/fw1/
[Expert@MDS:0]#
[Expert@MDS:0]# pwd
/opt/CPmds-R81.20/customers/MyDomain_Server/CPsuite-R81.20/fw1
[Expert@MDS:0]#
[Expert@MDS:0]# ls -1
av
bin
conf
cpm-server
database
doc
hash
lib
libsw
log
scripts
state
tmp
[Expert@MDS:0]#
```

```
[Expert@MDS:0]# mcd av
changing to /opt/CPmds-R81.20/customers/MyDomain_Server/CPsuite-R81.20/fw1/av
[Expert@MDS:0]#
[Expert@MDS:0]# mcd bin
changing to /opt/CPmds-R81.20/customers/MyDomain_Server/CPsuite-R81.20/fw1/bin
[Expert@MDS:0]#
[Expert@MDS:0]# mcd conf
changing to /opt/CPmds-R81.20/customers/MyDomain_Server/CPsuite-R81.20/fw1/conf
[Expert@MDS:0]#
[Expert@MDS:0]# mcd log
changing to /opt/CPmds-R81.20/customers/MyDomain_Server/CPsuite-R81.20/fw1/log
[Expert@MDS:0]#
[Expert@MDS:0]# mcd scripts
changing to /opt/CPmds-R81.20/customers/MyDomain_Server/CPsuite-R81.20/fw1/scripts
[Expert@MDS:0]#
```

mds_backup

Description

The `mds_backup` command backs up binaries and data from a Multi-Domain Server to a user specified working directory.

You then copy the backup files from the working directory to external storage.

This command requires Multi-Domain Superuser privileges.

The `mds_backup` command runs the `gtar` and `dump` commands to back up all databases. The collected information is stored in one `*.tar` file. The file name is a combination of the backup date and time and is saved in the current working directory. For example: `13Sep2015-141437.mdsbk.tar`

Backing up and restoring in Management High Availability environment:

- To back up and restore a consistent environment, make sure to collect and restore the backups and snapshots from all servers in the High Availability environment at the same time.
- Make sure other administrators do not make changes in SmartConsole until the backup operation is completed.

For more information:

- About Gaia Backup and Gaia Snapshot, see the *R81.20 Gaia Administration Guide*.
- About Virtual Machine Snapshots, see the vendor documentation.

Notes:

- You can restore a backup file on Gaia OS with the same software version, Jumbo Hotfix Accumulator, Hotfixes, and Check Point Automatic Updates as installed on the source Gaia OS, from which you collected this backup file.
- Do not create or delete Domains or Domain Management Servers until the backup operation completes.
- It is important to run the `mds_backup` command from directories that are not backed up.
  For example, when you back up a Multi-Domain Server, do not run the `mds_backup` command from the `/opt/CPmds-<Current_Release>/` directory, because it is a circular reference (backup of directory, in which it is necessary to write files).
  Run the `mds_backup` command from a location outside the product directory tree to be backed up (for example: `/home/admin, /var/log/`). This becomes the working directory.
- The `mds_backup` command does not collect the active Security log file (`*.log`) and Audit log file (`*.adtlog`).
  This is necessary to prevent inconsistencies during the read-write operations.
  Best Practice - Perform a log switch before you start the backup procedure.
- You can back up the Multi-Domain Server configuration without the log files.
  This backup is typically significantly smaller than a full backup with logs.
  To back up without log files, add this line to the file `$MDSDIR/conf/mds_exclude.dat` configuration file:

  ```
  log/*
  ```
- After the backup completes, copy the backup `*.tar` file, together with the `mds_restore`, and `gtar` binary files, to your external backup location.

Syntax

```
mds_backup -h
```

```
mds_backup [-b] [-d <Target Directory>] [-ds] [-l] [-mask] [-s] [-v] [-x]
```

Parameters

Parameter	Description
`-h`	Shows help text.
`-b`	Batch mode - executes without asking anything.
`-d <Target Directory>`	Specifies the output directory. If not specified explicitly, the backup file is saved to the current directory. You cannot save the backup file to the root directory.
`-ds`	Disconnects all current sessions and discards their unpublished changes before the backup starts.
`-l`	Excludes logs from the backup.
`-mask`	Hide sensitive information in the Postgres database in the backup.
`-s`	Stops Multi-Domain processes before the backup starts.
`-v`	"Dry run" - Shows all files to be backed up, but does not perform the backup operation.
`-x`	Excludes binary files from the backup. The binary files are listed in the `$MDSDIR/conf/mds_binaries_exclude.dat` file.

mds_restore

Description

Use the `mds_restore` command to restore a Multi-Domain Server / Multi-Domain Log Server that was backed up with the *"mds_backup" on page 756* command.

Important - You must restore on the server that runs same software version, Jumbo Hotfix Accumulator, Hotfixes, and Check Point Automatic Updates as installed on the source Gaia OS, from which you collected this backup.
Example: If you collected a backup on a server with version "XX" and Jumbo Hotfix Accumulator Take "YY", then you must restore on a server with version "XX" and Jumbo Hotfix Accumulator Take "YY".

Best Practice - If the Multi-Domain Security Management environment has multiple Multi-Domain Servers, restore all Multi-Domain Servers at the same time.

Backing up and restoring in Management High Availability environment:

- To back up and restore a consistent environment, make sure to collect and restore the backups and snapshots from all servers in the High Availability environment at the same time.
- Make sure other administrators do not make changes in SmartConsole until the backup operation is completed.

For more information:

- About Gaia Backup and Gaia Snapshot, see the *R81.20 Gaia Administration Guide*.
- About Virtual Machine Snapshots, see the vendor documentation.

To restore a Multi-Domain Server:

1. Connect to the command line on the Multi-Domain Server.
2. Log in to the Expert mode.
3. Go to the directory where the backup file is located.
4. Run:

   ```
   ./mds_restore <backup_file>
   ```

5. If you restore on a Multi-Domain Server with a new IP address, configure the new IP address.

mdscmd

Description

In versions lower than R80, this utility executed various commands on the Multi-Domain Server.

Starting from R80, this command is obsolete.

You must use other commands. If there is no alternative command, then perform the applicable action in SmartConsole.

MDSCMD command in pre-R80 versions	Alternative command in R80 and above
`mdscmd addadministrator <options>`	None
`mdscmd adddomain <options>`	`mgmt_cli add-domain` See *"mgmt_cli" on page 782*.
`mdscmd addlogserver <options>`	`mgmt_cli add-domain` See *"mgmt_cli" on page 782*.
`mdscmd addmanagement <options>`	`mgmt_cli add-domain` See *"mgmt_cli" on page 782*.
`mdscmd assign-globalpolicy <options>`	`mgmt_cli set global-assignment` See *"mgmt_cli" on page 782*.
`mdscmd assignadmin <options>`	`mgmt_cli set-administrator` See *"mgmt_cli" on page 782*.
`mdscmd assignguiclient <options>`	None
`mdscmd deleteadministrator <options>`	None
`mdscmd deletedomain <options>`	`mgmt_cli delete-domain` See *"mgmt_cli" on page 782*.
`mdscmd deletelogserver <options>`	None

MDSCMD command in pre-R80 versions	Alternative command in R80 and above
`mdscmd deletemanagement <options>`	`mgmt_cli delete-domain` See *"mgmt_cli" on page 782*.
`mdscmd disableglobaluse <options>`	None
`mdscmd enableglobaluse <options>`	None
`mdscmd install-globalpolicy <options>`	`mgmt_cli assign-global-assignment` See *"mgmt_cli" on page 782*.
`mdscmd migratemanagement <options>`	None
`mdscmd mirrormanagement <options>`	None

`mdscmd reassign-globalpolicy <options>`	`mgmt_cli set global-assignment`
	`mgmt_cli assign-global-assignment`
	See *"mgmt_cli" on page 782*.

`mdscmd remove-globalpolicy <options>`	`mgmt_cli delete global-assignment` See *"mgmt_cli" on page 782*.
`mdscmd removeadmin <options>`	`mgmt_cli set-administrator` See *"mgmt_cli" on page 782*.
`mdscmd removeguiclient <options>`	None
`mdscmd runcrossdomainquery <options>`	None
`mdscmd startmanagement <options>`	`mdsstart_customer` See *"mdsstart_customer" on page 774*.
`mdscmd stopmanagement <options>`	`mdsstop_customer` See *"mdsstop_customer" on page 781*.

mdsconfig

Description

This command starts the Multi-Domain Server Configuration Program. This tool configures specific settings for the installed Check Point products.

Note - This command updates the database schema before it imports. First, the command runs pre-upgrade verification. If no errors are found, migration continues. If there are errors, you must fix them on the source R7x Domain Management Server according to instructions in the error messages. Then do this procedure again.

For the complete procedure, see the *R81.20 Installation and Upgrade Guide*.

Syntax

```
mdsconfig
```

Menu Options

Menu Option	Description
Leading VIP Interfaces	The Leading VIP Interfaces are real interfaces connected to an external network. These interfaces are used when you configure virtual IP addresses for Domain Management Servers.
Licenses	Manages Check Point licenses and contracts on this server.
Random Pool	Configures the RSA keys, to be used by Gaia Operating System.
Groups	Usually, the Multi-Domain Server is given group permission for access and execution. You may now name such a group or instruct the installation procedure to give no group permissions to the server. In the latter case, only the Super-User is able to access and execute commands on the server.
Certificate's Fingerprint	Shows the ICA's Fingerprint. This fingerprint is a text string derived from the server's ICA certificate. This fingerprint verifies the identity of the server when you connect to it with SmartConsole.
Administrators	Configures Check Point system administrators for this server.
GUI Clients	Configures the GUI clients that can use SmartConsole to connect to this server.
Automatic Start of Multi-Domain Server	Shows and controls if Multi-Domain Server starts automatically during boot.
P1Shell	Obsolete. Do **not** use this option anymore. **Important** - This option and the `p1shell` command are **not** supported (Known Limitation PMTR-45085).
Start Multi-Domain Server Password	Configures a password to control the start of the Multi-Domain Server.
IPv6 Support for Multi-Domain Server	Enables or disables the IPv6 Support on the Multi-Domain Server. **Important** - Multi-Domain Server does not support IPv6 at all (Known Limitation PMTR-14989).

Menu Option	Description
IPv6 Support for Existing Domain Management Servers	Enables or disables the IPv6 Support on the Domain Management Servers. **Important** - Multi-Domain Server does not support IPv6 at all (Known Limitation PMTR-14989).
Exit	Exits from the Multi-Domain Server Configuration Program.

Example - Menu on a Multi-Domain Server

```
[Expert@MyMDS:0]# mdsconfig


Welcome to Multi-Domain Server Configuration Program
================================================================
This program will let you re-configure your Multi-Domain Server configuration.


Configuration Options:
----------------------
(1)  Leading VIP Interfaces
(2)  Licenses
(3)  Random Pool
(4)  Groups
(5)  Certificate's Fingerprint
(6)  Administrators
(7)  GUI clients
(8)  Automatic Start of Multi-Domain Server
(9)  P1Shell
(10) Start Multi-Domain Server Password
(11) IPv6 Support for Multi-Domain Server
(12) IPv6 Support for Existing Domain Management Servers

(13) Exit

Enter your choice (1-13):
```

mdsenv

Description

Use the `mdsenv` command to set shell environment variables to run commands on a specified Domain Management Server.

When run without an argument, the command sets the shell for Multi-Domain Server level commands (*"mdsstart" on page 770*, *"mdsstop" on page 777*, and so on).

Syntax

```
mdsenv [<Name or IP address of Domain Management Server>]
```

Parameters

Parameter	Description
<Name or IP address of Domain Management Server>	Specifies the Domain Management Server by its name or IPv4 address.

Example

```
[Expert@MyMDS:0]# mdsstat
+-------------------------------------------------------------------
-----------------------------------+
|                                        Processes status checking
                                   |
+------+--------------------+----------------+-------------+-----
-------+-------------+-------------+
| Type | Name               | IP address     | FWM         | FWD
       | CPD         | CPCA        |
+------+--------------------+----------------+-------------+-----
-------+-------------+-------------+
| MDS  |          -         | 192.168.3.51   | up 10086    | up
11422    | up 5427     | up 11440    |
+------+--------------------+----------------+-------------+-----
-------+-------------+-------------+
| CMA  | MyDomain_Server    | 192.168.3.240  | up 10891    | up
8199     | up 7670     | up 9536     |
+------+--------------------+----------------+-------------+-----
-------+-------------+-------------+
| Total Domain Management Servers checked: 1     1 up   0 down
                                   |
| Tip: Run mdsstat -h for legend
                                   |
+-------------------------------------------------------------------
-----------------------------------+
[Expert@MyMDS:0]#
[Expert@MyMDS:0]# mdsenv MyDomain_Server
[Expert@MyMDS:0]#
[Expert@MyMDS:0]# echo $FWDIR
/opt/CPmds-R81.20/customers/MyDomain_Server/CPsuite-R81.20/fw1
[Expert@MyMDS:0]#
```

mdsquerydb

Description

The `mdsquerydb` is an advanced database query tool that administrators can use to run shell scripts to get information from the Multi-Domain Security Management databases.

Use this command to get information from the Multi-Domain Server, Domain Management Server, and Global databases.

Note - The system comes with pre-defined queries, defined in the `$MDSDIR/confqueries.conf` configuration file. Do **not** change or delete these queries.

Syntax

```
mdsquerydb <key_name> [-f <output_file_name>]
```

Parameters

Parameter	Description
<key_name>	Query key, which must be defined in the pre-defined queries configuration file.
-f <output_file_name>	Send the query results to the specified file name. If this parameter is not specified, the data is sent to the standard output.

Pre-Defined Query Keys

```
Keys for Multi-Domain environment:
----------------------------------
GlobalNetworkObjects    Get name and type of all global network objects
NetworkObjects          Get all Domains' internal Check Point installed network objects
Domains                 Get names of all Domains Irit B comment from QA Draft
Administrators          Get names of all Administrators
MDSs                    Get names and IPs of all MDSs
DomainManagementServers Get names of all Domain Servers
GuiClients              Get names and IPs of all gui clients
CMAs                    Backwards Compatibility (DomainManagementServers)
Customers               Backwards Compatibility (Domains)
Keys for Domain environment:
----------------------------
NetworkObjects          Get name and type of all network objects
Gateways                Get names and IPs of all gateways
```

Example 1 - Retrieve list of all defined keys

```
[Expert@MDS:0]# mdsquerydb
```

Example 2 - Send a list of Domains in the Multi-Domain Server database to the standard output

```
[Expert@MDS:0]# mdsenv
[Expert@MDS:0]# mdsquerydb Domains
```

Example 3 - Send a list of network objects in the global database to the /tmp/gateways.txt file

```
[Expert@MDS:0]# mdsenv
[Expert@MDS:0]# mdsquerydb NetworkObjects -f /tmp/gateways.txt
```

Example 4 - Get a list of gateway objects in the Domain Management Server "DServer1"

```
[Expert@MDS:0]# mdsenv My_Domain_Server
[Expert@MDS:0]# mdsquerydb Gateways -f /tmp/gateways.txt
```

mdsstart

Description

Starts the Multi-Domain Server and all Domain Management Servers.

To start a specific Domain Management Server, see the *"mdsstart_customer" on page 774* command.

Syntax

```
mdsstart [-m | -s]
```

Parameters

Parameter	Description
`-m`	**Optional:** Starts only the Multi-Domain Server and not the Domain Management Servers.
`-s`	**Optional:** Starts all the Domain Management Servers sequentially. The command waits for each Domain Management Server to come up, before it starts the next one.

Controlling the number of Domain Management Servers to start sequentially

By default, the system attempts to start up to 10 Domain Management Servers at the same time.

You can decrease the amount of time it takes to start the Multi-Domain Server when there are many Domain Management Servers.

To do this, set the value of the environment variable `NUM_EXEC_SIMUL` to the number of Domain Management Servers that start at the same time.

Setting the environment variable 'NUM_EXEC_SIMUL' temporarily

This procedure configures the specified value for the environment variable `NUM_EXEC_SIMUL` in the current shell (does **not** survive reboot):

Step	Instructions
1	Connect to the command line on the Multi-Domain Server.
2	Log in to the Expert mode.

3	Set the value of the environment variable `NUM_EXEC_SIMUL`:
	`[Expert@MDS:0]# export NUM_EXEC_SIMUL=<Number of Domain Management Servers>`
	Example:
	`[Expert@MDS:0]# export NUM_EXEC_SIMUL=5`

4	Make sure the new value of the environment variable `NUM_EXEC_SIMUL` is set: `[Expert@MDS:0]# echo $NUM_EXEC_SIMUL` Output must show the configured value.

Unsetting the environment variable 'NUM_EXEC_SIMUL' temporarily

This procedure removes the configured value for the environment variable `NUM_EXEC_SIMUL` in the current shell (does **not** survive reboot):

Parameter	Description
1	Connect to the command line on the Multi-Domain Server.
2	Log in to the Expert mode.
3	Unset the value of the environment variable `NUM_EXEC_SIMUL`: `[Expert@MDS:0]# unset NUM_EXEC_SIMUL`
4	Make sure the environment variable `NUM_EXEC_SIMUL` is not set: `[Expert@MDS:0]# echo $NUM_EXEC_SIMUL` Output must be empty.

Setting the environment variable 'NUM_EXEC_SIMUL' permanently

This procedure configures the specified value for the environment variable `NUM_EXEC_SIMUL` for all shells (survives reboot):

Step	Instructions
1	Connect to the command line on the Multi-Domain Server.
2	Log in to the Expert mode.
3	Back up the current `/etc/rc.d/rc.local` file: `[Expert@MDS:0]# cp -v /etc/rc.d/rc.local{,_BKP}`
4	Edit the current `/etc/rc.d/rc.local` file: `[Expert@MDS:0]# vi /etc/rc.d/rc.local`

5	Add this line at the bottom of the file:
	`export NUM_EXEC_SIMUL=<Number of Domain Management Servers>`
	Important - After this line, you must press Enter to add a new line.
	Example:
	`export NUM_EXEC_SIMUL=5`

6	Save the changes in the file and exit the Vi editor.
7	Reboot.
8	Make sure the new value of the environment variable `NUM_EXEC_SIMUL` is set: `[Expert@MDS:0]# echo $NUM_EXEC_SIMUL` Output must show the configured value.

Unsetting the environment variable 'NUM_EXEC_SIMUL' permanently

This procedure removes the configured value for the environment variable `NUM_EXEC_SIMUL` for all shells (survives reboot):

Step	Instructions
1	Connect to the command line on the Multi-Domain Server.
2	Log in to the Expert mode.
3	Back up the current `/etc/rc.d/rc.local` file: `[Expert@MDS:0]# cp -v /etc/rc.d/rc.local{,_BKP_with_NUM_EXEC_SIMUL}`
4	Edit the current `/etc/rc.d/rc.local` file: `[Expert@MDS:0]# vi /etc/rc.d/rc.local`
5	Remove this line from the file: `export NUM_EXEC_SIMUL=<Number of Domain Management Servers>`
6	Save the changes in the file and exit the Vi editor.
7	Reboot.
8	Make sure the new value of the environment variable `NUM_EXEC_SIMUL` is not set: `[Expert@MDS:0]# echo $NUM_EXEC_SIMUL` Output must be empty.

mdsstart_customer

Description

Starts the specified Domain Management Server, if it was stopped with the *"mdsstop_customer" on page 781* command.

To start the entire Multi-Domain Server, see the *"mdsstart" on page 770* command.

Syntax

```
mdsstart_customer <IP address or Name of Domain Management Server>
```

Note - If the name of the Domain Management Server includes spaces, you must surround it with quotes ("*Name of Domain Management Server*").

mdsstat

Description

This command shows the status of specific processes on the Multi-Domain Server and Domain Management Servers.

Syntax

```
mdsstat [-h] [-m] [<Name or IP Address of Domain Management Server>]
```

Parameters

Parameter	Description
`-h`	Displays help message.
`-m`	Test status for Multi-Domain Server only.
<Name or IP address of Domain Management Server>	Specifies the Domain Management Server by its name or IPv4 address.

Possible Statuses of Processes

Status	Description
`up`	The process is up.
`down`	The process is down.
`pnd`	The process is pending initialization.
`init`	The process is initializing.
`N/A`	The process's PID is not yet available.
`N/R`	The process is not relevant for this Multi-Domain Server.

Example from a single Multi-Domain Security Management Server

```
[Expert@MDS:0]# mdsstat

CPM: Check Point Security Management Server is running and ready

+------+----------------+-----------------+------------+----------+----------+----------+
| Type| Name            | IP address      | FWM        | FWD      | CPD      | CPCA     |
+------+----------------+-----------------+------------+----------+----------+----------+
| MDS |        -        | 192.168.3.101   | up 17284   | up 17266 | up 17251 | up 17753 |
+------+----------------+-----------------+------------+----------+----------+----------+
| CMA |DOM211_Server    | 192.168.3.211   | up 32227   | up 32212 | up 25725 | up 32482 |
| CMA |DOM212_Server    | 192.168.3.212   | up 4248    | up 4184  | up 4094  | up 4441  |
+------+----------------+-----------------+------------+----------+----------+----------+
| Total Domain Management Servers checked: 2     2 up   0 down                          |
| Tip: Run mdsstat -h for legend                                                        |
+---------------------------------------------------------------------------------------+
[Expert@MDS:0]#
```

Example from a Multi-Domain Security Management Server in Management High Availability

```
[Expert@MDS:0]# mdsstat

CPM: Check Point Security Management Server is running and ready

+------+----------------+-----------------+------------+-------------+----------+----------+----
------+
| Typ e| Name            | IP address      | FWM        | FWMHA       | FWD      | CPD      |
CPCA     |
+------+----------------+-----------------+------------+-------------+----------+----------+----
------+
| MDS  |        -        | 192.168.3.101   | up 17284   | up 17289    | up 17266 | up 17251 | up
17753 |
+------+----------------+-----------------+------------+-------------+----------+----------+----
------+
| CMA  |DOM211_Server    | 192.168.3.211   | up 32227   | up 32231    | up 32212 | up 25725 | up
32482 |
| CMA  |DOM212_Server    | 192.168.3.212   | up 4248    | up 4250     | up 4184  | up 4094  | up
4441  |
+------+----------------+-----------------+------------+-------------+----------+----------+----
------+
| Total Domain Management Servers checked: 2     2 up   0 down
    |
| Tip: Run mdsstat -h for legend
     |
+-----------------------------------------------------------------------------------------------
------+
[Expert@MDS:0]#
```

mdsstop

Description

Stops the Multi-Domain Server and all Domain Management Servers.

To stop a specific Domain Management Server, see the *"mdsstop_customer" on page 781* command.

Syntax

```
mdsstop [-m | -s]
```

Parameters

Parameter	Description
`-m`	**Optional:** Stops only the Multi-Domain Server and not the Domain Management Servers.
`-s`	**Optional:** Stops all the Domain Management Servers sequentially. The command waits for each Domain Management Server to stop, before it stops the next one.

Controlling the number of Domain Management Servers to stop sequentially

By default, the system attempts to stop up to 10 Domain Management Servers at the same time.

You can decrease the amount of time it takes to stop the Multi-Domain Server when there are many Domain Management Servers.

To do this, set the value of the environment variable `NUM_EXEC_SIMUL` to the number of Domain Management Servers that stop at the same time.

Setting the environment variable 'NUM_EXEC_SIMUL' temporarily

This procedure configures the specified value for the environment variable `NUM_EXEC_SIMUL` in the current shell (does **not** survive reboot):

Step	Instructions
1	Connect to the command line on the Multi-Domain Server.
2	Log in to the Expert mode.

3	Set the value of the environment variable `NUM_EXEC_SIMUL`:
	`[Expert@MDS:0]# export NUM_EXEC_SIMUL=<Number of Domain Management Servers>`
	Example:
	`[Expert@MDS:0]# export NUM_EXEC_SIMUL=5`

4	Make sure the new value of the environment variable `NUM_EXEC_SIMUL` is set: `[Expert@MDS:0]# echo $NUM_EXEC_SIMUL` Output must show the configured value.

Unsetting the environment variable 'NUM_EXEC_SIMUL' temporarily

This procedure removes the configured value for the environment variable `NUM_EXEC_SIMUL` in the current shell (does **not** survive reboot):

Parameter	Description
1	Connect to the command line on the Multi-Domain Server.
2	Log in to the Expert mode.
3	Unset the value of the environment variable `NUM_EXEC_SIMUL`: `[Expert@MDS:0]# unset NUM_EXEC_SIMUL`
4	Make sure the environment variable `NUM_EXEC_SIMUL` is not set: `[Expert@MDS:0]# echo $NUM_EXEC_SIMUL` Output must be empty.

Setting the environment variable 'NUM_EXEC_SIMUL' permanently

This procedure configures the specified value for the environment variable `NUM_EXEC_SIMUL` for all shells (survives reboot):

Step	Instructions
1	Connect to the command line on the Multi-Domain Server.
2	Log in to the Expert mode.
3	Back up the current `/etc/rc.d/rc.local` file: `[Expert@MDS:0]# cp -v /etc/rc.d/rc.local{,_BKP}`
4	Edit the current `/etc/rc.d/rc.local` file: `[Expert@MDS:0]# vi /etc/rc.d/rc.local`

5	Add this line at the bottom of the file:
	`export NUM_EXEC_SIMUL=<Number of Domain Management Servers>`
	Important - After this line, you must press Enter to add a new line.
	Example:
	`export NUM_EXEC_SIMUL=5`

6	Save the changes in the file and exit the Vi editor.
7	Reboot.
8	Make sure the new value of the environment variable `NUM_EXEC_SIMUL` is set: `[Expert@MDS:0]# echo $NUM_EXEC_SIMUL` Output must show the configured value.

Unsetting the environment variable 'NUM_EXEC_SIMUL' permanently

This procedure removes the configured value for the environment variable `NUM_EXEC_SIMUL` for all shells (survives reboot):

Step	Instructions
1	Connect to the command line on the Multi-Domain Server.
2	Log in to the Expert mode.
3	Back up the current `/etc/rc.d/rc.local` file: `[Expert@MDS:0]# cp -v /etc/rc.d/rc.local{,_BKP_with_NUM_EXEC_SIMUL}`
4	Edit the current `/etc/rc.d/rc.local` file: `[Expert@MDS:0]# vi /etc/rc.d/rc.local`
5	Remove this line from the file: `export NUM_EXEC_SIMUL=<Number of Domain Management Servers>`
6	Save the changes in the file and exit the Vi editor.
7	Reboot.
8	Make sure the new value of the environment variable `NUM_EXEC_SIMUL` is not set: `[Expert@MDS:0]# echo $NUM_EXEC_SIMUL` Output must be empty.

mdsstop_customer

Description

Stops the specified Domain Management Server.

To stop the entire Multi-Domain Server, see the *"mdsstop" on page 777* command.

Syntax

```
mdsstop_customer <IP address or Name of Domain Management Server>
```

Notes:

- If the name of the Domain Management Server includes spaces, you must surround it with quotes ("*Name of Domain Management Server*").
- To start the specified Domain Management Server, run the *"mdsstart_customer" on page 774* command.

mgmt_cli

Description

The `mgmt_cli` tool works directly with the management database on your Management Server.

Syntax on Management Server or Security Gateway running on Gaia OS

```
mgmt_cli <Command Name> <Command Parameters> <Optional Switches>
```

Syntax on SmartConsole computer running on Windows OS 32-bit

Open Windows Command Prompt and run these commands:

```
cd /d "%ProgramFiles%\CheckPoint\SmartConsole\<VERSION>\PROGRAM\"
mgmt_cli.exe <Command Name> <Command Parameters> <Optional
Switches>
```

Syntax on SmartConsole computer running on Windows OS 64-bit

Open Windows Command Prompt and run these commands:

```
cd /d "%ProgramFiles
(x86)%\CheckPoint\SmartConsole\<VERSION>\PROGRAM\"
mgmt_cli.exe <Command Name> <Command Parameters> <Optional
Switches>
```

Notes

- For a complete list of the `mgmt_cli` options, enter the `mgmt_cli` (`mgmt_cli.exe`) command and press Enter.
- For more information, see the *Check Point Management API Reference* (at the top, select the correct version) .

migrate

Important - This command is used to migrate the management database from R80.10 and lower versions.
For more information, see the *R81.20 Installation and Upgrade Guide*.

Description

Exports the management database and applicable Check Point configuration.

Imports the exported management database and applicable Check Point configuration.

Backing up and restoring in Management High Availability environment:

- To back up and restore a consistent environment, make sure to collect and restore the backups and snapshots from all servers in the High Availability environment at the same time.
- Make sure other administrators do not make changes in SmartConsole until the backup operation is completed.

For more information:

- About Gaia Backup and Gaia Snapshot, see the *R81.20 Gaia Administration Guide*.
- About Virtual Machine Snapshots, see the vendor documentation.

Notes:

- You must run this command from the Expert mode.
- If it is necessary to back up the current management database, and you do **not** plan to import it on a Management Server that runs a higher software version, then you can use the built-in command in the `$FWDIR/bin/upgrade_tools/` directory.
- If you plan to import the management database on a Management Server that runs a higher software version, then you must use the `migrate` utility from the migration tools package created specifically for that higher software version. See the **Installation and Upgrade Guide** for that higher software version.
- If this command completes successfully, it creates this log file:
  `/var/log/opt/CPshrd-R81.20/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  For example: */var/log/opt/CPshrd-R81.20/migrate-2019.06.14_11.03.46.log*
- If this command fails, it creates this log file:
  `$CPDIR/log/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  For example: */opt/CPshrd-R81.20/log/migrate-2019.06.14_11.21.39.log*

Syntax

- To see the built-in help:

```
[Expert@MGMT:0]# ./migrate -h
```

- To export the management database and configuration:

```
[Expert@MGMT:0]# cd $FWDIR/bin/upgrade_tools/
[Expert@MGMT:0]# yes | nohup ./migrate export [-l | -x] [-n]
[--exclude-uepm-postgres-db] [--include-uepm-msi-files] /<Full
Path>/<Name of Exported File> &
```

- To import the management database and configuration:

```
[Expert@MGMT:0]# cd $FWDIR/bin/upgrade_tools/
[Expert@MGMT:0]# yes | nohup ./migrate import [-l | -x] [-n]
[--exclude-uepm-postgres-db] [--include-uepm-msi-files] /<Full
Path>/<Name of Exported File>.tgz &
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`yes | nohup ./migrate ... &`	This syntax: 1. Sends the "`yes`" input to the interactive "`migrate`" command through the pipeline. 2. The "`nohup`" forces the "`migrate`" command to ignore the hangup signals from the shell. 3. The "`&`" forces the command to run in the background. As a result, when the CLI session closes, the command continues to run in the background. See: ■ sk133312 ■ https://linux.die.net/man/1/bash ■ https://linux.die.net/man/1/nohup
`export`	Exports the management database and applicable Check Point configuration.
`import`	Imports the management database and applicable Check Point configuration that were exported from another Management Server.

Parameter	Description
`-l`	Exports and imports the Check Point logs *without* log indexes in the `$FWDIR/log/` directory. **Important:** ■ The command can export only closed logs (to which the information is not currently written). ■ If you use this parameter, it can take the command a long time to complete (depends on the number of logs).
`-x`	Exports and imports the Check Point logs *with* their log indexes in the `$FWDIR/log/` directory. **Important:** ■ This parameter only supports Management Servers and Log Servers R80.10 and higher. ■ The command can export only closed logs (to which the information is not currently written). ■ If you use this parameter, it can take the command a long time to complete (depends on the number of logs and indexes).
`-n`	Runs silently (non-interactive mode) and uses the default options for each setting. **Important:** ■ If you export a management database in this mode and the specified name of the exported file matches the name of an existing file, the command overwrites the existing file without prompting. ■ If you import a management database in this mode, the "`migrate import`" command runs the "`cpstop`" command automatically.
`--exclude-uepm-postgres-db`	■ During the export operation, does not back up the PostgreSQL database from the Endpoint Security Management Server. ■ During the import operation, does not restore the PostgreSQL database on the Endpoint Security Management Server.
`--include-uepm-msi-files`	■ During the export operation, backs up the MSI files from the Endpoint Security Management Server. ■ During the import operation, restores the MSI files on the Endpoint Security Management Server.
/<Full Path>/	Absolute path to the exported database file. This path must exist.

Parameter	Description
<Name of Exported File>	■ During the export operation, specifies the name of the output file. The command automatically adds the `*.tgz` extension. ■ During the import operation, specifies the name of the exported file. You must manually enter the `*.tgz` extension in the end.

Example 1 - Export operation succeeded

```
[Expert@MGMT:0]# cd $FWDIR/bin/upgrade_tools/
[Expert@MGMT:0]# ./migrate export /var/log/Migrate_Export

You are required to close all clients to Security Management Server
or execute 'cpstop' before the Export operation begins.

Do you want to continue? (y/n) [n]? y


Copying required files...
Compressing files...

The operation completed successfully.

Location of archive with exported database: /var/log/Migrate_Export.tgz

[Expert@MGMT:0]#
[Expert@MGMT:0]# find / -name migrate-\* -type f
/var/log/opt/CPshrd-R81.20/migrate-2019.06.14_11.03.46.log
[Expert@MGMT:0]#
```

Example 2 - Export operation failed

```
[Expert@MGMT:0]# ./migrate export /var/log/My_Migrate_Export
Execution finished with errors. See log file '/opt/CPshrd-R81.20/log/migrate-2019.06.14_
11.21.39.log' for further details
[Expert@MGMT:0]#
```

migrate_server

Important - This command is used to migrate the management database from R80.20.M1, R80.20, R80.20.M2, R80.30, and higher versions.
For more information, see:

- sk135172 - Upgrade Tools
- The *R81.20 Installation and Upgrade Guide*

Description

Exports the management database and applicable Check Point configuration.

Imports the exported management database and applicable Check Point configuration.

Backing up and restoring in Management High Availability environment:

- To back up and restore a consistent environment, make sure to collect and restore the backups and snapshots from all servers in the High Availability environment at the same time.
- Make sure other administrators do not make changes in SmartConsole until the backup operation is completed.

For more information:

- About Gaia Backup and Gaia Snapshot, see the *R81.20 Gaia Administration Guide*.
- About Virtual Machine Snapshots, see the vendor documentation.

Notes:

- You must run this command from the Expert mode.
- If it is necessary to back up the current management database, and you do **not** plan to import it on a Management Server that runs a higher software version, then you can use the built-in command in the `$FWDIR/scripts/` directory.
- If you plan to import the management database on a Management Server that runs a higher software version, then you must use the `migrate_server` utility from the migration tools package created specifically for that higher software version. See the **Installation and Upgrade Guide** for that higher software version.
- If this command completes successfully, it creates this log file:
  `/var/log/opt/CPshrd-R81.20/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  For example: */var/log/opt/CPshrd-R81.20/migrate-2022.06.14_11.03.46.log*
- If this command fails, it creates this log file:
  `$CPDIR/log/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  For example: */opt/CPshrd-R81.20/log/migrate-2022 - 2026.06.14_11.21.39.log*

Important - If it is necessary to back up the current management database, and you do **not** plan to import it on a Management Server that runs a higher software version, then you must make sure the source Management Server and the target Management Server run the same Jumbo Hotfix Accumulator Take and all other private hotfixes.
To see all the installed software packages, you can run this command: `cpinfo -y all`

Syntax

- To see the built-in help:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server -h
```

- To see the build number of the installed Upgrade Tools package:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server print_installed_tools -v
R81.20
```

- To run the Pre-Upgrade Verifier:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server verify -v R81.20 [-skip_
upgrade_tools_check]
```

- To export the management database and configuration:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server export -v R81.20 [-skip_
upgrade_tools_check] [-l | -x] [--include-uepm-msi-files] [--
exclude-uepm-postgres-db] [--ignore_warnings] /<Full
Path>/<Name of Exported File>
```

- To import the management database and configuration:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server import -v R81.20 [-skip_
upgrade_tools_check] [-l | -x] [/var/log/mdss.json] [--
include-uepm-msi-files] [--exclude-uepm-postgres-db] /<Full
Path>/<Name of Exported File>.tgz
```

- To import the Domain Management Server database and configuration on a Security Management Server:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server migrate_import_domain -v
R81.20 [-skip_upgrade_tools_check] [-l | -x]
[/var/log/mdss.json] [--include-uepm-msi-files] [--exclude-
uepm-postgres-db] /<Full Path>/<Name of Exported File>.tgz
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.

Parameter	Description
`--verify_all_servers`	Runs the Pre-Export Verifier for all Management Servers and Log Servers in your environment. **Notes**: ■ This parameter is valid only for the `migrate_server verify` and `migrate_server export` operations. ■ List of servers, on which you can run the `migrate_server verify -v <VERSION> --verify_all_servers` command and the `migrate_server export -v <VERSION> --verify_all_servers` command: • Security Management Server (Primary and Secondary) • Multi-Domain Security Management Server (Primary and Secondary) • Endpoint Security Management Server (Primary and Secondary) • Endpoint Security Management Server (Primary and Secondary) • Multi-Domain Log Server ■ List of remote servers, to which the `migrate_server verify -v <VERSION> --verify_all_servers` command and the `migrate_server export -v <VERSION> --verify_all_servers` command can connect from the current server: • Security Management Server (Primary and Secondary) • Multi-Domain Security Management Server (Primary and Secondary) • Endpoint Security Management Server (Primary and Secondary) • Endpoint Security Management Server (Primary and Secondary) • Multi-Domain Log Server • Dedicated Log Servers • Dedicated SmartEvent Servers • Security Management Servers configured as a Backup of a Domain Management Server **Note** - Servers that are configured on a specific Domain on a Multi-Domain Security Management Server will be verified only if there is a Domain Server of that Domain on the current Multi-Domain Security Management Server.

Parameter	Description
`--verify_local_only`	Runs the Pre-Export Verifier only for the current Management Server / Log Server, on which you run this command. **Note** - This parameter is valid only for the `migrate_server verify` and `migrate_server export` operations.
`-skip_tools_check_on_remote`	The remote Management Server / Log Servers do not try to connect to Check Point Cloud to check for a more recent version of the Upgrade Tools. **Notes**: ■ This parameter is valid only for the `migrate_server verify` and `migrate_server export` operations. ■ This parameter is valid only when you specify the parameter `--verify_all_servers`.
`export`	Exports the management database and applicable Check Point configuration.

Parameter	Description

`import`	Imports the management database and applicable Check Point configuration that were exported from another Management Server.
	Important:
	■ This command automatically restarts Check Point services (runs the "`cpstop`" and "`cpstart`" commands).
	■ This note applies to a Multi-Domain Security Management environment, if at least one of the servers changes its IPv4 address comparing to the source server, from which you exported its database.
	You must do these steps **before** you start the upgrade and import:
	1. You must create a special JSON configuration file with the new IPv4 address(es).
	Syntax:
	`[{"name":"<Name of Server 1 Object in SmartConsole>","newIpAddress4":"<New IPv4 Address of Server 1>"},`
	`{"name":"<Name of Server 2 Object in SmartConsole>","newIpAddress4":"<New IPv4 Address of Server 2>"}]`
	Example:
	`[{"name":"MyPrimaryMultiDomainServer","newIpAddress4":"172.30.40.51"},`
	`{"name":"MySecondaryMultiDomainServer","newIpAddress4":"172.30.40.52"}]`
	2. You must call this file: **mdss.json**
	3. You must put this file on **all** servers in this directory: **/var/log/**

`migrate_import_domain`	On a Security Management Server, imports the management database and applicable Check Point configuration that were exported from a Domain Management Server. **Important** - This command automatically restarts Check Point services (runs the "`cpstop`" and "`cpstart`" commands).
`verify`	Verifies the management database and applicable Check Point configuration that were exported from another Management Server.
`-v R81.20`	Specifies the version, to which you plan to migrate / upgrade.

Parameter	Description
`-skip_ upgrade_ tools_check`	The current Management Server / Log Server, on which you run this command, does not try to connect to Check Point Cloud to check for a more recent version of the Upgrade Tools. **Best Practice** - Use this parameter on the Management Server / Log Server that is **not** connected to the Internet.
`-l`	Exports and imports the Check Point logs *without* log indexes in the `$FWDIR/log/` directory. **Important:** ■ The command can export only closed logs (to which the information is not currently written). ■ If you use this parameter, it can take the command a long time to complete (depends on the number of logs).
`-l <Days>`	Exports the specified number of previous days of logs without log indexes.
`-x`	Exports and imports the Check Point logs *with* their log indexes in the `$FWDIR/log/` directory. **Important:** ■ Before you use this parameter, it is necessary to make sure all log indexes are closed and saved. Run this command in the Expert mode and wait for the output to show "`Solr stopped`": `$RTDIR/scripts/stopSolr.sh` ■ This parameter only supports Management Servers and Log Servers R80.10 and higher. ■ The command can export only closed logs (to which the information is not currently written). ■ If you use this parameter, it can take the command a long time to complete (depends on the number of logs and indexes).
`-x <Days>`	Exports the specified number of previous days of logs with log indexes.
`-n`	Runs silently (non-interactive mode) and uses the default options for each setting.

Parameter	Description

`/var/log/mdss.json`
 	
Previously:
`-change_ips_file /<Full Path>/<Name>.json`
	Important:
	■ In the Upgrade Tools for R81.10 build higher than 996000356, the syntax is (this filename is mandatory):
	`/var/log/mdss.json`
	You must create the file **/var/log/mdss.json** and not use the parameter "**-change_ips_file**".
	■ In the Upgrade Tools for R81.10 build 996000356 and lower, the syntax was:
	`-change_ips_file /<Full Path>/<Name of JSON File>.json`
	
	Specifies the absolute path to the special JSON configuration file with new IPv4 addresses.
	This file is mandatory during an upgrade of a Multi-Domain Security Management environment.
	Even if only one of the servers migrates to a new IP address, all the other servers must get this configuration file for the import process.
	Syntax:
	`[{"name":"<Name of Server 1 Object in SmartConsole>","newIpAddress4":"<New IPv4 Address of Server 1>"},`
	`{"name":"<Name of Server 2 Object in SmartConsole>","newIpAddress4":"<New IPv4 Address of Server 2>"}]`
	Example:
	`[{"name":"MyPrimaryMultiDomainServer","newIpAddress4":"172.30.40.51"},`
	`{"name":"MySecondaryMultiDomainServer","newIpAddress4":"172.30.40.52"}]`

`--include-uepm-msi-files`	■ During the export operation, backs up the MSI files from the Endpoint Security Management Server. ■ During the import operation, restores the MSI files on the Endpoint Security Management Server.
`--exclude-uepm-postgres-db`	■ During the export operation, does not back up the PostgreSQL database from the Endpoint Security Management Server. ■ During the import operation, does not restore the PostgreSQL database on the Endpoint Security Management Server.

Parameter	Description
`--ignore_warnings` or `-ivw`	If during an upgrade procedure, the Pre-Upgrade Verifier shows warnings, you can use this parameter to ignore warnings and continue the upgrade. **Important** - To prevent issues during and after upgrade, we strongly recommend to resolve all issues and not use this parameter.
`--exclude-licenses`	■ During the export operation, does not back up the licenses from the Management Server. ■ During the import operation, does not restore the license on the Management Server.
`-force-upgrade-flow`	When the source and target servers are on the same major version: ■ "`migrate_server`" uses an accelerated flow to migrate the data. ■ This flag forces the full migration flow.
`-mask`	Hides sensitive information in exported database.
`--no_progress_bar` or `-npb`	Disables the progress bar.
`-o <Path to File>`	Path to the archived file from which to import the database.
`-sn <Name of Domain Server>`	Name of the Domain Management Server
`-dsi <IP address of Domain Server>`	IP address of the Management Server.
`-skip_logs`	Skips the import of logs (without log indexes).

Example 1 - Export operation succeeded

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server export -v R81.20 /var/log/Migrate_Export

You are required to close all clients to Security Management Server
or execute 'cpstop' before the Export operation begins.

Do you want to continue? (y/n) [n]? y


Copying required files...
Compressing files...

The operation completed successfully.

Location of archive with exported database: /var/log/Migrate_Export.tgz

[Expert@MGMT:0]#
[Expert@MGMT:0]# find / -name migrate-\* -type f
/var/log/opt/CPshrd-R81.20/migrate-2022 - 2026.06.14_11.03.46.log
[Expert@MGMT:0]#
```

Example 2 - Export operation failed

```
[Expert@MGMT:0]# ./migrate_server export /var/log/My_Migrate_Export
Execution finished with errors. See log file '/opt/CPshrd-R81.20/log/migrate-2022 - 2026.06.14_
11.21.39.log' for further details
[Expert@MGMT:0]#
```

migrate_global_policies

Description

This utility transfers (and upgrades, if necessary) the global configuration database from one Multi-Domain Server to another Multi-Domain Server.

Notes:

- You can only use this command when the target Multi-Domain Server does **not** have global configurations defined.
- This utility replaces all existing global configurations. Each existing global configuration is saved with a `*.pre_migrate` extension.
- If you migrate only the global configurations (without the Domain Management Servers) to a new Multi-Domain Server, disable all Security Gateways that are enabled for global use.

Important - You cannot export an R80.X global configuration database and then use this utility on an R80.X Multi-Domain Server.

Syntax

```
migrate_global_policies <Path>
```

Parameters

Parameter	Description
<Path>	The **fully qualified** path to the directory where the global policies files, originally exported from the source Multi-Domain Server (`$MDSDIR/conf/`), are located.

Example

```
Expert@R81.20_MDS:0]# migrate_global_policies /var/log/exported_global_db.22Jul2019-124547.tgz
```

queryDB_util

Description

Searches in the management database for objects or policy rules.

Important - This command is obsolete for R80 and higher. Use the *"mgmt_cli" on page 386* command to search in the management database for objects or policy rules according to search parameters.

rs_db_tool

Description

Manages Dynamically Assigned IP address (DAIP) gateways in a DAIP database.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax

- **To add an entry to the DAIP database:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation add -name <Object Name> -ip <IPv4 Address> -ip6 <Pv6 Address> -TTL <Time-To-Live>
```

- **To fetch a specific entry from the DAIP database:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation fetch -name <Object Name>
```

- **To delete a specific entry from the DAIP database:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation delete -name <Object Name>
```

- **To list all entries in the DAIP database:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation list
```

- **To synchronize the DAIP database:**

```
[Expert@MGMT:0]# rs_db_tool [-d] -operation sync
```

Note - You must run this command from the Expert mode.

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-name <Object Name>`	Specifies the name of the DAIP object.
`-ip <IPv4 Address>`	Specifies the IPv4 address of the DAIP object
`-ip6 <IPv6 Address>`	Specifies the IPv6 address of the DAIP object.
`-TTL <Time-To-Live>`	Specifies the relative time interval (in seconds), during which the entry is valid.

sam_alert

Description

For SAM v1, this utility executes Suspicious Activity Monitoring (SAM) actions according to the information received from the standard input.

For SAM v2, this utility executes Suspicious Activity Monitoring (SAM) actions with User Defined Alerts mechanism.

Important:

- You must run this command on the Management Server.
- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Notes:

- VSX Gateways and VSX Cluster Members do **not** support Suspicious Activity Monitoring (SAM) Rules. See sk79700.
- See the *"fw sam" on page 295* and *"fw sam_policy" on page 303* commands.

SAM v1 syntax

```
sam_alert [-v] [-o] [-s <SAM Server>] [-t <Time>] [-f <Security
Gateway>] [-C] {-n|-i|-I} {-src|-dst|-any|-srv}
```

Parameters for SAM v1

Parameter	Description
`-v`	Enables the verbose mode for the "`fw sam`" command.
`-o`	Specifies to print the input of this tool to the standard output (to use with pipes in a CLI syntax).
`-s <SAM Server>`	Specifies the SAM Server to be contacted. Default is "localhost".
`-t <Time>`	Specifies the time (in seconds), during which to enforce the action. The default is forever.

Parameter	Description
`-f <Security Gateway>`	Specifies the Security Gateway / Cluster object, on which to run the operation. **Important** - If you do not specify the target Security Gateway / Cluster object explicitly, this command applies to all managed Security Gateways and Clusters.
`-C`	Cancels the specified operation.
`-n`	Specifies to notify every time a connection, which matches the specified criteria, passes through the Security Gateway / ClusterXL / Security Group.
`-i`	Inhibits (drops or rejects) connections that match the specified criteria.
`-I`	Inhibits (drops or rejects) connections that match the specified criteria and closes all existing connections that match the specified criteria.
`-src`	Matches the source address of connections.
`-dst`	Matches the destination address of connections.
`-any`	Matches either the source or destination address of connections.
`-srv`	Matches specific source, destination, protocol and port.

SAM v2 syntax

```
sam_alert -v2 [-v] [-O] [-S <SAM Server>] [-t <Time>] [-f
<Security Gateway>] [-n <Name>] [-c "<Comment">] [-o
<Originator>] [-l {r | a}] -a {d | r| n | b | q | i} [-C] {-ip
|-eth} {-src|-dst|-any|-srv}
```

Parameters for SAM v2

Parameter	Description
`-v2`	Specifies to use SAM v2.
`-v`	Enables the verbose mode for the "`fw sam`" command.
`-O`	Specifies to print the input of this tool to the standard output (to use with pipes in a CLI syntax).
`-S <SAM Server>`	Specifies the SAM server to be contacted. Default is "localhost".
`-t <Time>`	Specifies the time (in seconds), during which to enforce the action. The default is forever.
`-f <Security Gateway>`	Specifies the Security Gateway / Cluster object, on which to run the operation. **Important** - If you do not specify the target Security Gateway / Cluster object explicitly, this command applies to all managed Security Gateways and Clusters.
`-n <Name>`	Specifies the name for the SAM rule. Default is empty.
`-c "<Comment>"`	Specifies the comment for the SAM rule. Default is empty. You must enclose the text in the double quotes or single quotes.
`-o <Originator>`	Specifies the originator for the SAM rule. Default is "`sam_alert`".

Parameter	Description
`-l {r | a}`	Specifies the log type for connections that match the specified criteria: ■ `r` - Regular ■ `a` - Alert Default is `None`.
`-a {d | r| n | b | q | i}`	Specifies the action to apply on connections that match the specified criteria: ■ `d` - Drop ■ `r` - Reject ■ `n` - Notify ■ `b` - Bypass ■ `q` - Quarantine ■ `i` - Inspect
`-C`	Specifies to close all existing connections that match the criteria.
`-ip`	Specifies to use IP addresses as criteria parameters.
`-eth`	Specifies to use MAC addresses as criteria parameters.
`-src`	Matches the source address of connections.
`-dst`	Matches the destination address of connections.
`-any`	Matches either the source or destination address of connections.
`-srv`	Matches specific source, destination, protocol and port.

Example

See sk110873: How to configure Security Gateway to detect and prevent port scan.

stattest

Description

Check Point AMON client to query SNMP OIDs.

You can use this command as an alternative to the standard SNMP commands for debug purposes - to make sure the applicable SNMP OIDs provide the requested information.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax to query a Regular OID

- On a Management Server / Security Gateway / Cluster Member:

```
stattest get [-d] [-h <Host>] [-p <Port>] [-x <Proxy Server>] [-v <VSID>] [-t <Timeout>] <Regular_OID_1> <Regular_OID_2> ...
<Regular_OID_N>
```

- On a Scalable Platform Security Group:

```
g_all stattest get [-d] [-h <Host>] [-p <Port>] [-x <Proxy Server>] [-v <VSID>] [-t <Timeout>] <Regular_OID_1> <Regular_OID_2>
... <Regular_OID_N>
```

Notes:

- These Regular OIDs are specified in the SNMP MIB files.
- For Check Point MIB files, see sk90470.

Syntax to query a Statistical OID

- On a Management Server / Security Gateway / Cluster Member:

```
stattest get [-d] [-h <Host>] [-p <Port>] [-x <Proxy Server>] -l <Polling Interval> -r <Polling Duration> [-v <VSID>] [-t
<Timeout>] <Statistical_OID_1> <Statistical_OID_2> ... <Statistical_OID_N>
```

- On a Scalable Platform Security Group:

```
g_all stattest get [-d] [-h <Host>] [-p <Port>] [-x <Proxy Server>] -l <Polling Interval> -r <Polling Duration> [-v <VSID>] [-t
<Timeout>] <Statistical_OID_1> <Statistical_OID_2> ... <Statistical_OID_N>
```

Notes:

- These Statistical OIDs take some time to "initialize".
- For example, to calculate an average, it is necessary to collect enough samples.
- Check Point statistical OIDs are registered in the `$CPDIR/conf/statistical_oid.conf` file.

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-h <Host>`	Specifies the remote Check Point host to query by its IP address or resolvable hostname.
`-p <Port>`	Specifies the port number, on which the AMON server listens. Default port is 18192.
`-x <Proxy Server>`	Specifies the Proxy Server by its IP address or resolvable hostname. **Note** - Use only when you query a remote host.
`-l <Polling Interval>`	Specifies the time in seconds between queries. **Note** - Use only when you query a Statistical OID.

Parameter	Description
`-r <Polling Duration>`	Specifies the time in seconds, during which to run consecutive queries. **Note** - Use only when you query a Statistical OID.
`-v <VSID>`	On a VSX Gateway, specifies the context of a Virtual Device to query.
`-t <Timeout>`	Specifies the session timeout in milliseconds.
`<Regular_OID_1> <Regular_OID_2> ... <Regular_OID_N>`	Specifies the Regular OIDs to query. **Notes:** ■ OID must not start with period. ■ Separate the OIDs with spaces. ■ You can specify up to 100 OIDs.
`<Statistical_OID_1> <Statistical_OID_2> ... <Statistical_OID_N>`	Specifies the Statistical OIDs to query. **Notes:** ■ OID must not start with period. ■ Separate the OIDs with spaces. ■ You can specify up to 100 OIDs.

Example - Query a Regular OID

Query the CPU Idle utilization at the OID 1.3.6.1.4.1.2620.1.6.7.2.3 (`procIdleTime`).

```
[Expert@HostName]# stattest get 1.3.6.1.4.1.2620.1.6.7.4.2
```

Example - Query a Statistical OID

Query the CPU Idle utilization at the OID 1.3.6.1.4.1.2620.1.6.7.2.3 (`procIdleTime`).

Information is collected with intervals of 5 seconds during 5 seconds

```
[Expert@HostName]# stattest get -l 5 -r 5 1.3.6.1.4.1.2620.1.6.7.2.3
```

threshold_config

Description

You can configure a variety of different SNMP thresholds that generate SNMP traps, or alerts.

You can use these thresholds to monitor many system components automatically without requesting information from each object or device.

You configure these SNMP Monitoring Thresholds only on the Security Management Server, Multi-Domain Server, or Domain Management Server.

During policy installation, the managed a Security Gateway and Clusters receive and apply these thresholds as part of their policy.

For more information, see sk90860: How to configure SNMP on Gaia OS.

Procedure

Step	Instructions
1	Connect to the command line on the Management Server.
2	Log in to the Expert mode.
3	On a Multi-Domain Server, switch to the context of the applicable Domain Management Server: `[Expert@HostName:0]# mdsenv <Name or IP address of Domain Management Server>`
4	Go to the Threshold Engine Configuration menu: `[Expert@HostName:0]# threshold_config`

Step	Instructions

5	Select the applicable options and configure the applicable settings (see the **Threshold Engine Configuration Options** table below).
	`Threshold Engine Configuration Options:`
	`----------`
	
	`(1) Show policy name`
	`(2) Set policy name`
	`(3) Save policy`
	`(4) Save policy to file`
	`(5) Load policy from file`
	`(6) Configure global alert settings`
	`(7) Configure alert destinations`
	`(8) View thresholds overview`
	`(9) Configure thresholds`
	
	`(e) Exit (m) Main Menu`
	
	`Enter your choice (1-9) :`

6	Exit from the Threshold Engine Configuration menu.
7	Stop the CPD daemon: `[Expert@HostName:0]# cpwd_admin stop -name CPD -path "$CPDIR/bin/cpd_admin" -command "cpd_admin stop"` See *"cpwd_admin stop" on page 248*.
8	Start the CPD daemon: `[Expert@HostName:0]# cpwd_admin start -name CPD -path "$CPDIR/bin/cpd" -command "cpd"` See *"cpwd_admin start" on page 244*.
9	Wait for 10-20 seconds.
10	Verify that CPD daemon started successfully: `[Expert@HostName:0]# cpwd_admin list | egrep "STAT|CPD"` See *"cpwd_admin list" on page 238*.
11	In SmartConsole, install the Access Control Policy on Security Gateways and Clusters.

Threshold Engine Configuration Options

Menu item	Description
`(1) Show policy name`	Shows the name of the current configured threshold policy.
`(2) Set policy name`	Configures the name for the threshold policy. If you do not specify it explicitly, then the default name is "`Default Profile`".
`(3) Save policy`	Saves the changes in the current threshold policy.
`(4) Save policy to file`	Exports the configured threshold policy to a file. If you do not specify the path explicitly, the file is saved in the current working directory.
`(5) Load policy from file`	Imports a threshold policy from a file. If you do not specify the path explicitly, the file is imported from the current working directory.
`(6) Configure global alert settings`	Configures global settings: ■ How frequently alerts are sent (configured delay must be greater than 30 seconds) ■ How many alerts are sent

`(7) Configure alert destinations`	Configures the SNMP Network Management System (NMS), to which the managed Security Gateways and Cluster Members send their SNMP alerts.
	`Configure Alert Destinations Options:`
	`----------`
	`(1) View alert destinations`
	`(2) Add SNMP NMS`
	`(3) Remove SNMP NMS`
	`(4) Edit SNMP NMS`

`(8) View thresholds overview`	Shows a list of all available thresholds and their current settings. These include: ■ Name ■ Category (see the next option "`(9)`") ■ State (disabled or enabled) ■ Threshold (threshold point, if applicable) ■ Description

Menu item	Description

(9) Configure thresholds	Shows the list of threshold categories to configure.
	`Thresholds Categories`
	`----------`
	`(1) Hardware`
	`(2) High Availability`
	`(3) Local Logging Mode Status`
	`(4) Log Server Connectivity`
	`(5) Networking`
	`(6) Resources`
	See the **Thresholds Categories** table below.

Thresholds Categories

Category	Sub-Categories

(1) Hardware	`Hardware Thresholds:`
	`----------`
	`(1) RAID volume state`
	`(2) RAID disk state`
	`(3) RAID disk flags`
	`(4) Temperature sensor reading`
	`(5) Fan speed sensor reading`
	`(6) Voltage sensor reading`

(2) High Availability	`High Availability Thresholds:`
	`----------`
	`(1) Cluster member state changed`
	`(2) Cluster block state`
	`(3) Cluster state`
	`(4) Cluster problem status`
	`(5) Cluster interface status`

(3) Local Logging Mode Status	`Local Logging Mode Status Thresholds:`
	`----------`
	`(1) Local Logging Mode`

(4) Log Server Connectivity	`Log Server Connectivity Thresholds:`
	`----------`
	`(1) Connection with log server`
	`(2) Connection with all log servers`

Category	Sub-Categories
(5) Networking	Networking Thresholds: ---------- (1) Interface Admin Status (2) Interface removed (3) Interface Operational Link Status (4) New connections rate (5) Concurrent connections rate (6) Bytes Throughput (7) Accepted Packet Rate (8) Drop caused by excessive traffic
(6) Resources	Resources Thresholds: ---------- (1) Swap Memory Utilization (2) Real Memory Utilization (3) Partition free space (4) Core Utilization (5) Core interrupts rate

Notes:

- If you run the `threshold_config` command *locally* on a Security Gateway or Cluster Members to configure the SNMP Monitoring Thresholds, then each policy installation erases these *local* SNMP threshold settings and reverts them to the *global* SNMP threshold settings configured on the Management Server that manages this Security Gateway or Cluster.
- On a Security Gateway and Cluster Members, you can save the local Threshold Engine Configuration settings to a file and load it locally later.
- The Threshold Engine Configuration is stored in the `$FWDIR/conf/thresholds.conf` file.
- In a Multi-Domain Security Management environment:
  - You can configure the SNMP thresholds in the context of Multi-Domain Server (MDS) and in the context of each individual Domain Management Server.
  - Thresholds that you configure in the context of the Multi-Domain Server are for the Multi-Domain Server only.
  - Thresholds that you configure in the context of a Domain Management Server are for that Domain Management Server and its managed Security Gateway and Clusters.
  - If an SNMP threshold applies both to the Multi-Domain Server and a Domain Management Server, then configure the SNMP threshold both in the context of the Multi-Domain Server and in the context of the Domain Management Server.
    However, in this scenario you can only get alerts from the Multi-Domain Server, if the monitored object exceeds the threshold.
    Example:
    If you configure the CPU threshold, then when the monitored value exceeds the configured threshold, it applies to both the Multi-Domain Server and the Domain Management Server. However, only the Multi-Domain Server generates SNMP alerts.

$MDSVERUTIL

Description

This utility returns information about the Multi-Domain Server and Domain Management Servers.

This utility is intended for internal use by Check Point scripts on the Multi-Domain Server.

You can use this utility to get some information about the Multi-Domain Server and Domain Management Servers (for example, the names of all Domain Management Servers).

Syntax

```
$MDSVERUTIL help
```

```
$MDSVERUTIL
      AllCMAs <options>
      AllVersions
      CMAAddonDir <options>
      CMACompDir <options>
      CMAFgDir <options>
      CMAFw40Dir <options>
      CMAFw41Dir <options>
      CMAFwConfDir <options>
      CMAFwDir <options>
      CMAIp <options>
      CMAIp6 <options>
      CMALogExporterDir <options>
      CMALogIndexerDir <options>
      CMANameByFwDir <options>
      CMANameByIp <options>
      CMARegistryDir <options>
      CMAReporterDir <options>
      CMASmartLogDir <options>
      CMASvnConfDir <options>
      CMASvnDir <options>
      ConfDirVersion <options>
      CpdbUpParam <options>
      CPprofileDir <options>
      CPVer <options>
      CustomersBaseDir <options>
      DiskSpaceFactor <options>
      InstallationLogDir <options>
      IsIPv6Enabled
      IsLegalVersion <options>
      IsOsSupportsIPv6
      LatestVersion
      MDSAddonDir <options>
      MDSCompDir <options>
      MDSDir <options>
      MDSFgDir <options>
      MDSFwbcDir <options>
      MDSFwDir <options>
      MDSIp <options>
      MDSIp6 <options>
      MDSLogExporterDir <options>
      MDSLogIndexerDir <options>
      MDSPkgName <options>
      MDSRegistryDir <options>
      MDSReporterDir <options>
```

```
MDSSmartLogDir <options>
MDSSvnDir <options>
MDSVarCompDir <options>
MDSVarDir <options>
MDSVarFwbcDir <options>
MDSVarFwDir <options>
MDSVarSvnDir <options>
MSP <options>
OfficialName <options>
OptionPack <options>
ProductName <options>
RegistryCurrentVer <options>
ShortOfficialName <options>
SmartCenterPuvUpgradeParam <options>
SP <options>
SVNPkgName <options>
SvrDirectory <options>
SvrParam <options>
```

Parameters

Parameter	Description
`help`	Shows the list of available commands.
`AllCMAs <options>`	Returns the list of names of the configured Domain Management Servers. See *"$MDSVERUTIL AllCMAs" on page 826*.
`AllVersions`	Returns the internal representation of versions, this Multi-Domain Server recognizes. See *"$MDSVERUTIL AllVersions" on page 827*.
`CMAAddonDir <options>`	Returns the path to the Management Addon directory in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMAAddonDir" on page 830*.
`CMACompDir <options>`	Returns the full path for the specified Backward Compatibility Package in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMACompDir" on page 831*.

Parameter	Description
`CMAFgDir <options>`	Returns the full path for the `$FGDIR` directory in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMAFgDir" on page 832*.
`CMAFw40Dir <options>`	Returns the full path for the `$FWDIR` directory for FireWall-1 4.0 in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMAFw40Dir" on page 833*.
`CMAFw41Dir <options>`	Returns the full path for the `$FWDIR` directory for Edge devices (that are based on FireWall-1 4.1) in the context of the specified Domain Management Server. **Note** - R81.20 does not support UTM-1 Edge and Safe@Office devices. The information about this command is provided only to describe the existing syntax option until it is removed completely. See *"$MDSVERUTIL CMAFw41Dir" on page 834*.
`CMAFwConfDir <options>`	Returns the full path for the `$FWDIR/conf/` directory in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMAFwConfDir" on page 835*.
`CMAFwDir <options>`	Returns the full path for the `$FWDIR` directory in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMAFwDir" on page 836*.
`CMAIp <options>`	Returns the IPv4 address of the Domain Management Server specified by its name. See *"$MDSVERUTIL CMAIp" on page 837*.
`CMAIp6 <options>`	Returns the IPv6 address of the Domain Management Server specified by its name. See *"$MDSVERUTIL CMAIp6" on page 838*.
`CMALogExporterDir <options>`	Returns the full path for the `$EXPORTERDIR` directory in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMALogExporterDir" on page 839*.

Parameter	Description
`CMALogIndexerDir <options>`	Returns the full path for the `$INDEXERDIR` directory in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMALogIndexerDir" on page 840*.
`CMANameByFwDir <options>`	Returns the name of the Domain Management Server based on the context of the current `$FWDIR` directory. See *"$MDSVERUTIL CMANameByFwDir" on page 841*.
`CMANameByIp <options>`	Returns the name of the Domain Management Server based on the specified IPv4 address. See *"$MDSVERUTIL CMANameByIp" on page 842*.
`CMARegistryDir <options>`	Returns the full path for the `$CPDIR/registry/` directory in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMARegistryDir" on page 843*.
`CMAReporterDir <options>`	Returns the full path for the `$RTDIR` directory in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMAReporterDir" on page 844*.
`CMASmartLogDir <options>`	Returns the full path for the `$SMARTLOGDIR` directory in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMASmartLogDir" on page 845*.
`CMASvnConfDir <options>`	Returns the full path for the `$CPDIR/conf/` directory in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMASvnConfDir" on page 846*.
`CMASvnDir <options>`	Returns the full path for the `$CPDIR` directory in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMASvnDir" on page 847*.

Parameter	Description
`ConfDirVersion <options>`	Returns the internal Version ID based on the context of the current `$FWDIR/conf/` directory. See *"$MDSVERUTIL ConfDirVersion" on page 848*.
`CpdbUpParam <options>`	Returns internal version numbers from the internal database. See *"$MDSVERUTIL CpdbUpParam" on page 849*.
`CPprofileDir <options>`	Returns the path to the directory that contains the `.CPprofile.sh` and the `.CPprofile.csh` shell scripts. See *"$MDSVERUTIL CPprofileDir" on page 850*.
`CPVer <options>`	Returns internal Check Point version number. See *"$MDSVERUTIL CPVer" on page 851*.
`CustomersBaseDir <options>`	Returns the full path for the `$MDSDIR/customers/` directory. See *"$MDSVERUTIL CustomersBaseDir" on page 852*.
`DiskSpaceFactor <options>`	Returns the disk-space factor (the `mds_setup` command uses this value during an upgrade). See *"$MDSVERUTIL DiskSpaceFactor" on page 853*.
`InstallationLogDir <options>`	Returns the full path for directory with all installation logs (`/opt/CPInstLog/`). See *"$MDSVERUTIL InstallationLogDir" on page 854*.
`IsIPv6Enabled`	Returns `true`, if IPv6 is enabled in Gaia OS. Returns `false`, if IPv6 is disabled in Gaia OS. See *"$MDSVERUTIL IsIPv6Enabled" on page 855*.
`IsLegalVersion <options>`	Returns 0, if the specified internal Version ID is legal. Returns 1, if the specified internal Version ID is illegal. See *"$MDSVERUTIL IsLegalVersion" on page 856*.

Parameter	Description
`IsOsSupportsIPv6`	Returns `true`, if the OS supports IPv6. Returns `false`, if the OS does not support IPv6. See *"$MDSVERUTIL IsOsSupportsIPv6" on page 857*.
`LatestVersion`	Returns the internal Version ID of the latest installed version. See *"$MDSVERUTIL LatestVersion" on page 858*.
`MDSAddonDir <options>`	Returns the path to the Management Addon directory in the MDS context. See *"$MDSVERUTIL MDSAddonDir" on page 859*.
`MDSCompDir <options>`	Returns the full path for the specified Backward Compatibility Package in the MDS context. See *"$MDSVERUTIL MDSCompDir" on page 860*.
`MDSDir <options>`	Returns the full path in the `/opt/` directory to the `$MDSDIR` directory. See *"$MDSVERUTIL MDSDir" on page 861*.
`MDSFgDir <options>`	Returns the full path for the `$FGDIR` directory in the MDS context. See *"$MDSVERUTIL MDSFgDir" on page 862*.
`MDSFwbcDir <options>`	Returns the full path in the `/opt/` directory (in the MDS context) for the Backward Compatibility directory for Edge devices. See *"$MDSVERUTIL MDSFwbcDir" on page 863*.
`MDSFwDir <options>`	Returns the full path in the `/opt/` directory for the `$FWDIR` directory in the MDS context. See *"$MDSVERUTIL MDSFwDir" on page 864*.
`MDSIp <options>`	Returns the IPv4 address of Multi-Domain Server. See *"$MDSVERUTIL MDSIp" on page 865*.
`MDSIp6 <options>`	Returns the IPv6 address of Multi-Domain Server. See *"$MDSVERUTIL MDSIp6" on page 866*.
`MDSLogExporterDir <options>`	Returns the full path for the `$EXPORTERDIR` directory in the MDS context. See *"$MDSVERUTIL MDSLogExporterDir" on page 867*.

Parameter	Description
`MDSLogIndexerDir <options>`	Returns the full path for the `$INDEXERDIR` directory in the MDS context. See *"$MDSVERUTIL MDSLogIndexerDir" on page 868*.
`MDSPkgName <options>`	Returns the name of the MDS software package. See *"$MDSVERUTIL MDSPkgName" on page 869*.
`MDSRegistryDir <options>`	Returns the full path for the `$CPDIR/registry/` directory in the MDS context. See *"$MDSVERUTIL MDSRegistryDir" on page 870*.
`MDSReporterDir <options>`	Returns the full path for the `$RTDIR` directory in the MDS context. See *"$MDSVERUTIL MDSReporterDir" on page 871*.
`MDSSmartLogDir <options>`	Returns the full path for the `$SMARTLOGDIR` directory in the MDS context. See *"$MDSVERUTIL MDSSmartLogDir" on page 872*.
`MDSSvnDir <options>`	Returns the full path in the `/opt/` directory for the `$CPDIR` directory in the MDS context. See *"$MDSVERUTIL MDSSvnDir" on page 873*.
`MDSVarCompDir <options>`	Returns the full path in the `/var/opt/` directory for the specified Backward Compatibility Package in the MDS context. See *"$MDSVERUTIL MDSVarCompDir" on page 874*.
`MDSVarDir <options>`	Returns the full path in the `/var/opt/` directory to the `$MDSDIR` directory. See *"$MDSVERUTIL MDSVarCompDir" on page 874*.
`MDSVarFwbcDir <options>`	Returns the full path in the `/var/opt/` directory (in the MDS context) for the Backward Compatibility directory for Edge devices. See *"$MDSVERUTIL MDSVarFwbcDir" on page 876*.

Parameter	Description
`MDSVarFwDir <options>`	Returns the full path in the `/var/opt/` directory for the `$FWDIR` directory in the MDS context. See *"$MDSVERUTIL MDSVarFwDir" on page 877*.
`MDSVarSvnDir <options>`	Returns the full path in the `/var/opt/` directory for the `$CPDIR` directory in the MDS context. See *"$MDSVERUTIL MDSVarSvnDir" on page 878*.
`MSP <options>`	Returns the Minor Service Pack version. See *"$MDSVERUTIL MSP" on page 879*.
`OfficialName <options>`	Returns the official version name. See *"$MDSVERUTIL OfficialName" on page 880*.
`OptionPack <options>`	Returns the internal Option Pack version. See *"$MDSVERUTIL OptionPack" on page 881*.
`ProductName <options>`	Returns the official name of the Multi-Domain Server product. See *"$MDSVERUTIL ProductName" on page 882*.
`RegistryCurrentVer <options>`	Returns the current internal version of Check Point Registry. See *"$MDSVERUTIL RegistryCurrentVer" on page 883*.
`ShortOfficialName <options>`	Returns the short (without spaces) official version name. See *"$MDSVERUTIL ShortOfficialName" on page 884*.
`SmartCenterPuvUpgradeParam <options>`	Returns the version to the Pre-Upgrade Verifier (PUV) in order for it to upgrade to that version. See *"$MDSVERUTIL SmartCenterPuvUpgradeParam" on page 885*.
`SP <options>`	Returns the Service Pack version. See *"$MDSVERUTIL SP" on page 886*.
`SVNPkgName <options>`	Returns the name of the Secure Virtual Network (SVN) package. See *"$MDSVERUTIL SVNPkgName" on page 887*.

Parameter	Description
`SvrDirectory <options>`	Returns the full path for the SmartReporter directory. See *"$MDSVERUTIL SvrDirectory" on page 888*.
`SvrParam <options>`	Returns the SmartReporter version. See *"$MDSVERUTIL SvrParam" on page 889*.

$MDSVERUTIL AllCMAs

Description

Returns the list of names of the configured Domain Management Servers.

Syntax

```
$MDSVERUTIL AllCMAs [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL AllCMAs
MyDomain_Server_1
MyDomain_Server_2
MyDomain_Server_3
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL AllCMAs -v VID_92
MyDomain_Server_1
MyDomain_Server_2
MyDomain_Server_3
[Expert@MDS:0]#
```

$MDSVERUTIL AllVersions

Description

Returns the internal representation of versions, this Multi-Domain Server recognizes.

You can you these internal version strings in other commands.

In addition, see these commands:

- *"$MDSVERUTIL IsLegalVersion" on page 856*
- *"$MDSVERUTIL OfficialName" on page 880*

Syntax

```
$MDSVERUTIL AllVersions
```

Mapping

Internal Version ID	Official version
VID_94	R80.40
VID_93	R80.30
VID_92	R80.20
VID_91	R80
VID_90	R77.X
VID_89	R76
VID_88	R75.40VS
VID_87	R75.40
VID_86	R75.30
VID_85	R75.20
VID_84	R75
VID_83	R71.X
VID_80	R70.X
VID_65	NGX R65
VID_62	NGX R62
VID_NGX_61	NGX R61
VID_60	NGX R60
VID_541_A	NG AI R55W
VID_541	NG AI R55
VID_54_VSX_R2	VSX NG AI R2
VID_54_VSX	VSX NG AI 2.2N and VSX NG AI 2.3N
VID_54	NG AI R54
VID_53_VSX	VSX NG AI

Internal Version ID	Official version
VID_53	NG FP3
VID_52	NG FP2
VID_51	NG FP1
VID_41	4.1

Example

```
[Expert@MDS:0]# $MDSVERUTIL AllVersions
VID_94
VID_93
VID_92
VID_91
VID_90
VID_89
VID_88
VID_87
VID_86
VID_85
VID_84
VID_83
VID_80
VID_65
VID_62
VID_NGX_61
VID_61
VID_60
VID_541_A
VID_541
VID_54_VSX_R2
VID_54_VSX
VID_54
VID_53_VSX
VID_53
VID_52
VID_51
VID_41
[Expert@MDS:0]#
```

$MDSVERUTIL CMAAddonDir

Description

Returns the path to the Management Addon directory in the context of the specified Domain Management Server. Applies only to NG AI R55W version.

In addition, see the *"$MDSVERUTIL MDSAddonDir" on page 859* command.

Syntax

```
$MDSVERUTIL CMAAddonDir -n <Name or IP address of Domain
Management Server> [-v <Version_ID>]
```

Parameters

Parameter	Description
`-n <Name or IP address of Domain Management Server>`	Specifies the Domain Management Server by its name or IPv4 address.
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL CMAAddonDir -n MyDomain_Server
/opt/CPmds-R81.20/customers/MyDomain_Server/CPmgmt-R55W
[Expert@MDS:0]#
```

$MDSVERUTIL CMACompDir

Description

Returns the full path for the specified Backward Compatibility Package in the context of the specified Domain Management Server.

In addition, see these commands:

- *"$MDSVERUTIL MDSCompDir" on page 860*
- *"$MDSVERUTIL MDSVarCompDir" on page 874*

Syntax

```
$MDSVERUTIL CMACompDir -n <Name or IP address of Domain Management Server> -c <Name of Backward Compatibility Package>
```

Parameters

Parameter	Description
`-n <Name or IP address of Domain Management Server>`	Specifies the Domain Management Server by its name or IPv4 address.
`-c <Name of Backward Compatibility Package>`	Specifies the name of Backward Compatibility Package. The Backward Compatibility Package contains the applicable files to install policy on Security Gateways that run a lower version than the Multi-Domain Server. To see the list of all Backward Compatibility Packages, run in Expert mode: `ls -1 $MDSDIR/customers/<Name of Domain Management Server>/ | grep CMP`

Example

```
[Expert@MDS:0]# $MDSVERUTIL CMACompDir -n MyDomain_Server -c CPR77CMP-R81.20
/opt/CPmds-R81.20/customers/MyDomain_Server/CPR77CMP-R81.20
[Expert@MDS:0]#
```

$MDSVERUTIL CMAFgDir

Description

Returns the full path for the `$FGDIR` directory in the context of the specified Domain Management Server.

In addition, see the *"$MDSVERUTIL MDSFgDir" on page 862* command.

Syntax

```
$MDSVERUTIL CMAFgDir -n <Name or IP address of Domain Management Server> [-v <Version_ID>]
```

Parameters

Parameter	Description
`-n <Name or IP address of Domain Management Server>`	Specifies the Domain Management Server by its name or IPv4 address.
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL CMAFgDir -n MyDomain_Server
/opt/CPmds-R81.20/customers/MyDomain_Server/CPsuite-R81.20/fg1
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL CMAFgDir -n MyDomain_Server -v VID_90
/opt/CPmds-R77/customers/MyDomain_Server/CPsuite-R77/fg1
[Expert@MDS:0]#
```

$MDSVERUTIL CMAFw40Dir

Description

Returns the full path for the `$FWDIR` directory for FireWall-1 4.0 in the context of the specified Domain Management Server.

Syntax

```
$MDSVERUTIL CMAFw40Dir -n <Name or IP address of Domain Management Server> [-v <Version_ID>]
```

Parameters

Parameter	Description
`-n <Name or IP address of Domain Management Server>`	Specifies the Domain Management Server by its name or IPv4 address.
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL CMAFw40Dir -n MyDomain_Server
/opt/CPmds-R81.20/customers/MyDomain_Server/fw40
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL CMAFw40Dir -n MyDomain_Server -v VID_90
/opt/CPmds-R77/customers/MyDomain_Server/fw40
[Expert@MDS:0]#
```

$MDSVERUTIL CMAFw41Dir

Note - R81.20 does not support UTM-1 Edge and Safe@Office devices. The information about this command is provided only to describe the existing syntax option until it is removed completely.

Description

Returns the full path for the `$FWDIR` directory for UTM-1 Edge devices (that are based on FireWall-1 4.1) in the context of the specified Domain Management Server.

Syntax

```
$MDSVERUTIL CMAFw41Dir -n <Name or IP address of Domain Management Server> [-v <Version_ID>]
```

Parameters

Parameter	Description
`-n <Name or IP address of Domain Management Server>`	Specifies the Domain Management Server by its name or IPv4 address.
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL CMAFw41Dir -n MyDomain_Server
/opt/CPmds-R81.20/customers/MyDomain_Server/CPEdgecmp-R81.20
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL CMAFw41Dir -n MyDomain_Server -v VID_90
/opt/CPmds-R77/customers/MyDomain_Server/CPEdgecmp-R77
[Expert@MDS:0]#
```

$MDSVERUTIL CMAFwConfDir

Description

Returns the full path for the `$FWDIR/conf/` directory in the context of the specified Domain Management Server.

Syntax

```
$MDSVERUTIL CMAFwConfDir -n <Name or IP address of Domain Management Server> [-v <Version_ID>]
```

Parameters

Parameter	Description
`-n <Name or IP address of Domain Management Server>`	Specifies the Domain Management Server by its name or IPv4 address.
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL CMAFwConfDir -n MyDomain_Server
/opt/CPmds-R81.20/customers/MyDomain_Server/CPsuite-R81.20/fw1/conf
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL CMAFwConfDir -n MyDomain_Server -v VID_90
/opt/CPmds-R77/customers/MyDomain_Server/CPsuite-R77/fw1/conf
[Expert@MDS:0]#
```

$MDSVERUTIL CMAFwDir

Description

Returns the full path for the `$FWDIR` directory in the context of the specified Domain Management Server.

In addition, see the *"$MDSVERUTIL MDSFwDir" on page 864* command.

Syntax

```
$MDSVERUTIL CMAFwDir -n <Name or IP address of Domain Management Server> [-v <Version_ID>]
```

Parameters

Parameter	Description
`-n <Name or IP address of Domain Management Server>`	Specifies the Domain Management Server by its name or IPv4 address.
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL CMAFwDir -n MyDomain_Server
/opt/CPmds-R81.20/customers/MyDomain_Server/CPsuite-R81.20/fw1
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL CMAFwDir -n MyDomain_Server -v VID_90
/opt/CPmds-R77/customers/MyDomain_Server/CPsuite-R77/fw1
[Expert@MDS:0]#
```

$MDSVERUTIL CMAIp

Description

Returns the IPv4 address of the Domain Management Server specified by its name.

In addition, see the *"$MDSVERUTIL MDSIp" on page 865* command.

Syntax

```
$MDSVERUTIL CMAIp -n <Name or IP address of Domain Management
Server> [-v <Version_ID>]
```

Parameters

Parameter	Description
`-n <Name or IP address of Domain Management Server>`	Specifies the Domain Management Server by its name or IPv4 address.
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL CMAIp -n MyDomain_Server
192.168.3.240
[Expert@MDS:0]#
```

$MDSVERUTIL CMAIp6

Description

Returns the IPv6 address of the Domain Management Server specified by its name.

In addition, see the *"$MDSVERUTIL MDSIp6" on page 866* command.

Note - Multi-Domain Server does not support IPv6 at all (Known Limitation PMTR-14989).

Syntax

```
$MDSVERUTIL CMAIp6 -n <Name or IP address of Domain Management
Server> [-v <Version_ID>]
```

Parameters

Parameter	Description
`-n <Name or IP address of Domain Management Server>`	Specifies the Domain Management Server by its name or IPv6 address.
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

$MDSVERUTIL CMALogExporterDir

Description

Returns the full path for the `$EXPORTERDIR` directory in the context of the specified Domain Management Server.

In addition, see the *"$MDSVERUTIL MDSLogExporterDir" on page 867* command.

Syntax

```
$MDSVERUTIL CMALogExporterDir -n <Name or IP address of Domain
Management Server> [-v <Version_ID>]
```

Parameters

Parameter	Description
`-n <Name or IP address of Domain Management Server>`	Specifies the Domain Management Server by its name or IPv4 address.
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL CMALogExporterDir -n MyDomain_Server
/opt/CPmds-R81.20/customers/MyDomain_Server/CPrt-R81.20/log_exporter
[Expert@MDS:0]#
```

$MDSVERUTIL CMALogIndexerDir

Description

Returns the full path for the `$INDEXERDIR` directory in the context of the specified Domain Management Server.

In addition, see the *"$MDSVERUTIL MDSLogIndexerDir" on page 868* command.

Syntax

```
$MDSVERUTIL CMALogIndexerDir -n <Name or IP address of Domain
Management Server> [-v <Version_ID>]
```

Parameters

Parameter	Description
`-n <Name or IP address of Domain Management Server>`	Specifies the Domain Management Server by its name or IPv4 address.
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL CMALogIndexerDir -n MyDomain_Server
/opt/CPmds-R81.20/customers/MyDomain_Server/CPrt-R81.20/log_indexer
[Expert@MDS:0]#
```

$MDSVERUTIL CMANameByFwDir

Description

Returns the name of the Domain Management Server based on the context of the current `$FWDIR` directory.

Syntax

```
$MDSVERUTIL CMANameByFwDir -d $FWDIR [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL CMANameByFwDir -d $FWDIR
MyDomain_Server
[Expert@MDS:0]#
```

$MDSVERUTIL CMANameByIp

Description

Returns the name of the Domain Management Server based on the specified IPv4 address.

Syntax

```
$MDSVERUTIL CMANameByIp -i <IP address of Domain Management
Server> [-v <Version_ID>]
```

Parameters

Parameter	Description
`-i <IP address of Domain Management Server>`	Specifies the Domain Management Server by its IPv4 address.
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL CMANameByIp -i 192.168.3.240
MyDomain_Server
[Expert@MDS:0]#
```

$MDSVERUTIL CMARegistryDir

Description

Returns the full path for the `$CPDIR/registry/` directory in the context of the specified Domain Management Server.

In addition, see the *"$MDSVERUTIL MDSRegistryDir" on page 870* command.

Syntax

```
$MDSVERUTIL CMARegistryDir -n <Name of Domain Management Server>
[-v <Version_ID>]
```

Parameters

Parameter	Description
`-n <Name of Domain Management Server>`	Specifies the Domain Management Server by its name.
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL CMARegistryDir -n MyDomain_Server
/opt/CPmds-R81.20/customers/MyDomain_Server/CPshrd-R81.20/registry
[Expert@MDS:0]#
```

$MDSVERUTIL CMAReporterDir

Description

Returns the full path for the `$RTDIR` directory in the context of the specified Domain Management Server.

In addition, see the *"$MDSVERUTIL MDSReporterDir" on page 871* command.

Syntax

```
$MDSVERUTIL CMAReporterDir -n <Name of Domain Management Server>
[-v <Version_ID>]
```

Parameters

Parameter	Description
`-n <Name of Domain Management Server>`	Specifies the Domain Management Server by its name.
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL CMAReporterDir -n MyDomain_Server
/opt/CPmds-R81.20/customers/MyDomain_Server/CPrt-R81.20
[Expert@MDS:0]#
```

$MDSVERUTIL CMASmartLogDir

Description

Returns the full path for the `$SMARTLOGDIR` directory in the context of the specified Domain Management Server.

In addition, see the *"$MDSVERUTIL MDSSmartLogDir" on page 872* command.

Syntax

```
$MDSVERUTIL CMASmartLogDir -n <Name of Domain Management Server>
[-v <Version_ID>]
```

Parameters

Parameter	Description
`-n <Name of Domain Management Server>`	Specifies the Domain Management Server by its name.
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL CMASmartLogDir -n MyDomain_Server
/opt/CPmds-R81.20/customers/MyDomain_Server/CPSmartLog-R81.20
[Expert@MDS:0]#
```

$MDSVERUTIL CMASvnConfDir

Description

Returns the full path for the `$CPDIR/conf/` directory in the context of the specified Domain Management Server.

Syntax

```
$MDSVERUTIL CMASvnConfDir -n <Name of Domain Management Server> [-v <Version_ID>]
```

Parameters

Parameter	Description
`-n <Name of Domain Management Server>`	Specifies the Domain Management Server by its name.
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL CMASvnConfDir -n MyDomain_Server
/opt/CPmds-R81.20/customers/MyDomain_Server/CPshrd-R81.20/conf
[Expert@MDS:0]#
```

$MDSVERUTIL CMASvnDir

Description

Returns the full path for the `$CPDIR` directory in the context of the specified Domain Management Server.

In addition, see these commands:

- *"$MDSVERUTIL MDSSvnDir" on page 873*
- *"$MDSVERUTIL MDSVarSvnDir" on page 878*

Syntax

```
$MDSVERUTIL CMASvnDir -n <Name of Domain Management Server> [-v <Version_ID>]
```

Parameters

Parameter	Description
`-n <Name of Domain Management Server>`	Specifies the Domain Management Server by its name.
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL CMASvnDir -n MyDomain_Server
/opt/CPmds-R81.20/customers/MyDomain_Server/CPshrd-R81.20
[Expert@MDS:0]#
```

$MDSVERUTIL ConfDirVersion

Description

Returns the internal Version ID based on the context of the current `$FWDIR/conf/` directory.

For information about the internal Version ID, see the *"$MDSVERUTIL AllVersions" on page 827* command.

Syntax

```
$MDSVERUTIL ConfDirVersion -d $FWDIR/conf
```

Example

```
[Expert@MDS:0]# $MDSVERUTIL ConfDirVersion -d $FWDIR/conf
VID_92
[Expert@MDS:0]#
```

$MDSVERUTIL CpdbUpParam

Description

Returns internal version numbers from the internal database.

In addition, see these commands:

- *"$MDSVERUTIL MSP" on page 879*
- *"$MDSVERUTIL SP" on page 886*

Syntax

```
$MDSVERUTIL CpdbUpParam [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL CpdbUpParam
6.0.5.1
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL CpdbUpParam -v VID_90
6.0.4.0
[Expert@MDS:0]#
```

Example 3

```
[Expert@MDS:0]# $MDSVERUTIL CpdbUpParam -v VID_65
6.0.1.0
[Expert@MDS:0]#
```

$MDSVERUTIL CPprofileDir

Description

Returns the path to the directory that contains the `.CPprofile.sh` and the `.CPprofile.csh` shell scripts.

Syntax

```
$MDSVERUTIL CPprofileDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL CPprofileDir
/opt/CPshrd-R81.20/tmp
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL CPprofileDir -v VID_90
/opt/CPshrd-R77/tmp
[Expert@MDS:0]#
```

$MDSVERUTIL CPVer

Description

Returns internal Check Point version number.

Syntax

```
$MDSVERUTIL CPVer [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL CPVer
9.0
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL CPVer -v VID_80
8.0
[Expert@MDS:0]#
```

$MDSVERUTIL CustomersBaseDir

Description

Returns the full path for the `$MDSDIR/customers/` directory.

Syntax

```
$MDSVERUTIL CustomersBaseDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL CustomersBaseDir
/opt/CPmds-R81.20/customers
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL CustomersBaseDir -v VID_90
/opt/CPmds-R77/customers
[Expert@MDS:0]#
```

$MDSVERUTIL DiskSpaceFactor

Description

Returns the disk-space factor. The `mds_setup` command uses this value during an upgrade.

Syntax

```
$MDSVERUTIL DiskSpaceFactor [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL DiskSpaceFactor
1
[Expert@MDS:0]#
```

$MDSVERUTIL InstallationLogDir

Description

Returns the full path for directory with all installation logs (`/opt/CPInstLog/`).

Syntax

```
$MDSVERUTIL InstallationLogDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL InstallationLogDir
/opt/CPInstLog
[Expert@MDS:0]#
```

$MDSVERUTIL IsIPv6Enabled

Description

Returns `true`, if IPv6 is enabled in Gaia OS.

Returns `false`, if IPv6 is disabled in Gaia OS.

Note - Multi-Domain Server does not support IPv6 at all (Known Limitation PMTR-14989).

Syntax

```
$MDSVERUTIL IsIPv6Enabled
```

$MDSVERUTIL IsLegalVersion

Description

Returns 0, if the specified internal Version ID is legal.

Returns 1, if the specified internal Version ID is illegal.

Syntax

```
$MDSVERUTIL IsLegalVersion -v <Version_ID>
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL IsLegalVersion -v VID_92
0
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL IsLegalVersion -v VID_123456
1
[Expert@MDS:0]#
```

$MDSVERUTIL IsOsSupportsIPv6

Description

Returns `true`, if the OS supports IPv6.

Returns `false`, if the OS does not support IPv6.

Note - Multi-Domain Server does not support IPv6 at all (Known Limitation PMTR-14989).

Syntax

```
$MDSVERUTIL IsOsSupportsIPv6
```

$MDSVERUTIL LatestVersion

Description

Returns the internal Version ID of the latest installed version.

Syntax

```
$MDSVERUTIL LatestVersion
```

See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL LatestVersion
VID_92
[Expert@MDS:0]#
```

$MDSVERUTIL MDSAddonDir

Description

Returns the path to the Management Addon directory in the MDS context.

In addition, see the *"$MDSVERUTIL CMAAddonDir" on page 830* command.

Syntax

```
$MDSVERUTIL MDSAddonDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL MDSAddonDir
/opt/CPmgmt-R55W
[Expert@MDS:0]#
```

$MDSVERUTIL MDSCompDir

Description

Returns the full path for the specified Backward Compatibility Package in the MDS context.

In addition, see these commands:

- *"$MDSVERUTIL CMACompDir" on page 831*
- *"$MDSVERUTIL MDSVarCompDir" on page 874*

Syntax

```
$MDSVERUTIL MDSCompDir -c <Name of Backward Compatibility Package>
```

Parameters

Parameter	Description
`-c <Name of Backward Compatibility Package>`	Specifies the name of Backward Compatibility Package. The Backward Compatibility Package contains the applicable files to install policy on Security Gateways that run a lower version than the Multi-Domain Server. To see the list of all Backward Compatibility Packages, run in Expert mode: `ls -1 /opt/ | grep CMP`

Example

```
[Expert@MDS:0]# $MDSVERUTIL MDSCompDir -c CPR77CMP-R81.20
/opt/CPR77CMP-R81.20
[Expert@MDS:0]#
```

$MDSVERUTIL MDSDir

Description

Returns the full path in the `/opt/` directory to the `$MDSDIR` directory.

In addition, see the *"$MDSVERUTIL MDSVarDir" on page 875* command.

Syntax

```
$MDSVERUTIL MDSDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSDir
/opt/CPmds-R81.20
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL MDSDir -v VID_90
/opt/CPmds-R77
[Expert@MDS:0]#
```

$MDSVERUTIL MDSFgDir

Description

Returns the full path for the `$FGDIR` directory in the MDS context.

In addition, see the *"$MDSVERUTIL CMAFgDir" on page 832* command.

Syntax

```
$MDSVERUTIL MDSFgDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSFgDir
/opt/CPsuite-R81.20/fg1
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL MDSFgDir -v VID_90
/opt/CPsuite-R77/fg1
[Expert@MDS:0]#
```

$MDSVERUTIL MDSFwbcDir

Note - R81.20 does not support UTM-1 Edge and Safe@Office devices. The information about this command is provided only to describe the existing syntax option until it is removed completely.

Description

Returns the full path in the `/opt/` directory (in the MDS context) for the Backward Compatibility directory for UTM-1 Edge devices.

This Backward Compatibility directory contains the applicable files to install policy on UTM-1 Edge devices.

In addition, see the *"$MDSVERUTIL MDSVarFwbcDir" on page 876* command.

Syntax

```
$MDSVERUTIL MDSFwbcDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSFwbcDir
/opt/CPEdgecmp-R81.20
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL MDSFwbcDir -v VID_90
/opt/CPEdgecmp-R77
[Expert@MDS:0]#
```

$MDSVERUTIL MDSFwDir

Description

Returns the full path in the `/opt/` directory for the `$FWDIR` directory in the MDS context.

In addition, see these commands:

- *"$MDSVERUTIL MDSVarFwDir" on page 877*
- *"$MDSVERUTIL CMAFwDir" on page 836*

Syntax

```
$MDSVERUTIL MDSFwDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSFwDir
/opt/CPsuite-R81.20/fw1
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL MDSFwDir -v VID_90
/opt/CPsuite-R77/fw1
[Expert@MDS:0]#
```

$MDSVERUTIL MDSIp

Description

Returns the IPv4 address of Multi-Domain Server.

In addition, see the *"$MDSVERUTIL CMAIp" on page 837* command.

Syntax

```
$MDSVERUTIL MDSIp [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL MDSIp
192.168.3.51
[Expert@MDS:0]#
```

$MDSVERUTIL MDSIp6

Description

Returns the IPv6 address of Multi-Domain Server.

In addition, see the *"$MDSVERUTIL CMAIp6" on page 838* command.

Note - Multi-Domain Server does not support IPv6 at all (Known Limitation PMTR-14989).

Syntax

```
$MDSVERUTIL MDSIp6 [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

$MDSVERUTIL MDSLogExporterDir

Description

Returns the full path for the `$EXPORTERDIR` directory in the MDS context.

In addition, see the *"$MDSVERUTIL CMALogExporterDir" on page 839* command.

Syntax

```
$MDSVERUTIL MDSLogExporterDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSLogExporterDir
/opt/CPrt-R81.20/log_exporter
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL MDSLogExporterDir -v VID_91
/opt/CPrt-R80/
[Expert@MDS:0]#
```

$MDSVERUTIL MDSLogIndexerDir

Description

Returns the full path for the `$INDEXERDIR` directory in the MDS context.

In addition, see the *"$MDSVERUTIL CMALogIndexerDir" on page 840* command.

Syntax

```
$MDSVERUTIL MDSLogIndexerDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSLogIndexerDir
/opt/CPrt-R81.20/log_indexer
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL MDSLogIndexerDir -v VID_91
/opt/CPrt-R80/
[Expert@MDS:0]#
```

$MDSVERUTIL MDSPkgName

Description

Returns the name of the MDS software package.

In addition, see the *"$MDSVERUTIL SVNPkgName" on page 887* command.

Syntax

```
$MDSVERUTIL MDSPkgName [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSPkgName
CPmds-R81.20-00
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL MDSPkgName -v VID_90
CPmds-R77-00
[Expert@MDS:0]#
```

$MDSVERUTIL MDSRegistryDir

Description

Returns the full path for the `$CPDIR/registry/` directory in the MDS context.

In addition, see the *"$MDSVERUTIL CMARegistryDir" on page 843* command.

Syntax

```
$MDSVERUTIL MDSRegistryDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSRegistryDir
/opt/CPshrd-R81.20/registry
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL MDSRegistryDir -v VID_90
/opt/CPshrd-R77/registry
[Expert@MDS:0]#
```

$MDSVERUTIL MDSReporterDir

Description

Returns the full path for the `$RTDIR` directory in the MDS context.

In addition, see the *"$MDSVERUTIL CMAReporterDir" on page 844* command.

Syntax

```
$MDSVERUTIL MDSReporterDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSReporterDir
/opt/CPrt-R81.20
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL MDSReporterDir -v VID_91
/opt/CPrt-R80
[Expert@MDS:0]#
```

$MDSVERUTIL MDSSmartLogDir

Description

Returns the full path for the `$SMARTLOGDIR` directory in the MDS context.

In addition, see the *"$MDSVERUTIL CMASmartLogDir" on page 845* command.

Syntax

```
$MDSVERUTIL MDSSmartLogDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSSmartLogDir
/opt/CPSmartLog-R81.20
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL MDSSmartLogDir -v VID_91
/opt/CPSmartLog-R80
[Expert@MDS:0]#
```

$MDSVERUTIL MDSSvnDir

Description

Returns the full path in the `/opt/` directory for the `$CPDIR` directory in the MDS context.

In addition, see these commands:

- *"$MDSVERUTIL CMASvnDir" on page 847*
- *"$MDSVERUTIL MDSVarSvnDir" on page 878*

Syntax

```
$MDSVERUTIL MDSSvnDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSSvnDir
/opt/CPshrd-R81.20
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL MDSSvnDir -v VID_91
/opt/CPshrd-R80
[Expert@MDS:0]#
```

$MDSVERUTIL MDSVarCompDir

Description

Returns the full path in the `/var/opt/` directory for the specified Backward Compatibility Package in the MDS context.

In addition, see these commands:

- *"$MDSVERUTIL CMACompDir" on page 831*
- *"$MDSVERUTIL MDSCompDir" on page 860*

Syntax

```
$MDSVERUTIL MDSVarCompDir -c <Name of Backward Compatibility Package>
```

Parameters

Parameter	Description
`-c <Name of Backward Compatibility Package>`	Specifies the name of Backward Compatibility Package. The Backward Compatibility Package contains the applicable files to install policy on Security Gateways that run a lower version than the Multi-Domain Server. To see the list of all Backward Compatibility Packages, run in Expert mode: `ls -1 /var/opt/ | grep CMP`

Example

```
[Expert@MDS:0]# $MDSVERUTIL MDSVarCompDir -c CPR77CMP-R81.20
/var/opt/CPR77CMP-R81.20
[Expert@MDS:0]#
```

$MDSVERUTIL MDSVarDir

Description

Returns the full path in the `/var/opt/` directory to the `$MDSDIR` directory.

In addition, see the *"$MDSVERUTIL MDSDir" on page 861* command.

Syntax

```
$MDSVERUTIL MDSVarDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSVarDir
/var/opt/CPmds-R81.20
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL MDSVarDir -v VID_90
/var/opt/CPmds-R77
[Expert@MDS:0]#
```

$MDSVERUTIL MDSVarFwbcDir

Note - R81.20 does not support UTM-1 Edge and Safe@Office devices. The information about this command is provided only to describe the existing syntax option until it is removed completely.

Description

Returns the full path in the `/var/opt/` directory (in the MDS context) for the Backward Compatibility directory for UTM-1 Edge devices.

This Backward Compatibility directory contains the applicable files to install policy on UTM-1 Edge devices.

In addition, see the *"$MDSVERUTIL MDSFwbcDir" on page 863* command.

Syntax

```
$MDSVERUTIL MDSVarFwbcDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSVarFwbcDir
/var/opt/CPEdgecmp-R81.20
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL MDSVarFwbcDir -v VID_90
/var/opt/CPEdgecmp-R77
[Expert@MDS:0]#
```

$MDSVERUTIL MDSVarFwDir

Description

Returns the full path in the `/var/opt/` directory for the `$FWDIR` directory in the MDS context.

In addition, see the *"$MDSVERUTIL MDSFwDir" on page 864* command.

Syntax

```
$MDSVERUTIL MDSVarFwDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSVarFwDir
/var/opt/CPsuite-R81.20/fw1
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL MDSVarFwDir -v VID_90
/var/opt/CPsuite-R77/fw1
[Expert@MDS:0]#
```

$MDSVERUTIL MDSVarSvnDir

Description

Returns the full path in the `/var/opt/` directory for the `$CPDIR` directory in the MDS context.

In addition, see these commands:

- *"$MDSVERUTIL CMASvnDir" on page 847*
- *"$MDSVERUTIL MDSSvnDir" on page 873*

Syntax

```
$MDSVERUTIL MDSVarSvnDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSVarSvnDir
/var/opt/CPshrd-R81.20
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL MDSVarSvnDir -v VID_90
/var/opt/CPshrd-R77
[Expert@MDS:0]#
```

$MDSVERUTIL MSP

Description

Returns the Minor Service Pack version.

In addition, see these commands:

- *"$MDSVERUTIL SP" on page 886*
- *"$MDSVERUTIL CpdbUpParam" on page 849*

Syntax

```
$MDSVERUTIL MSP [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MSP
9
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL MSP -v VID_91
8
[Expert@MDS:0]#
```

$MDSVERUTIL OfficialName

Description

Returns the official version name.

In addition, see the *"$MDSVERUTIL ShortOfficialName" on page 884* command.

Syntax

```
$MDSVERUTIL OfficialName [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL OfficialName
R80.20
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL OfficialName -v VID_91
R80
[Expert@MDS:0]#
```

Example 3

```
[Expert@MDS:0]# $MDSVERUTIL OfficialName -v VID_65
NGX R65
[Expert@MDS:0]#
```

$MDSVERUTIL OptionPack

Description

Returns the internal Option Pack version.

Syntax

```
$MDSVERUTIL OptionPack [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL OptionPack
3
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL OptionPack -v VID_90
1
[Expert@MDS:0]#
```

$MDSVERUTIL ProductName

Description

Returns the official name of the Multi-Domain Server product.

Syntax

```
$MDSVERUTIL ProductName [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL ProductName
Multi-Domain Security Management
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL ProductName -v VID_65
Provider-1
[Expert@MDS:0]#
```

$MDSVERUTIL RegistryCurrentVer

Description

Returns the current internal version of Check Point Registry.

Syntax

```
$MDSVERUTIL RegistryCurrentVer [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL RegistryCurrentVer
6.0
[Expert@MDS:0]#
```

$MDSVERUTIL ShortOfficialName

Description

Returns the short (without spaces) official version name.

In addition, see the *"$MDSVERUTIL OfficialName" on page 880* command.

Syntax

```
$MDSVERUTIL ShortOfficialName [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL ShortOfficialName
R80.20
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# ShortOfficialName -v VID_65
NGX_65
[Expert@MDS:0]#
```

$MDSVERUTIL SmartCenterPuvUpgradeParam

Description

Returns the version to the Pre-Upgrade Verifier (PUV) in order for it to upgrade to that version.

Syntax

```
$MDSVERUTIL SmartCenterPuvUpgradeParam [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL SmartCenterPuvUpgradeParam
R80.20
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL SmartCenterPuvUpgradeParam -v VID_90
R77
[Expert@MDS:0]#
```

Example 3

```
[Expert@MDS:0]# $MDSVERUTIL SmartCenterPuvUpgradeParam -v VID_65
NGX_R65
[Expert@MDS:0]#
```

$MDSVERUTIL SP

Description

Returns the Service Pack version.

In addition, see these commands:

- *"$MDSVERUTIL MSP" on page 879*
- *"$MDSVERUTIL CpdbUpParam" on page 849*

Syntax

```
$MDSVERUTIL SP [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL SP
4
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL SP -v VID_91
4
[Expert@MDS:0]#
```

$MDSVERUTIL SVNPkgName

Description

Returns the name of the Secure Virtual Network (SVN) package. Applies to versions NGX R60 and above.

In addition, see the *"$MDSVERUTIL MDSPkgName" on page 869* command.

Syntax

```
$MDSVERUTIL SVNPkgName [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL SVNPkgName
CPsuite-R81.20-00
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL SVNPkgName -v VID_90
CPsuite-R77-00
[Expert@MDS:0]#
```

$MDSVERUTIL SvrDirectory

Description

Returns the full path for the SmartReporter directory.

Syntax

```
$MDSVERUTIL SvrDirectory [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

$MDSVERUTIL SvrParam

Description

Returns the SmartReporter version.

Syntax

```
$MDSVERUTIL SvrParam [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 827* command.

Creating a Domain Management Server with the 'mgmt_cli' Command

Prerequisites

- Name or Identifier of the Domain. For example: `MyDomain`
- Name or Identifier of the new Domain Management Server. For example: `MyDMS`
- IPv4 address for the new Domain Management Server.
- IPv4 Address for the Multi-Domain Server.
- The Multi-Domain Server username and password for a Multi-Domain Superuser, who has permission to create the new Domain Management Server.

To create a new Domain Management Server

1. Connect to the command line on the Multi-Domain Server.
2. Log in to the Expert mode with the Superuser credentials.
3. Create the Domain Management Server.

   Run this command:

   ```
   mgmt_cli add domain name <domain_name> servers.ip address
   "<ipv4>" servers.name "<server_name>" servers.multi-domain-
   server "<mdm_name>"
   ```

   For more information, see *"mgmt_cli" on page 782*.

   Example:

   ```
   mgmt_cli add domain name "domain1" servers.ip-address
   "192.0.2.1" servers.name "domain1_ManagementServer_1"
   servers.multi-domain-server "primary_mdm"
   ```

4. Connect with SmartConsole to the new Domain Management Server to configure the applicable settings.

SmartProvisioning Commands

For more information about SmartProvisioning, see the *R81.20 SmartProvisioning Administration Guide*.

In addition, see *"Security Management Server Commands" on page 44*.

Managing Security through API

This section describes the API Server on a Management Server and the applicable API Tools.

API

You can configure and manage the Management Server through API Requests that you send to the API Server that runs on the Management Server.

The API Server can automate daily tasks and integrate Check Point solutions with third party systems, such as virtualization, ticketing, and change management systems.

To learn more about the management APIs, to see code samples, and to take advantage of user forums, see:

- The API Documentation:
  - Online - *Check Point Management API Reference* (at the top, select the correct version)
  - Local - `https://<Server IP Address>/api_docs/#introduction`

    By default, access to the local API Documentation is disabled. Follow the instructions in sk174606.

    Note - On a Standalone server (a server which runs both a Security Management Server and a Security Gateway), the API Documentation web portal (`https://<Server IP Address>/api_docs`) stops working when you open SmartView Web Application (`https://<Server IP Address>/smartview`).
- The **Developers Network** section of *Check Point CheckMates Community*.

API Tools

You can use these tools to work with the API Server on the Management Server:

- Standalone management tool, included with Gaia operating system:

  `mgmt_cli`
- Standalone management tool, included with SmartConsole:

  `mgmt_cli.exe`

  You can copy this tool from the SmartConsole installation folder to other computers that run Windows operating system.
- Web Services APIs that allow communication and data exchange between the clients and the Management Server over the HTTP protocol.

These APIs also let other Check Point processes communicate with the Management Server over the HTTPS protocol.

`https://<IP Address of Management Server>/web_api/<command>`

Configuring the API Server

To configure the API Server:

1. Connect with SmartConsole to the Security Management Server or applicable Domain Management Server.
2. From the left navigation panel, click **Manage & Settings**.
3. In the upper left section, click **Blades**.
4. In the **Management API** section, click **Advanced Settings**.

   The **Management API Settings** window opens.
5. Configure the **Startup Settings** and the **Access Settings**.

   Configuring Startup Settings

   Select **Automatic start** to automatically start the API server when you start or reboot the Management Server.

   Notes:
   - If the Management Server has more than 4GB of RAM installed, the **Automatic start** option is activated by default during Management Server installation.
   - If the Management Server has less than 4GB of RAM, the **Automatic Start** option is deactivated.

Configuring Access Settings

Select one of these options to configure which clients can connect to the API Server:

- **Management server only** - Only the Management Server itself can connect to the API Server. This option only lets you use the `mgmt_cli` utility on the Management Server to send API requests. You cannot use SmartConsole or Web services to send API requests.
- **All IP addresses that can be used for GUI clients** - You can send API requests from all IP addresses that are defined as **Trusted Clients** in SmartConsole. This includes requests from SmartConsole, Web services, and the `mgmt_cli` utility on the Management Server.
- **All IP addresses** - You can send API requests from all IP addresses. This includes requests from SmartConsole, Web services, and the `mgmt_cli` utility on the Management Server.

6. Click **OK**.
7. In the upper left section, click **Permissions & Administrators**.
8. In the object of each applicable Administrator, make sure the assigned Permission Profile allows access to Management API.

   Instructions

   a. Edit the Administrator object.
   b. In the left panel, click **General**.
   c. In the **Permissions** section, on the right side of the selected Permission Profile, click the eye icon.

      The Permission Profile object opens in the read-only view.
   d. In the left panel, click **Management**.
   e. The permission **Management API Login** has to be selected.

      If it is not selected, then close this window and edit this Permission Profile object.
   f. Click **Close**.

9. Publish the SmartConsole session.
10. Restart the API Server on the Management Server with this command:

```
api restart
```

Notes:

- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

- The output of this command must show:

```
API started successfully
```

11. Examine the status of the API server on the Management Server with this command:

```
api status
```

Notes:

- The output of this command must show:

```
------------------------------------------
Overall API Status: Started
------------------------------------------

API readiness test SUCCESSFUL. The server is up and ready
to receive connections
```

- The output of this command may show the state of the "**API**" process as "**Stopped**" when the API access is set to "**All IP addresses that can be used for GUI clients**", and more than 200 Trusted Clients are configured:

```
Processes:

Name       State     PID       More Information
-----------------------------------------------
API        Stopped   ...
```

Discarding API Sessions with Locks or Pending Changes

Open SmartConsole and API sessions that contain locks or unpublished changes are not automatically discarded. As a result, some sessions can remain open for extended periods.

The `ENABLE_DISCARD_WORKSESSIONS_OLDER_THAN_DAYS` environment variable controls whether stale open sessions are automatically discarded. By default, this variable is disabled, and open sessions with locks or unpublished changes remain available until they are manually discarded.

When enabled, the Security Management Server periodically evaluates open sessions and discards sessions that exceed the configured age threshold.

To configure automatic discard of stale sessions:

1. Connect to the Security Management Server or Multi-Domain Server using SSH.
2. Switch to Expert mode.
3. To enable automatic discard of open sessions that contain locks or unpublished changes, set `ENABLE_DISCARD_WORKSESSIONS_OLDER_THAN_DAYS` to "`true`".

   Run:

   ```
   MDS_FWDIR/scripts/reload_env_vars.sh -e "ENABLE_DISCARD_
   WORKSESSIONS_OLDER_THAN_DAYS=true"
   ```

   ```
   $MDS_FWDIR/scripts/override_server_setting.sh -e ENABLE_DISCARD_
   WORKSESSIONS_OLDER_THAN_DAYS true
   ```
4. By default, only sessions which are open for more than 60 days are automatically discarded. To configure the number of days after which sessions are discarded, run:

   ```
   $MDS_FWDIR/scripts/reload_env_vars.sh -e "DISCARD_WORKSESSIONS_
   OLDER_THAN_DAYS=<Number_of_Days>" $MDS_FWDIR/scripts/override_
   server_setting.sh -e DISCARD_WORKSESSIONS_OLDER_THAN_DAYS
   <Number_of_Days>
   ```

   For example, to set the threshold to 30 days, run:

   ```
   $MDS_FWDIR/scripts/reload_env_vars.sh -e "DISCARD_WORKSESSIONS_
   OLDER_THAN_DAYS=30"
   $MDS_FWDIR/scripts/override_server_setting.sh -e DISCARD_
   WORKSESSIONS_OLDER_THAN_DAYS 30
   ```

Result:

When `ENABLE_DISCARD_WORKSESSIONS_OLDER_THAN_DAYS` is set to "`true`":

- The Security Management Server checks all open SmartConsole and API sessions one time per day.
- If a session remains open longer than the number of days configured in `DISCARD_WORKSESSIONS_OLDER_THAN_DAYS`, the session is automatically discarded.

Check Point LSMcli Overview

Description

Check Point SmartLSM Command Line Utility (LSMcli) is a simple command line utility, an alternative to SmartProvisioning SmartConsole GUI.

LSMcli performs SmartProvisioning GUI operations from a command line or through a script.

Notes:

- LSMcli can run from hosts other than SmartConsole clients. Make sure to define the hosts, from which you run the LSMcli as GUI clients.
- The first time you run the LSMcli from a client, it shows the Management Server's fingerprint. Confirm the fingerprint.
- In the LSMcli, commands can use the abbreviation *ROBO* (Remote Office/Branch Office) gateways.
  In SmartProvisioning GUI, these gateways are called SmartLSM Security Gateways.

Syntax

```
LSMcli {-h | --help}
```

```
LSMcli [-d] <Mgmt Server> <Username> <Password> <Action>
```

Parameters

Parameter	Description
`[-d]`	Runs the command in the debug mode.
<Mgmt Server>	Specifies the Security Management Server or Domain Management Server by its Name or IPv4 address.
<Username>	Specifies the username used in the standard Check Point authentication method.
<Password>	Specifies the password used in the standard Check Point authentication method.
<Action>	Specifies the function performed (see the next sub-sections for a complete list of actions).

Syntax Notation

Square brackets (**[ ]**) are used in the LSMcli utility syntax. These brackets are correct and syntactically necessary.

This is an example of how they are used:

- **A [b [c]]** - means that for parameter **A**, you can provide **b**. If you provide **b**, you can provide **c**.
- **A [b] [c]** - means that for parameter **A**, you can provide **b**, **c**, or **b** and **c**.
- **A [b c]** - means that for parameter **A**, you can provide **b** and **c**.

SmartLSM Security Gateway Management Actions

This section describes commands that perform management actions on SmartLSM Gateways.

LSMcli AddROBO VPN1

Description

This command adds a new Check Point SmartLSM Security Gateway to SmartProvisioning and assigns it a SmartLSM Security Profile.

If a one-time password is supplied, a SIC certificate is created.

If an IP address is also supplied, the SIC certificate is pushed to the SmartLSM Security Gateway (in such cases, the SmartLSM Security Gateway SIC one-time password must be initialized first).

If no IP address is supplied, the SIC certificate is pulled from the SmartLSM Security Gateway afterwards.

You can also assign an IP address range to Dynamic Objects, and specify whether or not to add them to the VPN domain.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> AddROBO VPN1
<ROBOName> <Profile> [-RoboCluster=<OtherROBOName>] [-
O=<ActivationKey> [-I=<IP>]] [[-CA=<CaName> [-
R=<CertificateIdentifier#>] [-KEY=<AuthorizationKey>]]] [-
D]:<DynamicObjectName>=<IP1>[-<IP2] [-D]:...
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of a SmartLSM Security Gateway.
<Profile>	Name of a SmartLSM Security Profile that was defined in SmartConsole.

Parameter	Description
<OtherROBOName>	Name for an already defined SmartLSM Security Gateway that participates in the SmartLSM Cluster with the newly created Security Gateway (if the "-RoboCluster" argument is provided).
<ActivationKey>	SIC one-time password (for this action, a certificate is generated).
<IP>	IP address of the Security Gateway (for this action, a certificate is pushed to the Security Gateway).
<CaName>	Name of the Trusted CA object (created from SmartConsole). The IKE certificate request is sent to this CA. Default is Check Point Internal CA.
<CertificateIdentifier#>	Key identifier for third-party CA.
<AuthorizationKey>	Authorization Key for third-party CA.
<DynamicObjectName>	Name of the Dynamic Object.
<IP1>	Single IP address for the Dynamic Object.
<IP1-IP2>	Range of IP addresses for the Dynamic Object.

Example 1

This command adds a new SmartLSM Security Gateway `MyRobo` and assigns it the specified SmartLSM Security Profile `AnyProfile`.

A SIC password and an IP address are supplied, so the SIC Activation Key can be sent to the new SmartLSM Security Gateway.

A Dynamic Object called `FirstDO` is resolved to an IP address for this Security Gateway.

```
LSMcli mySrvr name pass AddROBO VPN1 MyRobo AnyProfile -O=MyPass -
I=192.0.2.4 -DE:FirstDO=192.0.2.100
```

Example 2

```
LSMcli mySrvr name pass AddROBO VPN1 MyRobo AnyProfile -O=MyPass -
I=10.10.10.1 -DE:FirstDO=10.10.10.5 -CA=OPSEC_CA -R=cert123 -
KEY=abc456
```

LSMcli ModifyROBO VPN1

Description

This command modifies a Check Point SmartLSM Security Gateway.

This action modifies the SmartProvisioning details for an existing SmartLSM Security Gateway and can be used to update properties previously supplied by the user.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ModifyROBO VPN1
<RoboName> ...
```

and at least one of these:

```
... [-P=Profile] [-RoboCluster={<OtherROBOName> | -NoRoboCluster}]
[-D:<DO Name>=<IP1>[-<IP2>] [-KeepDOs]...]
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<Profile>	Name of a SmartLSM Security Profile that was defined in SmartConsole.
<OtherROBOName>	Name of the already defined SmartLSM Security Gateway that is to participate in the Cluster with the newly created Security Gateway (if the "`-RoboCluster`" argument is provided).
`-NoRoboCluster`	This parameter is equivalent to the **Remove Cluster** operation in the SmartProvisioning GUI. When you issue a `ModifyROBO VPN1` command with this argument on a Security Gateway that participates in a cluster, the cluster is removed.
<DO Name>	Name of the Dynamic Object.

Parameter	Description
<IP1>	Single IP address for the Dynamic Object.
<IP1-IP2>	Range of IP addresses for the Dynamic Object.
-KeepDOs	Keeps all existing dynamic objects in the dynamic objects list when you add new dynamic objects. If a dynamic object already exists in the list, its IP resolution is updated. If this flag is not specified, the dynamic objects list is deleted when you use the `LSMcli` command to add new dynamic objects.

Example

This example resolves Dynamic Objects for the given Security Gateway.

```
LSMcli mySrvr name pass ModifyROBO VPN1 MyRobo -
D:MyEmailServer=123.45.67.8 -D:MySpecialNet=10.10.10.1-10.10.10.6
```

LSMcli ModifyROBOManualVPNDomain

Description

This command modifies the SmartLSM VPN Domain, to take effect when the VPN Domain becomes defined as Manual.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password>
ModifyROBOManualVPNDomain <RoboName> {-Add=<FirstIP>-<LastIP> | -
Delete=<Index>} [-IfOverlappingIPRangesDetected={exit | ignore |
warn}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway or SmartLSM Cluster.
<FirstIP>-<LastIP>	IP address range.
<Index>	Value displayed by the *"LSMcli ShowInfo" on page 928* command or the *"LSMcli ShowROBOTopology" on page 917* command.
-IfOverlappingIPRangesDetected	Optional. Determines the course of action, if overlapping IP address ranges are detected: exit, ignore, or show a warning.

Example 1

```
LSMcli mySrvr name pass ModifyROBOManualVPNDomain MyRobo -
Add=192.0.2.1-192.0.2.20
```

Example 2

```
LSMcli mySrvr name pass ModifyROBOManualVPNDomain MyRobo -Delete=1
```

LSMcli ModifyROBOTopology VPN1

Description

This command modifies the SmartLSM VPN Domain configuration for a selected Security Gateway.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ModifyROBOTopology
VPN1 <RoboName> -VPNDomain={not_defined | external_ip_only |
topology | manual}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
`VPNDomain`	Specifies the VPN Domain topology: ■ `not_defined` - Equivalent to the **Not Defined** option on the **Topology** tab of a SmartLSM Security Gateway in the SmartProvisioning GUI (or in the output of the *"LSMcli ShowROBOTopology" on page 917* command). ■ `external_ip_only` - Equivalent to the **Only the external interface** configuration in the SmartProvisioning GUI. ■ `topology` - Equivalent to the **All IP Addresses behind the Gateway based on Topology information** configuration in the SmartProvisioning GUI. ■ `manual` - Equivalent to **Manually defined**. VPN domain is defined according to the configuration made with the *"LSMcli ModifyROBOManualVPNDomain" on page 904* command.

Example

```
LSMcli mySrvr name pass ModifyROBOTopology VPN1 MyRobo -
VPNDomain=manual
```

LSMcli ModifyROBOInterface VPN1

Description

This command modifies the Internal Interface list.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password>
ModifyROBOInterface VPN1 <RoboName> <InterfaceName> -i=<IPAddress>
[-Netmask=<NetMask>] [-IfOverlappingIPRangesDetected={exit |
ignore | warn}]
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<InterfaceName>	Name of the existing interface.
<IPAddress>	IP address of the interface.
<NetMask>	Net mask of the interface.
-IfOverlappingIPRangesDetected	Optional. Determines the course of action, if overlapping IP address ranges are detected: exit, ignore, or show a warning.

Example

```
LSMcli mySrvr name pass ModifyROBOInterface VPN1 MyRobo eth0 -
i=192.0.2.1 -Netmask=255.255.255.0
```

LSMcli AddROBOInterface VPN1

Description

This command adds a new interface to the selected SmartLSM Security Gateway.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> AddROBOInterface
VPN1 <RoboName> <InterfaceName> -i=<IPAddress> -NetMask=<NetMask>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<InterfaceName>	Name of an existing interface.
<IPAddress>	IP address of the interface.
<NetMask>	Net mask of the interface.

Example

```
LSMcli mySrvr name pass AddROBOInterface VPN1 MyRobo eth0 -
i=192.0.2.1 -Netmask=255.255.255.0
```

LSMcli DeleteROBOInterface VPN1

Description

This command deletes an interface from the selected Security Gateway.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password>
DeleteROBOInterface VPN1 <RoboName> <InterfaceName>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<InterfaceName>	Name of an existing interface.

Example

```
LSMcli mySrvr name pass DeleteROBOInterface VPN1 MyRobo eth0
```

LSMcli ExportIke

Description

This command exports the IKE Certificate into a P12 file(encrypted with a provided password) from SmartLSM Security Gateway, SmartLSM Cluster, or SmartLSM Cluster Member.

The default location of the exported file is the `$FWDIR/conf/` directory.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ExportIke
<RoboName> <Password> <FileName>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway, SmartLSM Cluster, or SmartLSM Cluster Member, whose certificate is exported.
<Password>	Password used to protect the p12 file.
<FileName>	Destination file name (is created).

Example

```
LSMcli mySrvr name pass ExportIke MyROBO ajg42k93N MyROBOCert.p12
```

LSMcli ResetIke

Description

This command resets the IKE Certificate of a SmartLSM Security Gateway, SmartLSM Cluster, or SmartLSM Cluster Member.

This action revokes the existing IKE certificate and creates a new one.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ResetIke
<RoboName> [-CA=<CaName> [-R=<CertificateIdentifier#>] [-
KEY=<AuthorizationKey>]]
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the Security Gateway, SmartLSM Cluster, or SmartLSM Cluster Member.
<CaName>	Name of the Trusted CA object (created from SmartConsole) the IKE certificate request is sent to this CA.
<CertificateIdentifier>	Key identifier of the specific certificate.
<AuthorizationKey>	Authorization Key to be sent to the CA for the certificate retrieval.

Example

```
LSMcli mySrvr name pass ResetIke MyROBO -CA=OPSEC_CA -R=cer3452s -
KEY=ad23fgh
```

LSMcli Remove

Description

This command deletes a SmartLSM Security Gateway.

This action revokes all the certificates used by the SmartLSM Security Gateway, releases all the licenses and, finally, removes the SmartLSM Security Gateway.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> Remove <RoboName>
<ID>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the Security Gateway.
<ID>	ID of the SmartLSM Security Gateway. Use the *"LSMcli Show" on page 915* command to check the ID of the specific SmartLSM Security Gateway.

Example

```
LSMcli mySrvr name pass Remove MyRobo 0.0.0.251
```

LSMcli ResetSic

Description

This command resets the SIC Certificate of a SmartLSM Security Gateway or SmartLSM Cluster Member.

This action revokes the Security Gateway's SIC certificate and creates a new one with the one-time password provided by the user.

If an IP address is supplied for the SmartLSM Security Gateway, the SIC certificate is pushed to the SmartLSM Security Gateway, in which case the SmartLSM Security Gateway SIC one-time password must be initialized first.

Otherwise, if no IP address is given, the SIC certificate is later pulled from the SmartLSM Security Gateway.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ResetSic
<RoboName> <ActivationKey> [-I=<IPAddress>]
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway or SmartLSM Cluster Member.
<ActivationKey>	One-time password for the Secure Internal Communications with the SmartLSM Security Gateway.
<IPAddress>	IP address of Security Gateway (for this action, the certificate is pushed to the Security Gateway).

Example 1

```
LSMcli mySrvr name pass ResetSic MyROBO aw47q1
```

Example 2

```
LSMcli mySrvr name pass ResetSic MyFixedIPROBO sp36rt1 -
I=10.20.30.1
```

LSMcli Show

Description

This command displays a list of existing Security Gateways.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> Show [-N=<Gateway Name>] [-F=<FilterFlags>]
```

Parameters

Parameter	Description
`<Mgmt Server>`	Name or IP address of the Security Management Server or Domain Management Server.
`<Username>`	User name of standard Check Point authentication method.
`<Password>`	Password of standard Check Point authentication method.
`<Gateway Name>`	Name of the Security Gateway to display. If the "`-N`" flag is not included, the command prints the existing **Devices** work space, including SmartLSM Security Gateways.
`-F=<` *`FilterFlags`*`>`	You can use these flags to filter the printed information: ■ `b` - ID ■ `c` - Cluster ID ■ `d` - List of Dynamic Objects assigned to this SmartLSM Security Gateways ■ `g` - Gateway status ■ `i` - IP address ■ `k` - IKE DN ■ `l` - Policy status ■ `n` - Name ■ `p` - SmartLSM Security Profile ■ `s` - SIC DN ■ `t` - Type ■ `v` - Version **Note** - To specify more than one filter flag, write them together. Example: `-F=bn`

Example 1

```
LSMcli mySrvr name pass Show -N=MyRobo
```

Example 2

```
LSMcli mySrvr name pass Show -F=binpt
```

LSMcli ShowROBOTopology

Description

This command displays the Topology information of the SmartLSM Security Gateway.

It lists the defined Interfaces and their respective IP Addresses and Network Masks, and the VPN Domain configuration.

You can use the indexes of the manually defined VPN domain IP address ranges, on the displayed list, when you request to delete a range, with the *"LSMcli ModifyROBOManualVPNDomain" on page 904* command.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ShowROBOTopology
<RoboName>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of Security Gateway.

Example

```
LSMcli mySrvr name pass ShowROBOTopology MyRobo
```

LSMcli UpdateCO

Description

This command updates a Corporate Office (CO) Security Gateway.

This action updates the CO Security Gateway with up-to-date available information about the VPN Domains of the SmartLSM Security Gateways.

Perform this action after you add a new SmartLSM Security Gateway to enable the CO gateway to initiate a VPN tunnel to the new SmartLSM Security Gateway.

Alternatively, you can Install Policy on the CO gateway to obtain updated VPN Domain information.

Note - This command supports CO Security Gateways only.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> UpdateCO {<COgw>
| COgwCluster}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<CoGw>	Name of a CO gateway.
<CoGwCluster>	Name of a cluster of CO gateways.

Example

```
LSMcli mySrvr name pass UpdateCO MyCO
```

SmartUpdate Actions

This section describes commands that perform SmartUpdateactions on SmartLSM Gateways.

Before you can install software on gateways, you must first load it to the Security Management Server.

Best Practice - Run the *"LSMcli VerifyInstall" on page 924* command to make sure that the software is compatible.

Use the *"LSMcli Install" on page 920* command to install the software.

Use the *"LSMcli Uninstall" on page 922* command to uninstall the software.

LSMcli Install

Description

This command installs the specified software on the SmartLSM Security Gateway or SmartLSM Cluster Member.

Note - Before you can install software on SmartLSM Security Gateways, you must first load it to the Security Management Server.

Best Practice - Run the *"LSMcli VerifyInstall" on page 924* command to make sure that the software is compatible.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> Install <RoboName>
<Product> <Vendor> <Version> <SP> [-P=<Profile>] [-boot] [-
DoNotDistribute]
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<Product>	Name of the package.
<Vendor>	Name of the vendor of the package.
<Version>	Major Version of the package.
<SP>	Minor Version of the package.
<Profile>	Assign a different SmartLSM Security Profile (already defined in SmartConsole) after installation.
boot	Reboot the SmartLSM Security Gateway after installation.
-DoNotDistribute	Optional. Install previously distributed packages.

Example

```
LSMcli mySrvr name pass Install MyRobo firewall checkpoint NG_AI
fcs -P=AnyProfile -boot
```

LSMcli Uninstall

Description

This command uninstalls the specified package from the SmartLSM Security Gateway or SmartLSM Cluster Member.

You can use the *"LSMcli ShowInfo" on page 928* command to see what products are installed on the SmartLSM Security Gateway.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> Uninstall
<RoboName> <Product> <Vendor> <Version> <SP> [-P=<Profile>] [-
boot]
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<Product>	Name of the package.
<Vendor>	Name of the vendor of the package.
<Version>	Major Version of the package.
<SP>	Minor Version of the package.
<Profile>	Assign a different SmartLSM Security Profile (already defined in SmartConsole) after uninstall.
`boot`	Reboot the SmartLSM Security Gateway after installation.

Example

```
LSMcli mySrvr name pass Uninstall MyRobo firewall checkpoint NG_AI
fcs -boot
```

LSMcli Distribute

Description

This command distributes a package from the Repository to the SmartLSM Security Gateway or SmartLSM Cluster Member, but does not install it.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> Distribute
<RoboName> <Product> <Vendor> <Version> <SP>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<Product>	Name of the package.
<Vendor>	Name of the vendor of the package.
<Version>	Major version of the package.
<SP>	Minor version of the package.

Example

```
LSMcli mySrvr name pass Distribute MyRobo fw1 checkpoint NG_AI R54
```

LSMcli VerifyInstall

Description

This command makes sure that the software is compatible to install on the SmartLSM Security Gateway or SmartLSM Cluster Member.

Note - Note that this action does not perform an installation.

Best Practice - Run this command before you install the software on the SmartLSM Security Gateway.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> VerifyInstall
<RoboName> <Product> <Vendor> <Version> <SP>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<Product>	Name of the package.
<Vendor>	Name of the vendor of the package.
<Version>	Major version of the package.
<SP>	Minor version of the package.

Example

```
LSMcli mySrvr name pass VerifyInstall MyRobo firewall checkpoint
NG_AI fcs
```

LSMcli VerifyUpgrade

Description

This command verifies if you can upgrade a selected software on the SmartLSM Security Gateway or SmartLSM Cluster Member.

Note - This command does not perform an installation.

Best Practice - Run this command before you run the *"LSMcli Upgrade" on page 926* command.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> VerifyUpgrade
<RoboName>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.

Example

```
LSMcli mySrvr name pass VerifyUpgrade MyRobo
```

LSMcli Upgrade

Description

This command upgrades all the (appropriate) available software packages on the SmartLSM Security Gateway or SmartLSM Cluster Member.

Best Practice - Run the *"LSMcli VerifyUpgrade" on page 925* command before you run this command.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> Upgrade <RoboName>
[-P=<Profile>] [-boot]
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<Profile>	Assign a different SmartLSM Security Profile (already defined in SmartConsole) after installation.
`boot`	Reboot the SmartLSM Security Gateway after the installation is finished.

Example

```
LSMcli mySrvr name pass Upgrade MyRobo -P=myprofile -boot
```

LSMcli GetInfo

Description

This command collects product information from the SmartLSM Security Gateway or SmartLSM Cluster Member.

Important - If you upgrade any package manually instead of using SmartUpdate, you must run this command before you run the *"LSMcli ShowInfo" on page 928* command.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> GetInfo <RoboName>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.

Example

```
LSMcli mySrvr name pass GetInfo MyRobo
```

LSMcli ShowInfo

Description

This command displays product information for the list of the products installed on the SmartLSM Security Gateway or SmartLSM Cluster Member.

Important - Before you run this command, run the *"LSMcli GetInfo" on page 927* command to make sure the information is up-to-date.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ShowInfo
<RoboName>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the Security Gateway.

Example

```
LSMcli mySrvr name pass ShowInfo MyRobo
```

LSMcli ShowRepository

Description

This command shows the list of the available products on the Management Server.

Use SmartUpdate to manage the products, load new products, remove products, and so on.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ShowRepository
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.

Example

```
LSMcli mySrvr name pass ShowRepository
```

LSMcli Stop

Description

This command stops Security Gateway services on the selected gateway.

Notes:

- The `CPRID` services must run on the selected gateway. See *"cprid" on page 186*.
- This command supports Security Gateways, SmartLSM Security Gateways, and SmartLSM Cluster Members.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> Stop {<RoboName>
| <GatewayName>}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<GatewayName>	Name of the standard Security Gateway.

Example

```
LSMcli mySrvr name pass Stop MyRobo
```

LSMcli Start

Description

This command starts Security Gateway services on the selected gateway.

Notes:

- The `CPRID` services must run on the selected gateway. See *"cprid" on page 186*.
- This command supports Security Gateways, SmartLSM Security Gateways, and SmartLSM Cluster Members.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> Start {<RoboName>
| <GatewayName>}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<GatewayName>	Name of the standard Security Gateway.

Example

```
LSMcli mySrvr name pass Start MyRobo
```

LSMcli Restart

Description

This command restarts Security Gateway services on the selected gateway.

Notes:

- The `CPRID` services must run on the selected gateway. See *"cprid" on page 186*.
- This command supports Security Gateways, SmartLSM Security Gateways, and SmartLSM Cluster Members.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> Restart
{<RoboName> | <GatewayName>}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<GatewayName>	Name of the standard Security Gateway.

Example

```
LSMcli mySrvr name pass Restart MyRobo
```

LSMcli Reboot

Description

This command reboots the selected gateway.

Notes:

- The `CPRID` services must run on the selected gateway. See *"cprid" on page 186*.
- This command supports Security Gateways, SmartLSM Security Gateways, and SmartLSM Cluster Members.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> Reboot {<RoboName>
| <GatewayName>}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway.
<GatewayName>	Name of the standard Security Gateway.

Example

```
LSMcli mySrvr name pass Reboot MyRobo
```

LSMcli Push Actions

These commands are used to push updated values, settings, and security rules to gateways.

After you create a gateway or a dynamic object in the SmartProvisioning system, you must assign (push) a security policy to it.

LSMcli PushPolicy

Description

This command pushes a policy to the selected gateway.

Notes:

- The `CPRID` services must run on the selected gateway. See *"cprid" on page 186*.
- This command supports Security Gateways, SmartLSM Security Gateways, and SmartLSM Clusters.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> PushPolicy
{<RoboName> | <GatewayName>}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway, or SmartLSM Cluster.
<GatewayName>	Name of the standard Security Gateway.

Example

```
LSMcli mySrvr name pass PushPolicy MyRobo
```

LSMcli PushDOs

Description

This command updates a Dynamic Object's information on the SmartLSM Security Gateway or SmartLSM Cluster Member.

Note - This command does not remove/release the IP address range for the deleted Dynamic Object, but only adds new ones. To overcome this difficulty, run the *"LSMcli PushPolicy" on page 935* command.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> PushDOs <RoboName>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway or SmartLSM Cluster Member.

Example

```
LSMcli mySrvr name pass PushDOs MyRobo
```

LSMcli GetStatus

Description

This command fetches various statistics from the selected gateway.

Note - This command supports Security Gateways, SmartLSM Security Gateways, and Gateway or SmartLSM Cluster Members.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> GetStatus
{<RoboName> | <GatewayName>}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboName>	Name of the SmartLSM Security Gateway or SmartLSM Cluster Member.
<GatewayName>	Name of the standard Security Gateway.

Example

```
LSMcli mySrvr name pass GetStatus MyRobo
```

Managing SmartLSM Clusters with LSMcli

With the `LSMcli` command, you can define SmartLSM clusters, and configure most of the options available in SmartProvisioning GUI (in the **New SmartLSM Cluster** wizard and in the **Edit** windows).

This section lists unique commands for SmartLSM Clusters.

Other commands that also apply to SmartLSM Clusters:

- *"LSMcli Distribute" on page 923*
- *"LSMcli GetInfo" on page 927*
- *"LSMcli GetStatus" on page 937*
- *"LSMcli Install" on page 920*
- *"LSMcli ModifyROBOManualVPNDomain" on page 904*
- *"LSMcli PushDOs" on page 936*
- *"LSMcli PushPolicy" on page 935*
- *"LSMcli Reboot" on page 933*
- *"LSMcli Reboot" on page 933*
- *"LSMcli ResetIke" on page 911*
- *"LSMcli ResetSic" on page 913*
- *"LSMcli Restart" on page 932*
- *"LSMcli ShowInfo" on page 928*
- *"LSMcli Start" on page 931*
- *"LSMcli Stop" on page 930*
- *"LSMcli Uninstall" on page 922*
- *"LSMcli Upgrade" on page 926*
- *"LSMcli VerifyInstall" on page 924*
- *"LSMcli VerifyUpgrade" on page 925*

Note - There is no convert action for or to SmartLSM clusters.

LSMcli AddROBO VPN1Cluster

Description

This command defines a new SmartLSM cluster.

You can configure all of the options available in the **New SmartLSM Cluster** wizard of the SmartProvisioning GUI.

The only exception is the configuration of Topology overrides (see *"LSMcli ModifyROBONetaccess VPN1Cluster" on page 943*).

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> AddROBO
VPN1Cluster <Profile> <MainIPAddress> <SuffixName> [-
S=<SubstitutedNamePart>] [-CA=<CaName> [-R=<KeyIdentifier#>] [-
KEY=<AuthorizationCode>]]
```

Parameters

Parameter	Description	SmartLSM GUI Location
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.	
<Username>	User name of standard Check Point authentication method.	
<Password>	Password of standard Check Point authentication method.	
<Profile>	Name of cluster Profile to which to map the new cluster.	**New SmartLSM Cluster** wizard.
<MainIPAddress>	Main IP address of cluster.	**New SmartLSM Cluster** wizard.
<SuffixName>	A suffix to be added to cluster and member Profile names.	**New SmartLSM Cluster** wizard.
<SubstitutedName Part>	A part of the Profile name to be replaced by the suffix in the previous field.	SmartProvisioning GUI supports adding Prefix and/or Suffix, not substitution.

Parameter	Description	SmartLSM GUI Location
<CaName>	The name of the Trusted CA object, defined in SmartConsole, to which a VPN certificate request is sent.	Double-click the SmartLSM cluster object > **Edit** window > **VPN** tab
<KeyIdentifier#>	Number to identify the specific certificate, once generated.	Double-click the SmartLSM cluster object > **Edit** window > **VPN** tab
<AuthorizationCode>	Authorization Key to be sent to CA to enable certificate retrieval.	Double-click the SmartLSM cluster object > **Edit** window > **VPN** tab

LSMcli ModifyROBO VPN1Cluster

Description

You can change a SmartLSM cluster main IP address.

You can resolve a dynamic object for a SmartLSM cluster.

Syntax for changing the Main IP Address

You can change a SmartLSM cluster main IP address in the SmartProvisioning GUI (double-click the SmartLSM cluster object > **Edit** window > **Cluster** tab), or with this command:

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ModifyROBO
VPN1Cluster <ROBOClusterName> -I=<MainIPAddress>
```

Syntax for resolving a Dynamic Object

You can resolve a dynamic object for a SmartLSM cluster in the SmartProvisioning GUI (double-click the SmartLSM cluster object > **Edit** window > **Dynamic Objects** tab), or with this command:

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ModifyROBO
VPN1Cluster <ROBOClusterName> -D:<DO Name>={<IP> | <IP1-IP2>}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<Profile>	Name of cluster Profile to which to map the new cluster.
<MainIPAddress>	Main IP address of cluster.
<DO Name>	Name of the Dynamic Object.
<IP>	Single IP address.
<IP1-IP2>	Range of IP addresses.

LSMcli ModifyROBOTopology VPN1Cluster

Description

You can set the VPN domain of a SmartLSM cluster in the SmartProvisioning GUI (double-click the SmartLSM cluster object > **Edit** window > **Topology** tab), or with this command.

Note - When the VPN domain is set to Manual, the IP address ranges are those set in the SmartProvisioning GUI, or with the *"LSMcli ModifyROBOManualVPNDomain" on page 904* command.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> ModifyROBOTopology
VPN1Cluster <RoboClusterName> -VPNDomain={not_defined | external_
ip_only | topology | manual}
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<RoboClusterName>	Name of the SmartLSM Cluster.
`VPNDomain`	Specifies the VPN Domain topology: ■ `not_defined` - Equivalent to the **Not Defined** option on the **Topology** tab of a SmartLSM Security Gateway in the SmartProvisioning GUI (or in the output of the *"LSMcli ShowROBOTopology" on page 917* command). ■ `external_ip_only` - Equivalent to the **Only the external interface** configuration in the SmartProvisioning GUI. ■ `topology` - Equivalent to the **All IP Addresses behind the Gateway based on Topology information** configuration in the SmartProvisioning GUI. ■ `manual` - Equivalent to **Manually defined**. VPN domain is defined according to the configuration made with the *"LSMcli ModifyROBOManualVPNDomain" on page 904* command.

LSMcli ModifyROBONetaccess VPN1Cluster

Description

For the actual SmartLSM cluster, you can override the profile topology definitions of a cluster (virtual) interface in the SmartProvisioning GUI (double-click the SmartLSM cluster object > **Edit** window > **Topology** tab), or with this command.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password>
ModifyROBONetaccess VPN1Cluster <ClusterName> <InterfaceName> -
Mode={by_profile|override} [-TopologyType={external|internal}] [-
DMZAccess={true|false}] [-InternalIP={not_defined|this|specific}
[-AllowedGroup=<GroupName>]] [-AntiSpoof={true|false} [-
AllowedGroup=<GroupName>][-SpoofTrack={none|log|alert}]]
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<ClusterName>	Name of SmartLSM cluster.
<InterfaceName>	Name of the cluster (virtual) interface. If the interface's **Network Objective** (as defined in the **Profile** topology) is **Sync only** (and not **Cluster+Sync**), there is no cluster interface, only cluster member interface. In this case, use the **Network Objective** (for example, **1st Sync**) for this parameter.
`-Mode`	Specifies the configuration mode: ■ `by_profile` - Configure as defined in the cluster **Profile**. ■ `override` - Configure the settings here. In this case, specify the "`-TopologyType`".

Parameter	Description
`-TopologyType`	Specifies the interface topology: ■ `external` - Leads out to the Internet. ■ `internal` - Leads to the local network.
`-DMZAccess`	Specifies whether this interfaces leads to DMZ (`true`), or not (`false`).
`-InternalIP`	Specifies the network behind an internal interface: ■ `not_defined` - Network is not defined. ■ `this` - Network is defined by the IP address and net mask of this interface. ■ `specific` - Network is defined by the value of the "`-AllowedGroup`".
`-AntiSpoof`	Specifies whether to perform Anti-Spoofing: ■ `true` - Perform Anti-Spoofing based on interface topology. In this case, optionally use the "`-AllowedGroup`" and "`-SpoofTrack`". ■ `false`- Do not perform Anti-Spoofing. If the interface is internal, and the IP addresses behind the interface are not defined, Anti-Spoofing is not possible.
`-AllowedGroup`	If Anti-Spoofing is performed, specifies the Network Group object, from which packets are not checked. ■ If "`-TopologyType=external`", this parameter defines a group, from which packets are not checked if Anti-Spoofing is performed ■ If "`-TopologyType=internal`", this parameter explicitly defines the networks behind the internal interface.
`-SpoofTrack`	If Anti-Spoofing is performed, specifies the tracking action when spoofing is detected: ■ `none` - No action ■ `log` - Generate a log ■ `alert` - Show an alert popup

LSMcli AddClusterSubnetOverride VPN1Cluster

Description

These settings in SmartLSM cluster objects get default values from their Profiles:

- Names of cluster member interfaces
- IP addresses of cluster member interfaces

These default values can (and in the case of IP addresses, usually must) be overridden for the individual SmartLSM cluster.

You can edit the interface properties in the SmartProvisioning GUI (in the **New SmartLSM Cluster** wizard, or double-click the SmartLSM cluster object > **Edit** window > **Topology** tab), or with this command.

Notes:

- If there is a set override value, and you want to change it, then use only the *"LSMcli ModifyClusterSubnetOverride VPN1Cluster" on page 947* command.
- If the override value you want to set is **not** defined (except at the **Profile** level), because it was never defined or because it was deleted, then use only this "`AddClusterSubnetOverride`" command.
- To cancel a value and return to the value set by the **Profile**, use the *"LSMcli DeleteClusterSubnetOverride VPN1Cluster" on page 949* command.
- To define overrides for a private (monitored or non-monitored) interface, use one of these commands:
  - *"LSMcli AddPrivateSubnetOverride VPN1ClusterMember" on page 951*
  - *"LSMcli ModifyPrivateSubnetOverride VPN1ClusterMember" on page 953*
  - *"LSMcli DeletePrivateSubnetOverride VPN1ClusterMember" on page 955*

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password>
AddClusterSubnetOverride VPN1Cluster <ROBOClusterName>
<InterfaceName> [-IName=<MembersInterfaceName>] [-
MNet=<MembersNetAddress>] [-CIP=<ClusterIPAddress> -
CNetMask=<ClusterNetMask>]
```

You must define at least one of these parameters:

- "`-IName`"
- "`-MNet`"
- "`-CIP`" *and* "`-CNetMask`"

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<ROBOClusterName>	Name of the SmartLSM cluster.
<InterfaceName>	Name of cluster (virtual) interface, as defined in the **Profile** topology. Use the name of the cluster interface even if you set values for cluster members' interfaces. If the cluster interface's **Network Objective** (as defined in the **Profile** topology) is **Sync only** (and not **Cluster+Sync**), there is no cluster interface, only cluster member interface. In this case use the **Network Objective** (for example, **1st Sync**) for this parameter.
`-IName`	New name of the interface for cluster members. The name must match the name defined in the operating system of the cluster members.
`-MNet`	New network address for cluster members. This address, together with the host parts defined in the **Profile**, produces complete IP addresses.
`-CIP`	New IP address for the cluster (virtual) interface.
`-CNetMask`	Net mask for the cluster (virtual) interface.

LSMcli ModifyClusterSubnetOverride VPN1Cluster

Description

These settings in SmartLSM cluster objects get default values from their Profiles:

- Names of cluster member interfaces
- IP addresses of cluster member interfaces

These default values can (and in the case of IP addresses, usually must) be overridden for the individual SmartLSM cluster.

You can edit the interface properties in the SmartProvisioning GUI (in the **New SmartLSM Cluster** wizard, or double-click the SmartLSM cluster object > **Edit** window > **Topology** tab), or with this command.

Notes:

- If there is a set override value, and you want to change it, then use only this "`ModifyClusterSubnetOverride`" command.
- If the override value you want to set is **not** defined (except at the **Profile** level), because it was never defined or because it was deleted, then use only the *"LSMcli AddClusterSubnetOverride VPN1Cluster" on page 945* command.
- To cancel a value and return to the value set by the **Profile**, use the *"LSMcli DeleteClusterSubnetOverride VPN1Cluster" on page 949* command.
- To define overrides for a private (monitored or non-monitored) interface, use one of these commands:
  - *"LSMcli AddPrivateSubnetOverride VPN1ClusterMember" on page 951*
  - *"LSMcli ModifyPrivateSubnetOverride VPN1ClusterMember" on page 953*
  - *"LSMcli DeletePrivateSubnetOverride VPN1ClusterMember" on page 955*

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password>
ModifyClusterSubnetOverride VPN1Cluster <ROBOClusterName>
<InterfaceName> [-IName=<MembersInterfaceName>] [-
MNet=<MembersNetAddress>] [-CIP=<ClusterIPAddress> -
CNetMask=<ClusterNetMask>]
```

You must define at least one of these parameters:

- "`-IName`"
- "`-MNet`"
- "`-CIP`" *and* "`-CNetMask`"

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<ROBOClusterName>	Name of the SmartLSM cluster.
<InterfaceName>	Name of cluster (virtual) interface, as defined in the **Profile** topology. Use the name of the cluster interface even if you set values for cluster members' interfaces. If the cluster interface's **Network Objective** (as defined in the **Profile** topology) is **Sync only** (and not **Cluster+Sync**), there is no cluster interface, only cluster member interface. In this case use the **Network Objective** (for example, **1st Sync**) for this parameter.
`-IName`	New name of the interface for cluster members. The name must match the name defined in the operating system of the cluster members.
`-MNet`	New network address for cluster members. This address, together with the host parts defined in the **Profile**, produces complete IP addresses.
`-CIP`	New IP address for the cluster (virtual) interface.
`-CNetMask`	Net mask for the cluster (virtual) interface.

LSMcli DeleteClusterSubnetOverride VPN1Cluster

Description

These settings in SmartLSM cluster objects get default values from their Profiles:

- Names of cluster member interfaces
- IP addresses of cluster member interfaces

These default values can (and in the case of IP addresses, usually must) be overridden for the individual SmartLSM cluster.

You can edit the interface properties in the SmartProvisioning GUI (in the **New SmartLSM Cluster** wizard, or double-click the SmartLSM cluster object > **Edit** window > **Topology** tab), or with this command.

Notes:

- If there is a set override value, and you want to change it, then use only this *"LSMcli ModifyClusterSubnetOverride VPN1Cluster" on page 947* command.
- If the override value you want to set is **not** defined (except at the **Profile** level), because it was never defined or because it was deleted, then use only the *"LSMcli AddClusterSubnetOverride VPN1Cluster" on page 945* command.
- To cancel a value and return to the value set by the **Profile**, use this "`DeleteClusterSubnetOverride`" command.
- To define overrides for a private (monitored or non-monitored) interface, use one of these commands:
  - *"LSMcli AddPrivateSubnetOverride VPN1ClusterMember" on page 951*
  - *"LSMcli ModifyPrivateSubnetOverride VPN1ClusterMember" on page 953*
  - *"LSMcli DeletePrivateSubnetOverride VPN1ClusterMember" on page 955*

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password>
DeleteClusterSubnetOverride VPN1Cluster <ROBOClusterName>
<InterfaceName> [-IName=<MembersInterfaceName>] [-
MNet=<MembersNetAddress>] [-CIP=<ClusterIPAddress> -
CNetMask=<ClusterNetMask>]
```

You must define at least one of these parameters:

- "`-IName`"
- "`-MNet`"
- "`-CIP`" *and* "`-CNetMask`"

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<ROBOClusterName>	Name of the SmartLSM cluster.
<InterfaceName>	Name of cluster (virtual) interface, as defined in the **Profile** topology. Use the name of the cluster interface even if you set values for cluster members' interfaces. If the cluster interface's **Network Objective** (as defined in the **Profile** topology) is **Sync only** (and not **Cluster+Sync**), there is no cluster interface, only cluster member interface. In this case use the **Network Objective** (for example, **1st Sync**) for this parameter.
`-IName`	New name of the interface for cluster members. The name must match the name defined in the operating system of the cluster members.
`-MNet`	New network address for cluster members. This address, together with the host parts defined in the **Profile**, produces complete IP addresses.
`-CIP`	New IP address for the cluster (virtual) interface.
`-CNetMask`	Net mask for the cluster (virtual) interface.

LSMcli AddPrivateSubnetOverride VPN1ClusterMember

Description

These settings in SmartLSM cluster objects get default values from their Profiles:

- Names of cluster member monitored interfaces or non-monitored interfaces
- IP addresses of cluster member monitored interfaces or non-monitored interfaces

These default values can (and in the case of IP addresses, usually must) be overridden for the individual SmartLSM cluster.

You can edit the interface properties in the SmartProvisioning GUI (in the **New SmartLSM Cluster** wizard, or double-click the SmartLSM cluster object > **Edit** window > **Topology** tab), or with this command.

Notes:

- If there is a set override value, and you want to change it, then use only the *"LSMcli ModifyPrivateSubnetOverride VPN1ClusterMember" on page 953* command.
- If the override value you want to set is **not** defined (except at the **Profile** level), because it was never defined or because it was deleted, then use only this "`AddPrivateSubnetOverride`" command.
- To cancel a value and return to the value set by the **Profile**, use the *"LSMcli DeletePrivateSubnetOverride VPN1ClusterMember" on page 955* command.
- To define overrides for a cluster interface, use one of these commands:
  - *"LSMcli AddClusterSubnetOverride VPN1Cluster" on page 945*
  - *"LSMcli ModifyClusterSubnetOverride VPN1Cluster" on page 947*
  - *"LSMcli DeleteClusterSubnetOverride VPN1Cluster" on page 949*

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password>
AddPrivateSubnetOverride VPN1ClusterMember <ROBOMemberName>
<InterfaceName> [-IName=<MembersInterfaceName>] [-
MNet=<MembersNetAddress>]
```

You must define at least one of these parameters:

- "`-IName`"
- "`-MNet`"

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<ROBOMemberName>	Name of the SmartLSM cluster member.
<InterfaceName>	Name of cluster member private interface, as defined in the **Profile** topology.
-IName	New name of the interface for cluster members. The name must match the name defined in the operating system of the cluster members.
-MNet	New network address for cluster members. This address, together with the host parts defined in the **Profile**, produces complete IP addresses.

LSMcli ModifyPrivateSubnetOverride VPN1ClusterMember

Description

These settings in SmartLSM cluster objects get default values from their Profiles:

- Names of cluster member monitored interfaces or non-monitored interfaces
- IP addresses of cluster member monitored interfaces or non-monitored interfaces

These default values can (and in the case of IP addresses, usually must) be overridden for the individual SmartLSM cluster.

You can edit the interface properties in the SmartProvisioning GUI (in the **New SmartLSM Cluster** wizard, or double-click the SmartLSM cluster object > **Edit** window > **Topology** tab), or with this command.

Notes:

- If there is a set override value, and you want to change it, then use only the "`ModifyPrivateSubnetOverride`" command.
- If the override value you want to set is **not** defined (except at the **Profile** level), because it was never defined or because it was deleted, then use only the *"LSMcli AddPrivateSubnetOverride VPN1ClusterMember" on page 951* command.
- To cancel a value and return to the value set by the **Profile**, use the *"LSMcli DeletePrivateSubnetOverride VPN1ClusterMember" on page 955* command.
- To define overrides for a cluster interface, use one of these commands:
  - *"LSMcli AddClusterSubnetOverride VPN1Cluster" on page 945*
  - *"LSMcli ModifyClusterSubnetOverride VPN1Cluster" on page 947*
  - *"LSMcli DeleteClusterSubnetOverride VPN1Cluster" on page 949*

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password>
ModifyPrivateSubnetOverride VPN1ClusterMember <ROBOMemberName>
<InterfaceName> [-IName=<MembersInterfaceName>] [-
MNet=<MembersNetAddress>]
```

You must define at least one of these parameters:

- "`-IName`"
- "`-MNet`"

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<ROBOMemberName>	Name of the SmartLSM cluster member.
<InterfaceName>	Name of cluster member private interface, as defined in the **Profile** topology.
`-IName`	New name of the interface for cluster members. The name must match the name defined in the operating system of the cluster members.
`-MNet`	New network address for cluster members. This address, together with the host parts defined in the **Profile**, produces complete IP addresses.

LSMcli DeletePrivateSubnetOverride VPN1ClusterMember

Description

These settings in SmartLSM cluster objects get default values from their Profiles:

- Names of cluster member monitored interfaces or non-monitored interfaces
- IP addresses of cluster member monitored interfaces or non-monitored interfaces

These default values can (and in the case of IP addresses, usually must) be overridden for the individual SmartLSM cluster.

You can edit the interface properties in the SmartProvisioning GUI (in the **New SmartLSM Cluster** wizard, or double-click the SmartLSM cluster object > **Edit** window > **Topology** tab), or with this command.

Notes:

- If there is a set override value, and you want to change it, then use only the *"LSMcli ModifyPrivateSubnetOverride VPN1ClusterMember" on page 953* command.
- If the override value you want to set is **not** defined (except at the **Profile** level), because it was never defined or because it was deleted, then use only the *"LSMcli AddPrivateSubnetOverride VPN1ClusterMember" on page 951* command.
- To cancel a value and return to the value set by the **Profile**, use the "`DeletePrivateSubnetOverride`" command.
- To define overrides for a cluster interface, use one of these commands:
  - *"LSMcli AddClusterSubnetOverride VPN1Cluster" on page 945*
  - *"LSMcli ModifyClusterSubnetOverride VPN1Cluster" on page 947*
  - *"LSMcli DeleteClusterSubnetOverride VPN1Cluster" on page 949*

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password>
DeletePrivateSubnetOverride VPN1ClusterMember <ROBOMemberName>
<InterfaceName> [-IName=<MembersInterfaceName>] [-
MNet=<MembersNetAddress>]
```

You must define at least one of these parameters:

- "`-IName`"
- "`-MNet`"

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<ROBOMemberName>	Name of the SmartLSM cluster member.
<InterfaceName>	Name of cluster member private interface, as defined in the **Profile** topology.
-IName	New name of the interface for cluster members. The name must match the name defined in the operating system of the cluster members.
-MNet	New network address for cluster members. This address, together with the host parts defined in the **Profile**, produces complete IP addresses.

LSMcli RemoveCluster

Description

This command:

1. Revokes all the certificates used by the SmartLSM cluster and its members.
2. Releases all the licenses.
3. Deletes the SmartLSM cluster and member objects.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> RemoveCluster
<ROBOClusterName>
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<ROBOClusterName>	Name of the SmartLSM Cluster.

Using LSMcli Commands for Small Office Appliances

This section describes `LSMcli` commands for managing Small Office Appliances and Small Office Appliance Clusters.

LSMcli AddROBO <Appliance_Model>

Description

This command adds a Small Office Appliance Gateway.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> AddROBO
<Appliance_Model> <ROBOName> <Profile> [-O=<ActivationKey> [-
I=<IP>]] [[-CA=<CaName> [-R=<CertificateIdentifier#>] [-
KEY=<AuthorizationKey>]]
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
<Appliance_Model>	Model of appliance: ■ For 1100 appliances, enter: `CPSG80` ■ For 1200R appliances, enter: `1200R` ■ For 1430 or 1450 appliances, enter: `1430/1450` ■ For 1470 or 1490 appliances, enter: `1470/1490` ■ For 1530 or 1550 appliances, enter: `1530/1550` ■ For 1570 or 1590 appliances, enter: `1570/1590`
<RoboName>	Name of a SmartLSM Security Gateway.
<Profile>	Name of a SmartLSM Security Profile that was defined in SmartConsole.
<ActivationKey>	SIC one-time password (for this action, a certificate is generated).
`IP`	IP address of the gateway (for this action, a certificate is pushed to the gateway).

Parameter	Description
<CaName>	Name of the Trusted CA object (created from SmartConsole). The IKE certificate request is sent to this CA. Default is Check Point Internal CA.
<CertificateIdentifier#>	Key identifier for third-party CA.
<AuthorizationKey>	Authorization Key for third-party CA.

Examples

- To add a 1100 appliance Security Gateway:

```
LSMcli 192.168.3.26 aa aaaa AddROBO CPSG80 Paris_GW small_
office_profile
```

- To add a 1470/1490 appliance Security Gateway:

```
LSMcli 192.168.3.26 aa aaaa AddROBO 1470/1490 Paris_GW small_
office_profile
```

LSMcli AddROBO <Appliance_Model>Cluster

Description

This command adds a Small Office Appliance Cluster.

Syntax

```
LSMcli [-d] <Mgmt Server> <Username> <Password> AddROBO
<Appliance_Model>Cluster <Profile> <MainIPAddress> <SuffixName> [-
S=<SubstitutedNamePart>] [-CA=<CaName> [-R=<KeyIdentifier#>] [-
KEY=<AuthorizationCode>]]
```

Parameters

Parameter	Description
<Mgmt Server>	Name or IP address of the Security Management Server or Domain Management Server.
<Username>	User name of standard Check Point authentication method.
<Password>	Password of standard Check Point authentication method.
*<Appliance_Model>*Cluster	Model of appliance: ■ For 1100 appliances, enter: `CPSG80Cluster` ■ For 1200R appliances, enter: `1200RCluster` ■ For 1430 or 1450 appliance, enter: `1430/1450Cluster` ■ For 1470 or 1490 appliance, enter: `1470/1490Cluster` ■ For 1530 or 1550 appliance, enter: `1530/1550Cluster` ■ For 1570 or 1590 appliance, enter: `1570/1590Cluster`
<Profile>	Name of cluster Profile to which to map the new cluster.
<MainIPAddress>	Main IP address of cluster.
<SuffixName>	A suffix to be added to cluster and member Profile names.
<SubstitutedNamePart>	A part of the Profile name to be replaced by the suffix in the previous field.
<CaName>	The name of the Trusted CA object, defined in SmartConsole, to which a VPN certificate request is sent.
<KeyIdentifier#>	Number to identify the specific certificate, once generated.

Parameter	Description
<AuthorizationCode>	Authorization Key to be sent to CA to enable certificate retrieval.

Example

To add a 1450 cluster:

```
LSMcli 192.168.3.26 aa aaaa AddRobo 1430/1450Cluster cluster_
profile 1.1.1.1 Paris
```

Other LSMcli Commands for Small Office Appliances

- For all other commands on Small Office Appliance Gateways, replace the "`VPN1`" with the "`CPSG80`", for all appliance types.

  For example, change the profile (see *"LSMcli ModifyROBO VPN1" on page 902*):

  - For a 1100 Security Gateway:

    ```
    LSMcli 192.168.3.26 aa aaaa ModifyROBO CPSG80 Paris_GW -
    P=second_small_office_profile
    ```

  - For a 1200R Security Gateway:

    ```
    LSMcli 192.168.3.26 aa aaaa ModifyROBO CPSG80 Paris_GW -
    P=second_small_office_profile
    ```

- For all other commands on Small Office Appliance clusters, replace the "`VPN1Cluster`" with the "`CPSG80Cluster`", for all appliance types (for example, in *"LSMcli ModifyROBO VPN1Cluster" on page 941*).

Security Gateway Commands

For more information about Security Gateway, see the:

- *R81.20 Security Management Administration Guide*
- *R81.20 Security Gateway Guide*

comp_init_policy

Important - This section does **not** apply to Scalable Platforms (Maestro and Chassis).

Description

Generates, loads, or removes the Initial Policy on a Security Gateway, or a Cluster Member.

Until the Security Gateway or cluster administrator installs the user-defined Security Policy on the Security Gateway or Cluster Members for the first time, security is enforced by an Initial Policy.

The Initial Policy operates by adding Check Point "implied rules" to the Default Filter to allow internal Check Point communication between the Management Server and the Security Gateway / Cluster Member.

The Initial Policy also protects a Security Gateway or Cluster Members in these cases:

- During Check Point product upgrades.
- When a SIC certificate is reset on the Security Gateway or Cluster Member.
- When Check Point product license expires.

The Security Gateway enforces the Initial until an administrator installs a user-defined policy. In subsequent boots, the Security Gateway loads the user-defined policy immediately after the Default Filter.

Important - In a Cluster, you must configure all the Cluster Members in the same way.

Notes:

- You must run this command from the Expert mode.
- The Initial Policy overwrites the user-defined policy.
- Output of the "`cpstat -f policy fw`" command (see *"cpstat" on page 1019*) shows the name of this policy as "`InitialPolicy`".
- Security Gateway, or Cluster Member stores the installed Access Control Policy in these directories:
  - `$FWDIR/state/__tmp/FW1/`
  - `$FWDIR/state/local/FW1/`
  - `$FWDIR/state/<Name of Cluster Object>/FW1/`
- Refer to these related commands:
  - *"control_bootsec" on page 973*
  - *"fwboot bootconf" on page 1253*
  - *"fw defaultgen" on page 1117*
  - *"fwboot default" on page 1266*

Syntax

```
[Expert@HostName:0]# $FWDIR/bin/comp_init_policy [-u | -U]
[Expert@HostName:0]# $FWDIR/bin/comp_init_policy [-g | -G]
```

Parameters

Parameter	Description
No Parameters	The command runs with the last used parameter.
`-u` `-U`	Performs these steps: 1. Removes an attribute **:InitialPolicySafe (true)** from the **": (FW1"** section the Check Point Registry file (`$CPDIR/registry/HKLM_registry.data`). 2. Removes the "`InitialPolicy`" policy files from the `$FWDIR/state/local/FW1/` directory.

`-g`
`-G`
	Performs these steps:
	1. Removes an attribute **:InitialPolicySafe (true)** from the **": (FW1"** section in the Check Point Registry file (`$CPDIR/registry/HKLM_registry.data`).
	2. Generates the "`InitialPolicy`" in the `$FWDIR/state/local/FW1/` directory.
	
	You can use this parameter, if there is no Initial Policy generated yet.
	If Initial Policy was already generated, make sure that after removing the Initial Policy, you delete the `$FWDIR/state/local/FW1/` directory on the Security Gateway, or Cluster Member.
	This parameter generates the Initial Policy and ensures that Security Gateway loads it the next time it fetches a policy (at "`cpstart`", at next boot, or with the "`fw fetch localhost`" command).
	The "`comp_init_policy -g`" command only works, if currently there is no policy installed on the Security Gateway, or Cluster Member.
	If you run one of these pairs of the commands, the original policy is still loaded:
	■ `comp_init_policy -g`
	`fw fetch localhost`
	■ `comp_init_policy -g`
	`cpstart`
	■ `comp_init_policy -g`
	`reboot`

Example

```
[Expert@GW:0]# cd $FWDIR/state/local/FW1/
[Expert@GW:0]#

[Expert@GW:0]# pwd
/opt/CPsuite-R81.20/fw1/state/local/FW1
[Expert@GW:0]#

[Expert@GW:0]# ls -l
total 7744
-rw-r--r-- 1 admin root   20166 Jun 13 16:34 install_policy_report.txt
-rw-r--r-- 1 admin root      55 Jun 13 16:34 install_policy_report_timing.txt
-rw-r--r-- 1 admin root   37355 Jun 13 16:34 local.Sandbox-persistence.xml
... output was cut for brevity ...
-rw-r--r-- 1 admin root    2278 Jun 13 16:34 local.vsx_cluster_netobj
-rw-r--r-- 1 admin root    5172 Jun 13 16:34 local.{939922F7-DF98-4988-B776-B70B9B8340F3}
-rw-r--r-- 1 admin root   10328 Jun 13 16:34 local.{B9D14722-3936-4B33-814B-F87EA4062BEB}
-rw-r----- 1 admin root   14743 Jun 13 16:34 manifest.C
-rw-r--r-- 1 admin root    7381 Jun 13 16:34 policy.info
-rw-r--r-- 1 admin root    2736 Jun 13 16:34 policy.map
-rw-r--r-- 1 admin root      51 Jun 13 16:34 sig.map
[Expert@GW:0]#

[Expert@GW:0]# comp_init_policy -u
erasing local state..
[Expert@GW:0]#

[Expert@GW:0]# ls -l
total 0
[Expert@GW:0]#

[Expert@GW:0]# comp_init_policy -g
initial_module:
Compiled OK.
initial_module:
Compiled OK.
[Expert@GW:0]#

[Expert@GW:0]# ls -l
total 56
-rw-rw---- 1 admin root    8 Jul 19 19:51 local.ctlver
-rw-rw---- 1 admin root 4514 Jul 19 19:51 local.fc
-rw-rw---- 1 admin root 4721 Jul 19 19:51 local.fc6
-rw-rw---- 1 admin root  235 Jul 19 19:51 local.ft
-rw-rw---- 1 admin root  317 Jul 19 19:51 local.ft6
-rw-rw---- 1 admin root  135 Jul 19 19:51 local.fwrl.conf
-rw-rw---- 1 admin root   14 Jul 19 19:51 local.ifs
-rw-rw---- 1 admin root  833 Jul 19 19:51 local.inspect.lf
-rw-rw---- 1 admin root  243 Jul 19 19:51 local.lg
-rw-rw---- 1 admin root  243 Jul 19 19:51 local.lg6
-rw-rw---- 1 admin root    0 Jul 19 19:51 local.magic
-rw-rw---- 1 admin root    3 Jul 19 19:51 local.set
-rw-rw---- 1 admin root   51 Jul 19 19:51 sig.map
[Expert@GW:0]#
```

Unloading the user-defined policy

If the installed Access Control Policy prevents administrator access to the Security Gateway or drops traffic incorrectly, you need to uninstall the current user-defined policy and install the updated policy from the Management Server.

Follow these steps to keep your Security Gateway and your networks protected when you uninstall the user-defined policy:

1. Connect to the problematic Security Gateway / each Cluster Member **through the console port**.

   Warning - If you connect over SSH, the "Initial Policy" blocks your connection.

2. Log in to the Expert mode.
3. Back up the current user-defined policy files:

   ```
   cd $FWDIR/state/local/
   tar cvf /var/log/FW1_Policy_Bkp.tar FW1
   ```

4. Remove the current user-defined policy files:

   ```
   rm $FWDIR/state/local/FW1/*
   ```

5. Generate the default Check Point policy called "`InitialPolicy`":

   ```
   comp_init_policy
   ```

6. Load the "Initial Policy":

   ```
   fw fetch local
   ```

7. Make sure the "Initial Policy" is loaded:

   ```
   cpstat -f policy fw | head -n 3
   ```

8. In SmartConsole, make the required changes and install the Access Control policy on the Security Gateway / Cluster.

connection_pipelining

Description

Controls the HyperFlow.

For more information, see the *R81.20 Performance Tuning Administration Guide*. > Section *HyperFlow*.

Syntax

Important:

- You must run this command in the Expert mode.
- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms (Maestro and Chassis), you must connect to the applicable Security Group.

```
{connection_pipelining | g_connection_pipelining}
      advanced
      on
      off
      heaviest_conn
      pipelined
      status
```

```
{connection_pipelining | g_connection_pipelining} advanced
      allow_accelerated_pipeline
      async
      default
      prevent_accelerated_pipeline
      sleep
      sync
      wake_up
```

Parameters

Parameter	Description
No Parameters	Shows the built-in help.
`connection_pipelining`	Must enter this command only on Security Gateways other than Scalable Platforms.

Parameter	Description
`g_connection_pipelining`	Must enter this command only on Scalable Platforms.
`advanced`	Shows the advanced options.
`allow_accelerated_pipeline`	Allows new connections to be opened as accelerated pipeline connections - the Security Gateway uses the new asynchronous parsers for connections. This is the default. **Notes:** ▪ This command applies only to elephant connections that opened after you run this command. ▪ When you run this command, the Security Gateway deletes all SecureXL Connection Templates with this command: `fw tab -t cphwd_tmpl -x -y` ▪ This command does **not** require a reboot.
`async`	Configures the asynchronous flow mode (this is the default). In this mode, CoreXL Firewall instances send jobs to the PPE. **Notes:** ▪ This command applies to existing elephant connections. ▪ This command does **not** require a reboot.
`default`	Restores default settings
`heaviest_conn`	Shows the statistics for the heaviest connection with the maximum duration (number of packets and bytes).
`off`	Disables the feature. **Important** - This change requires a reboot.
`on`	Enables the feature. This is the default (on Check Point Appliances that meet the requirements). **Important** - This change requires a reboot.
`pipelined`	Shows the accelerated elephant connections in the pipeline.

Parameter	Description
`prevent_accelerated_pipeline`	Prevents new connections from being opened as accelerated pipeline connections. In this mode, the Security Gateway uses the legacy parsers for connections. **Notes:** ■ Use this command only to troubleshoot issues with elephant connections. ■ This command applies only to elephant connections that opened after you run this command. ■ This command does **not** require a reboot. ■ When you run this command, the Security Gateway deletes all SecureXL Connection Templates with this command: `fw tab -t cphwd_tmpl -x -y`
`sleep`	Configures the Job Dispatcher (PPE) and Working Threads (WTs) to sleep. **Notes:** ■ Use this command only to troubleshoot issues with elephant connections, if the issue persists after you configured the synchronous flow mode. ■ This command does **not** require a reboot.
`status`	Shows the status and configuration of the feature. The output shows these lines with the applicable values: ■ `Status of connection pipelining: <Status>` ■ `Flow mode: <Mode>` ■ `Status of PPE_MGR and PPE_WT: <Status>` ■ `Status of accelerated pipeline: <Status>`
`sync`	Configures the synchronous flow mode. In this mode, CoreXL Firewall instances do **not** send jobs to the PPE. **Notes:** ■ Use this mode only to troubleshoot issues with elephant connections. ■ This command applies to existing elephant connections. ■ This command does **not** require a reboot.
`wake_up`	Wakes up the Job Dispatcher (PPE) and Working Threads (WTs) from sleep. The PPE gets CPU cores available for allocation.

Note - The terms Parallel Processing Engine (PPE) and Dual Mode Job Dispatcher (DMD) are used interchangeably.

Example 1 - On a supported appliance

```
[Expert@MyGW:0]# connection_pipelining status
Status of connection pipelining:        On
Flow mode:                              Asynchronous
Status of PPE_MGR and PPE_WT:           Active
Status of accelerated pipeline:         Allowed
[Expert@MyGW:0]#
```

Example 2 - On a non-supported appliance

```
[Expert@MyGW:0]# connection_pipelining status
Status of connection pipelining:        Off. Appliances with CPU
that does not support the AVX2 flag are not supported
[Expert@MyGW:0]#
```

control_bootsec

Important - This section does **not** apply to Scalable Platforms (Maestro and Chassis).

Description

Controls the boot security - loading of both the Default Filter policy (`defaultfilter`) and the Initial Policy (`InitialPolicy`) during boot on a Security Gateway, or a Cluster Member.

Warning - If you disable the boot security, you leave your Security Gateway, or a Cluster Member without any protection during the boot. Before you disable the boot security, we recommend to disconnect your Security Gateway, or a Cluster Member from the network completely.

Important - In a Cluster, you must configure all the Cluster Members in the same way.

Notes:

- You must run this command from the Expert mode.
- The changes made with this command survive reboot.
- Refer to these related commands:
  - *"comp_init_policy" on page 965*
  - *"fwboot bootconf" on page 1253*
  - *"fw defaultgen" on page 1117*
  - *"fwboot default" on page 1266*

Syntax

```
[Expert@GW:0]# $FWDIR/bin/control_bootsec [-g | -G]
```

```
[Expert@GW:0]# $FWDIR/bin/control_bootsec {-r | -R}
```

Parameters

Parameter	Description

No Parameter
`-g`
`-G`
	Enables the boot security:
	1. Executes the "`$FWDIR/boot/fwboot bootconf set_def $FWDIR/boot/default.bin`" command that updates the path to the Default Filter policy in the `$FWDIR/boot/boot.conf` file to point to the correct policy file (`DEFAULT_FILTER_PATH /etc/fw.boot/default.bin`).
	2. Executes the "`$FWDIR/bin/comp_init_policy -g`" command that:
	a. Removes the attribute "**:InitialPolicySafe (true)**" from the section "**: (FW1**" in the Check Point Registry (the `$CPDIR/registry/HKLM_registry.data` file).
	b. Generates the Initial Policy files in the `$FWDIR/state/local/FW1/` directory.

`-r` `-R`	Disables the boot security: 1. Executes the "`$FWDIR/boot/fwboot bootconf set_def`" command that updates the path to the Default Filter policy in the `$FWDIR/boot/boot.conf` file to point nowhere (`DEFAULT_FILTER_PATH 0`). 2. Executes the "`$FWDIR/bin/comp_init_policy -u`" command that: a. Adds the attribute "**:InitialPolicySafe (true)**" to the section "**: (FW1**" in the Check Point Registry (the `$CPDIR/registry/HKLM_registry.data` file). b. Deletes all files in the `$FWDIR/state/local/FW1/` directory.

Example 1 - Disabling the boot security

```
[Expert@GW:0]# cd $FWDIR/state/local/FW1/
[Expert@GW:0]#

[Expert@GW:0]# pwd
/opt/CPsuite-R81.20/fw1/state/local/FW1
[Expert@GW:0]#

[Expert@GW:0]# ls -l
total 7736
-rw-rw---- 1 admin root   11085 Jul 19 20:16 install_policy_report.txt
-rw-rw---- 1 admin root      56 Jul 19 20:16 install_policy_report_timing.txt
-rw-rw---- 1 admin root   37355 Jul 19 20:16 local.Sandbox-persistence.xml
-rw-rw---- 1 admin root       3 Jul 19 20:16 local.ad_query_profiles
... ... ...
-rw-r----- 1 admin root   14743 Jul 19 20:16 manifest.C
-rw-rw---- 1 admin root    7381 Jul 19 20:16 policy.info
-rw-rw---- 1 admin root    2736 Jul 19 20:16 policy.map
-rw-rw---- 1 admin root      51 Jul 19 20:16 sig.map
[Expert@GW:0]#

[Expert@GW:0]# $FWDIR/bin/control_bootsec -r
Disabling boot security
FW-1 will not load a default filter on boot
[Expert@GW:0]#

[Expert@GW:0]# cat $FWDIR/boot/boot.conf
CTL_IPFORWARDING        1
DEFAULT_FILTER_PATH     0
KERN_INSTANCE_NUM       3
COREXL_INSTALLED        1
KERN6_INSTANCE_NUM      2
IPV6_INSTALLED  0
CORE_OVERRIDE   4
[Expert@GW:0]#

[Expert@GW:0]# grep InitialPolicySafe $CPDIR/registry/HKLM_registry.data
                                      :InitialPolicySafe (true)
[Expert@GW:0]#

[Expert@GW:0]# ls -l
total 0
[Expert@GW:0]#
```

Example 2 - Enabling the boot security

```
[Expert@GW:0]# cd $FWDIR/state/local/FW1/
[Expert@GW:0]#

[Expert@GW:0]# pwd
/opt/CPsuite-R81.20/fw1/state/local/FW1
[Expert@GW:0]#

[Expert@GW:0]# control_bootsec -g
Enabling boot security
[Expert@GW:0]#

[Expert@GW:0]# cat $FWDIR/boot/boot.conf
CTL_IPFORWARDING        1
DEFAULT_FILTER_PATH     /opt/CPsuite-R81.20/fw1/boot/default.bin
KERN_INSTANCE_NUM       3
COREXL_INSTALLED        1
KERN6_INSTANCE_NUM      2
IPV6_INSTALLED  0
CORE_OVERRIDE   4
[Expert@GW:0]#

[Expert@GW:0]# grep InitialPolicySafe $CPDIR/registry/HKLM_registry.data
[Expert@GW:0]#

[Expert@GW:0]# ls -l
total 56
-rw-rw---- 1 admin root    8 Jul 19 20:22 local.ctlver
-rw-rw---- 1 admin root 4514 Jul 19 20:22 local.fc
-rw-rw---- 1 admin root 4721 Jul 19 20:22 local.fc6
-rw-rw---- 1 admin root  235 Jul 19 20:22 local.ft
-rw-rw---- 1 admin root  317 Jul 19 20:22 local.ft6
-rw-rw---- 1 admin root  135 Jul 19 20:22 local.fwrl.conf
-rw-rw---- 1 admin root   14 Jul 19 20:22 local.ifs
-rw-rw---- 1 admin root  833 Jul 19 20:22 local.inspect.lf
-rw-rw---- 1 admin root  243 Jul 19 20:22 local.lg
-rw-rw---- 1 admin root  243 Jul 19 20:22 local.lg6
-rw-rw---- 1 admin root    0 Jul 19 20:22 local.magic
-rw-rw---- 1 admin root    3 Jul 19 20:22 local.set
-rw-rw---- 1 admin root   51 Jul 19 20:22 sig.map
[Expert@GW:0]#
```

cp_conf

Description

Configures or reconfigures a Check Point product installation.

Note - The available options for each Check Point server depend on the configuration and installed products.

Syntax on a Management Server

```
cp_conf
      -h
      admin <options>
      auto <options>
      ca <options>
      client <options>
      finger <options>
      lic <options>
      snmp <options>
```

Syntax on a Security Gateway / each Cluster Member in Gaia Clish or the Expert mode

```
cp_conf
      -h
      adv_routing <options>
      auto <options>
      corexl <options>
      fullha <options>
      ha <options>
      intfs <options>
      lic <options>
      sic <options>
      snmp <options>
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cp_conf
      -h
      adv_routing <options>
      auto <options>
      corexl <options>
      fullha <options>
      ha <options>
      intfs <options>
      lic <options>
      sic <options>
      snmp <options>
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cp_conf
      -h
      adv_routing <options>
      auto <options>
      corexl <options>
      fullha <options>
      ha <options>
      intfs <options>
      lic <options>
      sic <options>
      snmp <options>
```

Parameters

Parameter	Description
`-h`	Shows the entire built-in usage.
`admin <options>`	Configures Check Point system administrators for the Security Management Server. See *"cp_conf admin" on page 65*.
`adv_routing <options>`	Enables or disables the Advanced Routing feature on this Security Gateway. **Important** - Do **not** use these outdated commands. To configure Advanced Routing, see the *R81.20 Gaia Advanced Routing Administration Guide*.

Parameter	Description
`auto <options>`	Shows and configures the automatic start of Check Point products during boot. See *"cp_conf auto" on page 68*.
`ca <options>`	■ Configures the Certificate Authority's (CA) Fully Qualified Domain Name (FQDN). ■ Initializes the Internal Certificate Authority (ICA). See *"cp_conf ca" on page 70*.
`client <options>`	Configures the GUI clients that can use SmartConsole to connect to the Security Management Server. See *"cp_conf client" on page 72*.
`corexl <options>`	Enables or disables CoreXL on this Security Gateway / Cluster Member / Security Group. See *"cp_conf corexl" on page 983*.
`finger <options>`	Shows the ICA's Fingerprint. See *"cp_conf finger" on page 76*.
`fullha <options>`	Manages Full High Availability Cluster. See *"cp_conf fullha" on page 986*. **Note** - This command does **not** apply to Scalable Platforms (Maestro and Chassis).
`ha <options>`	Enables or disables cluster membership on this Security Gateway / Cluster Member. See *"cp_conf ha" on page 987*. **Note** - This command does **not** apply to Scalable Platforms (Maestro and Chassis).
`intfs <options>`	Sets the topology of interfaces on a Security Gateway / Cluster Member, which you manage with SmartProvisioning. See *"cp_conf intfs" on page 989*. **Note** - This command does **not** apply to Scalable Platforms (Maestro and Chassis).
`lic <options>`	Manages Check Point licenses. See *"cp_conf lic" on page 78*.
`sic <options>`	Manages SIC on this Security Gateway / Cluster Member / Security Group. See *"cp_conf sic" on page 994*.

Parameter	Description
`snmp <options>`	Do **not** use these outdated commands. To configure SNMP, see the *R81.20 Gaia Administration Guide* - Chapter *System Management* - Section *SNMP*.

cp_conf auto

Description

Shows and controls which of Check Point products start automatically during boot.

Note - This command corresponds to the option **Automatic start of Check Point Products** in the *"cpconfig" on page 134* menu.

Note - On a Multi-Domain Server, use the option **Automatic Start of Multi-Domain Server** in the *"mdsconfig" on page 762*menu.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cp_conf auto
      -h
      {enable | disable} <Product1> <Product2> ...
      get all
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cp_conf auto
      -h
      {enable | disable} <Product1> <Product2> ...
      get all
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cp_conf auto
      -h
      {enable | disable} <Product1> <Product2> ...
      get all
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cp_conf auto
      -h
      {enable | disable} <Product1> <Product2> ...
      get all
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`{enable | disable} <Product1> <Product2> ...`	Controls whether the installed Check Point products start automatically during boot. This command is for Check Point use only.
`get all`	Shows which of these Check Point products start automatically during boot: ■ Check Point Security Gateway ■ QoS (former FloodGate-1) ■ SmartEvent Suite

Example from a Security Management Server

```
[Expert@MGMT:0]# cp_conf auto get all
Check Point Security Gateway is not installed

QoS is not installed

The SmartEvent Suite will start automatically at boot time.

[Expert@MGMT:0]#
```

Example from a Security Gateway

```
[Expert@GW:0] cp_conf auto get all
The Check Point Security Gateway will start automatically at boot time.

QoS will start automatically at boot time.

SmartEvent Suite is not installed.

[Expert@GW:0]#
```

cp_conf corexl

Description

Enables or disables CoreXL.

For more information, see the *R81.20 Performance Tuning Administration Guide*.

Important:

- This command is for Check Point use only.
  To configure CoreXL, use the **Check Point CoreXL** option in the *"cpconfig" on page 996* menu.
- After all changes in CoreXL configuration on the Security Gateway / Cluster Member / Security Group, you must reboot it.
- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms (Maestro and Chassis), you must connect to the applicable Security Group.

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

- To enable CoreXL with 'n' IPv4 Firewall instances and optionally 'k' IPv6 Firewall instances:

```
cp_conf corexl [-v] enable [n] [-6 k]
```

- To disable CoreXL:

```
cp_conf corexl [-v] disable
```

Syntax on a Scalable Platform Security Group in Gaia gClish

- To enable CoreXL with 'n' IPv4 Firewall instances and optionally 'k' IPv6 Firewall instances:

```
cp_conf corexl [-v] enable [n] [-6 k]
```

- To disable CoreXL:

```
cp_conf corexl [-v] disable
```

Syntax on a Scalable Platform Security Group in the Expert mode

- To enable CoreXL with 'n' IPv4 Firewall instances and optionally 'k' IPv6 Firewall instances:

```
g_all cp_conf corexl [-v] enable [n] [-6 k]
```

- To disable CoreXL:

```
g_all cp_conf corexl [-v] disable
```

The related command is: *"fwboot corexl" on page 1257*.

Parameters

Parameter	Description
-v	Leaves the high memory (vmalloc) unchanged.
n	Denotes the number of IPv4 CoreXL Firewall instances.
k	Denotes the number of IPv6 CoreXL Firewall instances.

Example

Currently, the Security Gateway runs two IP4v CoreXL Firewall instances (`KERN_INSTANCE_NUM = 2`).

We change the number of IP4v CoreXL Firewall instances to three.

```
[Expert@MyGW:0]# fw ctl multik stat
ID | Active  | CPU    | Connections | Peak
----------------------------------------------
 0 | Yes     | 2      |           7 |       28
 1 | Yes     | 1      |           0 |       11
[Expert@MyGW:0]#
[Expert@MyGW:0]# cat /etc/fw.boot/boot.conf
CTL_IPFORWARDING 1
DEFAULT_FILTER_PATH 0
KERN_INSTANCE_NUM 2
COREXL_INSTALLED 1
KERN6_INSTANCE_NUM 2
IPV6_INSTALLED 0
CORE_OVERRIDE 4
[Expert@MyGW:0]#
[Expert@MyGW:0]# cp_conf corexl -v enable 3
[Expert@MyGW:0]#
[Expert@MyGW:0]# cat /etc/fw.boot/boot.conf
CTL_IPFORWARDING 1
DEFAULT_FILTER_PATH 0
KERN_INSTANCE_NUM 3
COREXL_INSTALLED 1
KERN6_INSTANCE_NUM 2
IPV6_INSTALLED 0
CORE_OVERRIDE 4
[Expert@MyGW:0]#
[Expert@MyGW:0]# reboot
.. ... ...
[Expert@MyGW:0]# fw ctl multik stat
ID | Active  | CPU    | Connections | Peak
----------------------------------------------
 0 | Yes     | 3      |           7 |       28
 1 | Yes     | 2      |           0 |       11
 2 | Yes     | 1      |           4 |       10
[Expert@MyGW:0]#
```

cp_conf fullha

Important - This command does **not** apply to Scalable Platforms (Maestro and Chassis).

Description

Manages the state of the Full High Availability Cluster:

- Enables the Full High Availability Cluster
- Disables the Full High Availability Cluster
- Deletes the Full High Availability peer
- Shows the Full High Availability state

Important - To configure a Full High Availability cluster, follow the *R81.20 Installation and Upgrade Guide*.

Syntax

```
cp_conf fullha
      enable
      del_peer
      disable
      state
```

Parameters

Parameter	Description
`enable`	Enables the Full High Availability on this computer.
`del_peer`	Deletes the Full High Availability peer from the configuration.
`disable`	Disables the Full High Availability on this computer.
`state`	Shows the Full High Availability state on this computer.

Example

```
[Expert@Cluster_Member:0]# cp_conf fullha state
FullHA is currently enabled
[Expert@Cluster_Member:0]#
```

cp_conf ha

Important - This command does **not** apply to Scalable Platforms (Maestro and Chassis).

Description

Enables or disables cluster membership on this Security Gateway.

Important - This command is for Check Point use only. To configure cluster membership, you must use the *"cpconfig" on page 996* command.
For more information, see the *R81.20 ClusterXL Administration Guide*.

Syntax

```
cp_conf ha {enable | disable} [norestart]
```

Parameters

Parameter	Description
`enable`	Enables cluster membership on this Security Gateway. This command is equivalent to the option **Enable cluster membership for this gateway** in the *"cpconfig" on page 996* menu.
`disable`	Disables cluster membership on this Security Gateway. This command is equivalent to the option **Disable cluster membership for this gateway** in the *"cpconfig" on page 996* menu.
`norestart`	**Optional:** Specifies to apply the configuration change without the restart of Check Point services. The new configuration takes effect only after reboot.

Example 1 - Enable the cluster membership without restart of Check Point services

```
[Expert@MyGW:0]# cp_conf ha enable norestart

Cluster membership for this gateway was enabled successfully
Important: This change will take effect after reboot.

[Expert@MyGW:0]#
```

Example 2 - Disable the cluster membership without restart of Check Point services

```
[Expert@MyGW:0]# cp_conf ha disable norestart
cpwd_admin:
Process CPHAMCSET process has been already terminated

Cluster membership for this gateway was disabled successfully
Important: This change will take effect after reboot.

[Expert@MyGW:0]#
```

cp_conf intfs

Important - This command does **not** apply to Scalable Platforms (Maestro and Chassis).

Description

Sets the topology of interfaces on a Security Gateway, which you manage with SmartProvisioning.

For more information, see the *R81.20 SmartProvisioning Administration Guide*.

Syntax

```
cp_conf intfs
      get
      set
            auxiliary <Name of Interface>
            DMZ <Name of Interface>
            external <Name of Interface>
            internal <Name of Interface>
```

Parameters

Parameter	Description
`get`	Shows the list of configured interfaces.
`set`	Configures the topology of the specified interface: ■ `auxiliary` ■ `DMZ` ■ `external` ■ `internal`

cp_conf lic

Description

Shows, adds and deletes Check Point licenses.

Note - This command corresponds to the option **Licenses and contracts** in the *"cpconfig" on page 134* menu.

Note:
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cp_conf lic
      -h
      add -f <Full Path to License File>
      add -m <Host> <Date> <Signature Key> <SKU/Features>
      del <Signature Key>
      get [-x]
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cp_conf lic
      -h
      add -f <Full Path to License File>
      add -m <Host> <Date> <Signature Key> <SKU/Features>
      del <Signature Key>
      get [-x]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cp_conf lic
      -h
      add -f <Full Path to License File>
      add -m <Host> <Date> <Signature Key> <SKU/Features>
      del <Signature Key>
      get [-x]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cp_conf lic
      -h
      add -f <Full Path to License File>
      add -m <Host> <Date> <Signature Key> <SKU/Features>
      del <Signature Key>
      get [-x]
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`add -f <Full Path to License File>`	Adds a license from the specified Check Point license file. You get this license file in the *Check Point User Center*. This is the same command as the *"cplic db_add" on page 144*.
`add -m <Host> <Date> <Signature Key> <SKU/Features>`	Adds the license manually. You get these license details in the *Check Point User Center*. This is the same command as the *"cplic db_add" on page 144*.
`del <Signature Key>`	Delete the license based on its signature. This is the same command as the *"cplic del" on page 149*.
`get [-x]`	Shows the local installed licenses. If you specify the "`-x`" parameter, output also shows the signature key for every installed license. This is the same command as the *"cplic print" on page 153*.

Example 1 - Adding the license from the file

```
[Expert@HostName:0]# cp_conf lic add -f ~/License.lic
License was installed successfully.
[Expert@HostName:0]#

[Expert@HostName:0]# cp_conf lic get
Host            Expiration   Signature                                  Features
192.168.3.28    25Aug2019    xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx   CPMP-XXX
[Expert@HostName:0]#
```

Example 2 - Adding the license manually

```
[Expert@MyHostName:0]# cp_conf lic add -m MyHostName 25Aug2019
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx CPMP-XXX
License was successfully installed
[Expert@MyHostName:0]#

[Expert@MyHostName:0]# cp_conf lic get
Host             Expiration   Signature                                 Features
192.168.3.28     25Aug2019    xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx   CPMP-XXX
[Expert@MyHostName:0]#
```

cp_conf sic

Description

Manages SIC on the Security Gateway.

For additional information, see sk65764: How to reset SIC.

Note - This command corresponds to the option **Secure Internal Communication** in the *"cpconfig" on page 996* menu.

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cp_conf
      -h
      sic
            cert_pull <Management Server> <DAIP GW object>
            init <Activation Key> [norestart]
            state
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cp_conf
      -h
      sic
            cert_pull <Management Server> <DAIP GW object>
            init <Activation Key> [norestart]
            state
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cp_conf
      -h
      sic
            cert_pull <Management Server> <DAIP GW object>
            init <Activation Key> [norestart]
            state
```

Parameters

Parameter	Description
`-h`	Shows the built-in usage.
`cert_pull <Management Server> <DAIP GW object>`	For DAIP Security Gateways, pulls a SIC certificate from the specified Management Server for the specified DAIP Security Gateway: ■ *<Management Server>* - IPv4 address or HostName of the Security Management Server or Domain Management Server ■ *<DAIP GW object>* - Name of the DAIP Security Gateway object as configured in SmartConsole
`init <Activation Key> [norestart]`	Resets the one-time SIC activation key. The optional parameter "`norestart`" specifies not to restart Check Point services.
`state`	Shows the current state of the SIC Trust.

Example

```
[Expert@MyGW:0]# cp_conf sic state

Trust State: Trust established

[Expert@MyGW:0]#
```

cpconfig

Description

This command starts the Check Point Configuration Tool.

This tool configures specific settings for the installed Check Point products.

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms (Maestro and Chassis), you must connect to the applicable Security Group.

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpconfig
```

Syntax on a Scalable Platform Security Group in Gaia gClish or the Expert mode

```
cpconfig
```

Menu Options

Note - The options shown depend on the configuration and installed products.

Menu Option	Description
Licenses and contracts	Manages Check Point licenses and contracts on this Security Gateway or Cluster Member.
SNMP Extension	Obsolete. Do **not** use this option anymore. To configure SNMP, see the *R81.20 Gaia Administration Guide* - Chapter *System Management* - Section *SNMP*.
PKCS#11 Token	Register a cryptographic token, for use by Gaia Operating System. See details of the token, and test its functionality.
Random Pool	Configures the RSA keys, to be used by Gaia Operating System.

Menu Option	Description
Secure Internal Communication	Manages SIC on the Security Gateway or Cluster Member. This change requires a restart of Check Point services on the Security Gateway or Cluster Member. For more information, see: ■ The *R81.20 Security Management Administration Guide*. ■ sk65764: How to reset SIC.
Enable cluster membership for this gateway	Enables the cluster membership on the Security Gateway. This change requires a reboot of the Security Gateway. For more information, see the: ■ *R81.20 Installation and Upgrade Guide*. ■ *R81.20 ClusterXL Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (Maestro and Chassis).
Disable cluster membership for this gateway	Disables the cluster membership on the Security Gateway. This change requires a reboot of the Security Gateway. For more information, see the: ■ *R81.20 Installation and Upgrade Guide*. ■ *R81.20 ClusterXL Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (Maestro and Chassis).
Enable Check Point Per Virtual System State	Enables Virtual System Load Sharing on the VSX Cluster Member. For more information, see the *R81.20 VSX Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (Maestro and Chassis).
Disable Check Point Per Virtual System State	Disables Virtual System Load Sharing on the VSX Cluster Member. For more information, see the *R81.20 VSX Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (Maestro and Chassis).

Menu Option	Description
Enable Check Point ClusterXL for Bridge Active/Standby	Enables Check Point ClusterXL for Bridge mode. This change requires a reboot of the Cluster Member. For more information, see the: ■ *R81.20 Installation and Upgrade Guide*. ■ *R81.20 ClusterXL Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (Maestro and Chassis).
Disable Check Point ClusterXL for Bridge Active/Standby	Disables Check Point ClusterXL for Bridge mode. This change requires a reboot of the Cluster Member. For more information, see the: ■ *R81.20 Installation and Upgrade Guide*. ■ *R81.20 ClusterXL Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (Maestro and Chassis).
Check Point CoreXL	Manages CoreXL and Firewall mode on the Security Gateway / Cluster Member / Scalable Platform Security Group. After all changes in CoreXL configuration, you must reboot the Security Gateway / Cluster Member / Security Group. For more information, see the *R81.20 Performance Tuning Administration Guide*.
Automatic start of Check Point Products	Shows and controls which of the installed Check Point products start automatically during boot.
Exit	Exits from the Check Point Configuration Tool.

Example 1 - Menu on a single Security Gateway

```
[Expert@MySingleGW:0]# cpconfig
This program will let you re-configure
your Check Point products configuration.


Configuration Options:
----------------------
(1) Licenses and contracts
(2) SNMP Extension
(3) PKCS#11 Token
(4) Random Pool
(5) Secure Internal Communication
(6) Enable cluster membership for this gateway
(7) Check Point CoreXL
(8) Automatic start of Check Point Products

(9) Exit

Enter your choice (1-9) :
```

Example 2 - Menu on a Cluster Member

```
[Expert@MyClusterMember:0]# cpconfig
This program will let you re-configure
your Check Point products configuration.


Configuration Options:
----------------------
(1) Licenses and contracts
(2) SNMP Extension
(3) PKCS#11 Token
(4) Random Pool
(5) Secure Internal Communication
(6) Disable cluster membership for this gateway
(7) Enable Check Point Per Virtual System State
(8) Enable Check Point ClusterXL for Bridge Active/Standby
(9) Check Point CoreXL
(10) Automatic start of Check Point Products

(11) Exit

Enter your choice (1-11) :
```

cplic

Description

The `cplic` command manages Check Point licenses.

You can run this command:

- On a Security Gateway / Cluster Member in Gaia Clish or the Expert mode
- On a Scalable Platform Security Group in Gaia gClish or the Expert mode

License Management is divided into three types of commands:

Licensing Commands	Applies To	Description
Local licensing commands	Management Servers, Security Gateways, Cluster Members, and Scalable Platform Security Groups	You execute these commands locally on the Check Point servers and gateways.
Remote licensing commands	Management Servers only	You execute these commands on the Security Management Server or Domain Management Server. These changes apply to the managed Security Gateways and Cluster Members.
License Repository commands	Management Servers only	You execute these commands on the Security Management Server or Domain Management Server. These changes apply to the licenses stored in the local license repository.

For more about managing licenses, see the *R81.20 Security Management Administration Guide*.

Syntax for Local Licensing on a Security Gateway / Cluster Member / Security Group

```
cplic [-d]
      {-h | -help}
      check <options>
      contract <options>
      del <options>
      print <options>
      put <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{-h | -help}`	Shows the applicable built-in usage.
`check <options>`	Confirms that the license includes the feature on the local Security Gateway or Security Management Server. See *"cplic check" on page 1002*.
`contract <options>`	Manages (deletes and installs) the Check Point Service Contract on the local Check Point server. See *"cplic contract" on page 1004*.
`del <options>`	Deletes a Check Point license on a host, including unwanted evaluation, expired, and other licenses. See *"cplic del" on page 1006*.
`print <options>`	Prints details of the installed Check Point licenses on the local Check Point server. See *"cplic print" on page 1007*.
`put <options>`	Installs and attaches licenses on a Check Point server. See *"cplic put" on page 1009*.

cplic check

Description

Confirms that the license includes the feature on the local Security Gateway or Management Server. See sk66245.

Syntax

```
cplic check {-h | -help}
```

```
cplic [-d] check [-p <Product>] [-v <Version>] [{-c | -count}] [-t <Date>] [{-r | -routers}] [{-S | -SRusers}] <Feature>
```

You can run this command:

- On a Management Server / Security Gateway / Cluster Member in Gaia Clish or the Expert mode
- On a Scalable Platform Security Group in Gaia gClish or the Expert mode

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p <Product>`	Product, for which license information is requested. Some examples of products: ■ `fw1` - FireWall-1 infrastructure on Security Gateway / Cluster Member / Security Group (all Software Blades), or Management Server (all Software Blades) ■ `mgmt` - Multi-Domain Server infrastructure ■ `services` - Entitlement for various services ■ `cvpn` - Mobile Access ■ `etm` - QoS (FloodGate-1) ■ `eps` - Endpoint Software Blades on Management Server
`-v <Version>`	Product version, for which license information is requested.

Parameter	Description
`{-c | -count}`	Outputs the number of licenses connected to this feature.
`-t <Date>`	Checks license status on future date. Use the format **ddmmyyyy**. A feature can be valid on a given date on one license, but invalid on another.
`{-r | -routers}`	Checks how many routers are allowed. The *<Feature>* option is not needed.
`{-S | -SRusers}`	Checks how many SecuRemote users are allowed.
<Feature>	Feature, for which license information is requested.

Example from a Management Server

```
[Expert@MGMT]# cplic print -p
Host Expiration Primitive-Features
W.X.Y.Z 24Mar2016 ::CK-XXXXXXXXXXX fw1:6.0:swb fw1:6.0:comp fw1:6.0:compunlimited fw1:6.0:cluster-1 fw1:6.0:cpxmgmt_qos_u_sites
fw1:6.0:sprounl fw1:6.0:nxunlimit fw1:6.0:swp evnt:6.0:smrt_evnt fw1:6.0:fwc fw1:6.0:ca fw1:6.0:rtmui fw1:6.0:sstui fw1:6.0:fwlv
fw1:6.0:cmd evnt:6.0:alzd5 evnt:6.0:alzc1 evnt:6.0:alzs1 fw1:6.0:sstui fw1:6.0:fwlv fw1:6.0:sme10 etm:6.0:rtm_u fw1:6.0:cep1 fw1:6.0:rt
fw1:6.0:cemid fw1:6.0:web_sec_u fw1:6.0:workflow fw1:6.0:ram1 fw1:6.0:routers fw1:6.0:supmgmt fw1:6.0:supunlimit fw1:6.0:prov
fw1:6.0:atlas-unlimit fw1:6.0:filter fw1:6.0:ui psmp:6.0:psmsunlimited fw1:6.0:vpe_unlimit fw1:6.0:cluster-u fw1:6.0:remote1 fw1:6.0:aes
fw1:6.0:strong fw1:6.0:rdp fw1:6.0:des fw1:6.0:isakmp fw1:6.0:dbvr_unlimit fw1:6.0:cmpmgmt fw1:6.0:rtmmgmt fw1:6.0:fgmgmt fw1:6.0:blades
fw1:6.0:cpipv6 fw1:6.0:mgmtha fw1:6.0:remote
[Expert@MGMT]#
```

Example from a Management Server in High Availability

```
[Expert@MGMT]# cplic check -p fw1 -v 6.0 -c mgmtha
cplic check 'mgmtha': 1 licenses
[Expert@MGMT]#
```

Example from a Security Gateway

```
[Expert@GW]# cplic print -p
Host Expiration Primitive-Features
W.X.Y.Z 23Mar2016 ::CK-XXXXXXXXXXX fw1:6.0:swb fw1:6.0:abot fw1:6.0:ips fw1:6.0:appi fw1:6.0:aspm fw1:6.0:av1000 fw1:6.0:urlf fw1:6.0:av
fw1:6.0:vsx5 fw1:6.0:cpls fw1:6.0:cluster-u fw1:6.0:mpu fw1:6.0:sxl_vpn fw1:6.0:sxl_fw fw1:6.0:sxl_ppk fw1:6.0:connect fw1:6.0:pam
etm:6.0:fgcountunl etm:6.0:fg etm:6.0:tclog etm:6.0:fgvpn fw1:6.0:identity cvpn:6.0:ccvunl cvpn:6.0:cvpnunlimited fw1:6.0:des
fw1:6.0:strong fw1:6.0:encryption cvpn:6.0:cvpn fw1:6.0:dlp evnt:6.0:smrt_evnt fw1:6.0:ipsa fw1:6.0:spcps fw1:6.0:pam
fw1:6.0:enchostsunlimit fw1:6.0:aes fw1:6.0:rdp fw1:6.0:isakmp fw1:6.0:xlate fw1:6.0:auth fw1:6.0:content fw1:6.0:sync fw1:6.0:fm
fw1:6.0:blades fw1:6.0:sr5000 fw1:6.0:hostsunlimit fw1:6.0:mc_all_8 fw1:6.0:multicore
[Expert@GW]#
```

Example from a Cluster Member

```
[Expert@GW]# cplic check cluster-u
cplic check 'cluster-u': license valid
[Expert@GW]#
[Expert@GW]# cplic check -c cluster-u
cplic check 'cluster-u': 9 licenses
[Expert@GW]#
```

cplic contract

Description

Deletes the Check Point Service Contract on the local Check Point server.

Installs the Check Point Service Contract on the local Check Point server.

Note

- For more information about Service Contract files, see sk33089: What is a Service Contract File?
- If you install a Service Contract on a managed Security Gateway / Cluster Member / Scalable Platform Security Group, you must update the license repository on the applicable Management Server - either with the *"cplic get" on page 151* command, or in SmartUpdate.

Syntax

```
cplic contract -h
```

```
cplic [-d] contract
      del
            -h
            <Service Contract ID>
      put
            -h
            [{-o | -overwrite}] <Service Contract File>
```

You can run this command:

- On a Management Server / Security Gateway / Cluster Member in Gaia Clish or the Expert mode
- On a Scalable Platform Security Group in Gaia gClish or the Expert mode

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`del`	Deletes the Service Contract from the `$CPDIR/conf/cp.contract` file on the local Check Point server.
`put`	Merges the Service Contract to the `$CPDIR/conf/cp.contract` file on the local Check Point server.
<Service Contract ID>	ID of the Service Contract.
`{-o | -overwrite}`	Specifies to overwrite the current Service Contract.
<Service Contract File>	Path to and the name of the Service Contract file. First, you must download the Service Contract file from your *Check Point User Center* account.

cplic del

Description

Deletes a Check Point license on a host, including unwanted evaluation, expired, and other licenses.

This command can delete a license on both local server, and on remote managed servers.

Syntax

```
cplic del {-h | -help}
cplic [-d] del [-F <Output File>] <Signature> <Object Name>
```

You can run this command:

- On a Management Server / Security Gateway / Cluster Member in Gaia Clish or the Expert mode
- On a Scalable Platform Security Group in Gaia gClish or the Expert mode

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-F <Output File>`	Saves the command output to the specified file.
`<Signature>`	The signature string within the license. To see the license signature string, run the *"cplic print" on page 153* command.
`<Object Name>`	The name of the Security Gateway / Cluster Member object as configured in SmartConsole.

cplic print

Description

Prints details of the installed Check Point licenses on the local Check Point server.

Note - On a Security Gateway / Cluster Member / Scalable Platform Security Group, this command prints all installed licenses (both Local and Central).

Syntax

```
cplic print {-h | -help}
```

```
cplic [-d] print[{-n | -noheader}] [-x] [{-t | -type}] [-F <Output File>] [{-p | -preatures}] [-D]
```

You can run this command:

- On a Management Server / Security Gateway / Cluster Member in Gaia Clish or the Expert mode
- On a Scalable Platform Security Group in Gaia gClish or the Expert mode

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{-n | -noheader}`	Prints licenses with no header.
`-x`	Prints licenses with their signature.
`{-t | -type]`	Prints licenses showing their type: Central or Local.
`-F <Output File>`	Saves the command output to the specified file.
`{-p | -preatures}`	Prints licenses resolved to primitive features.
`-D`	On a Multi-Domain Server, prints only Domain licenses.

Example 1

```
[Expert@HostName:0]# cplic print
Host             Expiration   Features
192.168.3.28     25Aug2019    CPMP-XXX  CK-XXXXXXXXXXX
[Expert@HostName:0]#
```

Example 2

```
[Expert@HostName:0]# cplic print -x
Host             Expiration   Signature                          Features
192.168.3.28     25Aug2019    xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx   CPMP-XXX  CK-XXXXXXXXXXX
[Expert@HostName:0]#
```

cplic put

Description

Installs one or more Local licenses on a Check Point server.

Note - You get the license details in the *Check Point User Center*.

Syntax

```
cplic put {-h | -help}
```

```
cplic [-d] put [{-o | -overwrite}] [{-c | -check-only}] [{-s | -select}] [-F <Output File>] [{-P | -Pre-boot}] [{-k | -kernel-only}] -l <License File> [<Host>] [<Expiration Date>] [<Signature>] [<SKU/Features>]
```

You can run this command:

- On a Management Server / Security Gateway / Cluster Member in Gaia Clish or the Expert mode
- On a Scalable Platform Security Group in Gaia gClish or the Expert mode

Parameters

Parameter	Description
`{-h | -help}`	Shows the applicable built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{-o | -overwrite}`	On a Security Gateway / Cluster Member / Scalable Platform Security Group, this command erases only the local licenses, but not central licenses that are installed remotely.
`{-c | -check-only}`	Verifies the license. Checks if the IP of the license matches the Check Point server and if the signature is valid.
`{-s | -select}`	Selects only the local license whose IP address matches the IP address of the Check Point server.

Parameter	Description
`-F <Output File>`	Saves the command output to the specified file.
`{-P | -Pre-boot}`	Use this option after you have upgraded and before you reboot the Check Point server. Use of this option will prevent certain error messages.
`{-K | -kernel-only}`	Pushes the current valid licenses to the kernel. For use by Check Point Support only.
`-l <License File>`	Name of the file that contains the license.
<Host>	Hostname or IP address of the Security Gateway / Cluster Member / Scalable Platform Security Group for a local license. Hostname or IP address of the Security Management Server / Domain Management Server for a central license.
<Expiration Date>	The license expiration date.
<Signature>	The signature string within the license. Case sensitive. The hyphens are optional.
<SKU/Features>	The SKU of the license summarizes the features included in the license. For example: `CPSUITE-EVAL-3DES-vNG`

Copy and paste the parameters from the license received from the User Center:

Parameter	Description
`host`	The IPv4 address of the external interface (in quad-dot notation).
`expiration date`	The license expiration date. It can be `never`.
`signature`	The license signature string. Case sensitive. The hyphens are optional.
`SKU/features`	A string listing the SKU and the Certificate Key of the license. The SKU of the license summarizes the features included in the license. For example: `CPSB-SWB CPSB-ADNC-M CK0123456789ab`

Example

```
[Expert@HostName:0]# cplic put -l License.lic
Host Expiration SKU
192.168.2.3 14Jan2016  CPSB-SWB CPSB-ADNC-M CK0123456789ab
[Expert@HostName:0]#
```

cpprod_util

Description

This utility works with Check Point Registry (`$CPDIR/registry/HKLM_registry.data`) without manually opening it:

- Shows which Check Point products and features are enabled on this Check Point server.
- Enables and disables Check Point products and features on this Check Point server.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpprod_util CPPROD_GetValue "<Product>" "<Parameter>" {0|1}
```

```
cpprod_util CPPROD_SetValue "<Product>" "<Parameter>" {1|4}
"<Value>" {0|1}
```

```
cpprod_util -dump
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpprod_util CPPROD_GetValue "<Product>" "<Parameter>" {0|1}
```

```
cpprod_util CPPROD_SetValue "<Product>" "<Parameter>" {1|4}
"<Value>" {0|1}
```

```
cpprod_util -dump
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpprod_util CPPROD_GetValue "<Product>" "<Parameter>" {0|1}
```

```
cpprod_util CPPROD_SetValue "<Product>" "<Parameter>" {1|4}
"<Value>" {0|1}
```

```
cpprod_util -dump
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpprod_util CPPROD_GetValue "<Product>" "<Parameter>" {0|1}
```

```
g_all cpprod_util CPPROD_SetValue "<Product>" "<Parameter>" {1|4}
"<Value>" {0|1}
```

```
g_all cpprod_util -dump
```

Parameters

Parameter	Description
`CPPROD_GetValue`	Gets the configuration status of the specified product or feature: ■ 0 - Disabled ■ 1 - Enabled
`CPPROD_SetValue`	Sets the configuration for the specified product or feature. **Important** - Do not run these commands unless explicitly instructed by Check Point Support or R&D to do so.
"<*Product*>"	Specifies the product or feature.
"<*Parameter*>"	Specifies the configuration parameter for the specified product or feature.
"<*Value*>"	Specifies the value of the configuration parameter for the specified product or feature: ■ One of these integers: 0, 1, 4 ■ A string
`dump`	Creates a dump file of the Check Point Registry (`$CPDIR/registry/HKLM_registry.data`) in the current working directory. The name of the output file is `RegDump`.

Notes

- On a Multi-Domain Server, you must run this command in the context of the relevant Domain Management Server.
- If you run the "`cpprod_util`" command without parameters, it prints:
  - The list of all available products and features (for example, "`FwIsFirewallMgmt`", "`FwIsLogServer`", "`FwIsStandAlone`")
  - The type of the expected argument when you configure a product or feature ("`no-parameter`", "`string-parameter`", or "`integer-parameter`")
  - The type of the returned output ("`status-output`", or "`no-output`")
- To redirect the output of the "`cpprod_util`" command, it is necessary to redirect the *stderr* to *stdout*:

  ```
  cpprod_util <options> > <output file> 2>&1
  ```

  Example:

  ```
  cpprod_util > /tmp/output_of_cpprod_util.txt 2>&1
  ```

Examples

Example - Showing a list of all installed Check Point Products Packages on a Management Server

```
[Expert@MGMT:0]# cpprod_util CPPROD_GetInstalledProducts
CPFC
IDA
MGMT
FW1
SecurePlatform
NGXCMP
EdgeCmp
SFWCMP
SFWR75CMP
SFWR77CMP
FLICMP
R75CMP
R7520CMP
R7540CMP
R76CMP
R77CMP
PROVIDER-1
Reporting Module
SmartLog
CPinfo
VSEC
DIAG
[Expert@MGMT:0]#
```

Example - Checking if this Check Point server is configured as a Management Server

```
[Expert@MGMT:0]# cpprod_util FwIsFirewallMgmt
1
[Expert@MGMT:0]#
```

Example - Checking if this Check Point server is configured as a Standalone

```
[Expert@MGMT:0]# cpprod_util FwIsStandAlone
0
[Expert@MGMT:0]#
```

Example - Checking if this Management Server is configured as a Primary in High Availability

```
[Expert@MGMT:0]# cpprod_util FwIsPrimary
1
[Expert@MGMT:0]#
```

Example - Checking if this Management Server is configured as Active in High Availability

```
[Expert@MGMT:0]# cpprod_util FwIsActiveManagement
1
[Expert@MGMT:0]#
```

Example - Checking if this Management Server is configured as Backup in High Availability

```
[Expert@MGMT:0]# cpprod_util FwIsSMCBackup
1
[Expert@MGMT:0]#
```

Example - Checking if this Check Point server is configured as a dedicated Log Server

```
[Expert@MGMT:0]# cpprod_util FwIsLogServer
1
[Expert@MGMT:0]#
```

Example - Checking if on this Management Server the SmartProvisioning blade is enabled

```
[Expert@MGMT:0]# cpprod_util FwIsAtlasManagement
1
[Expert@MGMT:0]#
```

Example - Checking if on this Management Server the SmartEvent Server blade is enabled

```
[Expert@MGMT:0]# cpprod_util RtIsAnalyzerServer
1
[Expert@MGMT:0]#
```

Example - Checking if on this Management Server the SmartEvent Correlation Unit blade is enabled

```
[Expert@MGMT:0]# cpprod_util RtIsAnalyzerCorrelationUnit
1
[Expert@MGMT:0]#
```

Example - Checking if on this Management Server the Endpoint Policy Management blade is enabled

```
[Expert@MGMT:0]# cpprod_util UepmIsInstalled
1
[Expert@MGMT:0]#
```

Example - Checking if this Management Server is configured as Endpoint Policy Server

```
[Expert@MGMT:0]# cpprod_util UepmIsPolicyServer
0
[Expert@MGMT:0]#
```

Example - Showing a list of all installed Check Point Products Packages on a Security Gateway

```
[Expert@MyGW:0]# cpprod_util CPPROD_GetInstalledProducts
CPFC
IDA
MGMT
FW1
SecurePlatform
CPinfo
DIAG
PPACK
CVPN
[Expert@MyGW:0]#
```

Example - Checking if this Security Gateway is configured as a VSX Gateway

```
[Expert@MyGW:0]# cpprod_util FwIsVSX
0
[Expert@MyGW:0]#
```

Example - Checking if on this Security Gateway the QoS blade is enabled

```
[Expert@MyGW:0]# cpprod_util FwIsFloodGate
1
[Expert@MyGW:0]#
```

Example - Checking if on this Security Gateway the SmartProvisioning is enabled

```
[Expert@MyGW:0]# cpprod_util FwIsAtlasModule
0
[Expert@MyGW:0]#
```

Example - Checking if this Security Gateway is configured in Bridge Mode

```
[Expert@MyGW:0]# cpprod_util FwIsBridge
0
[Expert@MyGW:0]#
```

Example - Checking if this Security Gateway is a member of Full HA cluster

```
[Expert@MyGW:0]# cpprod_util FwIsFullHA
0
[Expert@MyGW:0]#
```

Example - Checking if this Security Gateway is configured with Dynamically Assigned IP (DAIP)

```
[Expert@MyGW:0]# cpprod_util FwIsDAG
0
[Expert@MyGW:0]#
```

Example - Checking if this Security Gateway is configured with IPv6 addresses

```
[Expert@MyGW:0]# cpprod_util FwIsFireWallIPv6
1
[Expert@MyGW:0]#
```

cpstart

Description

Manually starts all Check Point processes and applications.

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpstart
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpstart
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpstart
```

Log Files

- `$CPDIR/cpstart.log`
- `/opt/CPInstLog/cpstart_error.log`

cpstat

Description

Shows the status and statistics information for Check Point applications.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpstat [-d] [-h <Host>] [-p <Port>] [-s <SICname>] [-f <Flavor>]
[-o <Polling Interval> [-c <Count>] [-e <Period>]] <Application
Flag>
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpstat [-d] [-h <Host>] [-p <Port>] [-s <SICname>] [-f <Flavor>]
[-o <Polling Interval> [-c <Count>] [-e <Period>]] <Application
Flag>
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpstat [-d] [-h <Host>] [-p <Port>] [-s <SICname>] [-f <Flavor>]
[-o <Polling Interval> [-c <Count>] [-e <Period>]] <Application
Flag>
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpstat [-d] [-h <Host>] [-p <Port>] [-s <SICname>] [-f
<Flavor>] [-o <Polling Interval> [-c <Count>] [-e <Period>]]
<Application Flag>
```

Note - You can write the parameters in the syntax in any order.

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session. The output shows the SNMP queries and SNMP responses for the applicable SNMP OIDs.
`-h <Host>`	Optional. When you run this command on a Management Server, this parameter specifies the managed Security Gateway / ClusterXL object. *<Host>* is an IPv4 address, a resolvable hostname, or a DAIP object name. The default is `localhost`. **Note** - On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:`mdsenv <IP Address or Name of Domain Management Server>`.
`-p <Port>`	Optional. Port number of the Application Monitoring (AMON) server. The default port is 18192.
`-s <SICname>`	Optional. Secure Internal Communication (SIC) name of the Application Monitoring (AMON) server.
`-f <Flavor>`	Optional. Specifies the type of the information to collect. If you do not specify a flavor explicitly, the command uses the first flavor in the *<Application Flag>*. To see all flavors, run the `cpstat` command without any parameters.

Parameter	Description
`-o <Polling Interval>`	Optional. Specifies the polling interval (in seconds) - how frequently the command collects and shows the information. Examples: ■ 0 - The command shows the results only once and the stops (this is the default value). ■ 5 - The command shows the results every 5 seconds in the loop. ■ 30 - The command shows the results every 30 seconds in the loop. ■ N - The command shows the results every N seconds in the loop. Use this parameter together with the "`-c <Count>`" parameter and the "`-e <Period>`" parameter. Example: `cpstat os -f perf -o 2`
`-c <Count>`	Optional. Specifies how many times the command runs and shows the results before it stops. You must use this parameter together with the "`-o <Polling Interval>`" parameter. Examples: ■ 0 - The command shows the results repeatedly every <*Polling Interval*> (this is the default value). ■ 10 - The command shows the results 10 times every <*Polling Interval*> and then stops. ■ 20 - The command shows the results 20 times every <*Polling Interval*> and then stops. ■ N - The command shows the results N times every <*Polling Interval*> and then stops. Example: `cpstat os -f perf -o 2 -c 2`

Parameter	Description
`-e <Period>`	Optional. Specifies the time (in seconds), over which the command calculates the statistics. You must use this parameter together with the "`-o <Polling Interval>`" parameter. You can use this parameter together with the "`-c <Count>`" parameter. Example: `cpstat os -f perf -o 2 -c 2 -e 60`
`<Application Flag>`	Mandatory. See the table below with flavors for the application flags.

These flavors are available for the application flags

Note - The available flags depend on the enabled Software Blades. Some flags are supported only by a Security Gateway / ClusterXL, and some flags are supported only by a Management Server.

Feature or Software Blade	Flag	Flavors
List of enabled Software Blades	`blades`	`fw, ips, av, urlf, vpn, cvpn, aspm, dlp, appi, anti_bot, default, content_awareness, threat-emulation, default`
Operating System	`os`	`default, ifconfig, routing, routing6, memory, old_memory, cpu, disk, perf, multi_cpu, multi_disk, raidInfo, sensors, power_supply, hw_info, all, average_cpu, average_memory, statistics, updates, licensing, connectivity, vsx`
Firewall	`fw`	`default, interfaces, policy, perf, hmem, kmem, inspect, cookies, chains, fragments, totals, totals64, ufp, http, ftp, telnet, rlogin, smtp, pop3, sync, log_connection, all`

Feature or Software Blade	Flag	Flavors
HTTPS Inspection	`https_inspection`	`default, hsm_status, all`
Identity Awareness	`identityServer`	`default, authentication, logins, ldap, components, adquery, idc, muh`
Application Control	`appi`	`default, subscription_status, update_status, RAD_status, top_last_hour, top_last_day, top_last_week, top_last_month`
URL Filtering	`urlf`	`default, subscription_status, update_status, RAD_status, top_last_hour, top_last_day, top_last_week, top_last_month`
IPS	`ips`	`default, statistics, all`
Anti-Virus	`ci`	`default`
Threat Prevention	`antimalware`	`default, scanned_hosts, scanned_mails, subscription_status, update_status, ab_prm_contracts, av_prm_contracts, ab_prm_contracts, av_prm_contracts`

Feature or Software Blade	Flag	Flavors
Threat Emulation	`threat-emulation`	`default, general_statuses, update_status, scanned_files, malware_detected, scanned_on_cloud, malware_on_cloud, average_process_time, emulated_file_size, queue_size, peak_size, file_type_stat_file_scanned, file_type_stat_malware_detected, file_type_stat_cloud_scanned, file_type_stat_cloud_malware_scanned, file_type_stat_filter_by_analysis, file_type_stat_cache_hit_rate, file_type_stat_error_count, file_type_stat_no_resource_count, contract, downloads_information_current, downloading_file_information, queue_table, history_te_incidents, history_te_comp_hosts`
Threat Extraction	`scrub`	`default, subscription_status, threat_extraction_statistics`
Mobile Access	`cvpn`	`cvpnd, sysinfo, products, overall`
VSX	`vsx`	`default, stat, traffic, conns, cpu, all, memory, cpu_usage_per_core`
IPSec VPN	`vpn`	`default, product, IKE, ipsec, traffic, compression, accelerator, nic, statistics, watermarks, all`
Data Loss Prevention	`dlp`	`default, dlp, exchange_agents, fingerprint`
Content Awareness	`ctnt`	`default`
QoS	`fg`	`all`
High Availability	`ha`	`default, all`
Policy Server for Remote Access VPN clients	`polsrv`	`default, all`

Feature or Software Blade	Flag	Flavors
Desktop Policy Server for Remote Access VPN clients	`dtps`	`default, all`
LTE / GX	`gx`	`default, contxt_create_info, contxt_delete_info, contxt_update_info, contxt_path_mng_info, GXSA_GPDU_info, contxt_initiate_info, gtpv2_create_info, gtpv2_delete_info, gtpv2_update_info, gtpv2_path_mng_info, gtpv2_cmd_info, all`
Management Server	`mg`	`default, log_server, indexer`
Certificate Authority	`ca`	`default, crl, cert, user, all`
SmartEvent	`cpsemd`	`default`
SmartEvent Correlation Unit	`cpsead`	`default`
Log Server	`ls`	`default`
CloudGuard Controller	`vsec`	`default`
SmartReporter	`svr`	`default`
Provisioning Agent	`PA`	`default`
Thresholds configured with the "`threshold_config`" command	`thresholds`	`default, active_thresholds, destinations, error`
Historical status values	`persistency`	`product, TableConfig, SourceConfig`

Examples

Example - Interfaces on a Security Gateway

```
[Expert@MyGW:0]# cpstat -f interfaces fw

Network interfaces
-------------------------------------------------------------------------------------------------
-----------------------
|Name|IP           |Netmask      |Flags|Peer name|Remote IP|Topology|Proxy
name|Slaves|Ports|IPv6 Address|IPv6 Len|
-------------------------------------------------------------------------------------------------
-----------------------
|eth0|192.168.30.40|255.255.255.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
|eth1| 172.30.60.80|255.255.255.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
|eth2|      0.0.0.0|      0.0.0.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
|eth3|      0.0.0.0|      0.0.0.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
|eth4|      0.0.0.0|      0.0.0.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
|eth5|      0.0.0.0|      0.0.0.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
|eth6|      0.0.0.0|      0.0.0.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
|eth7|      0.0.0.0|      0.0.0.0|    0|         |  0.0.0.0|       4|          |      |     |
         ::|       0|
-------------------------------------------------------------------------------------------------
-----------------------

[Expert@MyGW:0]#
```

Example - Policy on a Security Gateway

```
[Expert@MyGW:0]# cpstat -f default fw

Policy name:  MyGW_Policy
Install time: Wed May 23 18:14:32 2018


Interface table
----------------------------------------
|Name|Dir|Total   |Accept|Deny    |Log|
----------------------------------------
|eth0|in | 2393126| 32589| 2360537| 52|
|eth0|out|   33016| 33016|       0|  0|
|eth1|in | 2360350|     0| 2360350|  0|
|eth1|out|       0|     0|       0|  0|
|eth2|in | 2360350|     0| 2360350|  0|
|eth2|out|       0|     0|       0|  0|
|eth3|in | 2348704|     0| 2348704|  1|
|eth3|out|       0|     0|       0|  0|
|eth4|in | 2360350|     0| 2360350|  0|
|eth4|out|       0|     0|       0|  0|
----------------------------------------
|    |   |11855896| 65605|11790291| 53|
----------------------------------------

... ... [truncated for brevity] ... ...

[Expert@MyGW:0]#
```

Example - CPU utilization

```
[Expert@HostName:0]# cpstat -f cpu os
CPU User Time (%):   1
CPU System Time (%): 0
CPU Idle Time (%):   99
CPU Usage (%):       1
CPU Queue Length:    -
CPU Interrupts/Sec:  172
CPUs Number:         8

[Expert@HostName:0]#
```

Example - Performance

```
[Expert@HostName:0]# cpstat os -f perf -o 2 -c 2 -e 60

Total Virtual Memory (Bytes):            12417720320
Active Virtual Memory (Bytes):           3741331456
Total Real Memory (Bytes):               8231063552
Active Real Memory (Bytes):              3741331456
Free Real Memory (Bytes):                4489732096
Memory Swaps/Sec:                        -
Memory To Disk Transfers/Sec:            -
CPU User Time (%):                       0
CPU System Time (%):                     0
CPU Idle Time (%):                       100
CPU Usage (%):                           0
CPU Queue Length:                        -
CPU Interrupts/Sec:                      135
CPUs Number:                             8
Disk Servicing Read\Write Requests Time: -
Disk Requests Queue:                     -
Disk Free Space (%):                     61
Disk Total Free Space (Bytes):           12659716096
Disk Available Free Space (Bytes):       11606188032
Disk Total Space (Bytes):                20477751296


Total Virtual Memory (Bytes):            12417720320
Active Virtual Memory (Bytes):           3741556736
Total Real Memory (Bytes):               8231063552
Active Real Memory (Bytes):              3741556736
Free Real Memory (Bytes):                4489506816
Memory Swaps/Sec:                        -
Memory To Disk Transfers/Sec:            -
CPU User Time (%):                       3
CPU System Time (%):                     0
CPU Idle Time (%):                       97
CPU Usage (%):                           3
CPU Queue Length:                        -
CPU Interrupts/Sec:                      140
CPUs Number:                             8
Disk Servicing Read\Write Requests Time: -
Disk Requests Queue:                     -
Disk Free Space (%):                     61
Disk Total Free Space (Bytes):           12659716096
Disk Available Free Space (Bytes):       11606188032
Disk Total Space (Bytes):                20477751296

[Expert@HostName:0]#
```

Example - List of current connected sessions on a Management Server

```
[Expert@MGMT:0]# cpstat -f default mg

Product Name:  Check Point Security Management Server
Major version: 6
Minor version: 0
Build number:  994000031
Is started:    1
Active status: active
Status:        OK

Connected clients
-----------------------------------------------------
|Client type |Administrator|Host        |Database lock|
-----------------------------------------------------
|SmartConsole|admin        |JOHNDOE-PC  |false        |
-----------------------------------------------------

[Expert@MGMT:0]#
```

cpstop

Description

Manually stops all Check Point processes and applications.

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpstop [-fwflag {-default | -proc | -driver}]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpstop [-fwflag {-default | -proc | -driver}]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpstop [-fwflag {-default | -proc | -driver}]
```

Parameters

Important - These parameters are for Check Point internal use. Do **not** use them, unless explicitly instructed by Check Point Support or R&D to do so.

Parameter	Description
`-fwflag -default`	■ Shuts down Check Point processes ■ Loads the Default Filter policy (`defaultfilter`)
`-fwflag -proc`	■ Shuts down Check Point processes ■ Keeps the currently loaded kernel policy ■ Maintains the Connections table, so that after you run the *"cpstart" on page 1018* command, you do not experience dropped packets because they are "out of state" **Note** - Only security rules that do not use user space processes continue to work.
`-fwflag -driver`	Unloads the Check Point kernel modules. Therefore, no policy is loaded. **Warning** - This leaves your Security Gateway, or aCluster Member without protection. Before you run this command, we recommend to disconnect your Security Gateway, or aCluster Member from the network completely.

dynamic_objects

Description

Manages dynamic objects and their applicable ranges of IP addresses on the Security Gateway / Cluster Members / Scalable Platform Security Group.

Important:

- You can run this command only in the Expert mode.
- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms (Maestro and Chassis), you must connect to the applicable Security Group.

Workflow

Step	Instructions
1	In SmartConsole: 1. Configure the applicable dynamic object. 2. Install the Access Control Policy on the Security Gateway / ClusterXL object.
2	On the Security Gateway / *each* Cluster Member / Security Group, run the "`dynamic_objects`" command to: 1. Create the applicable dynamic object with the same name 2. Assign the applicable ranges of IP address to the new dynamic object.

General syntax on a Security Gateway / Cluster Member in the Expert mode

```
dynamic_objects <Parameters>
```

General syntax on a Scalable Platform Security Group in the Expert mode

```
g_all dynamic_objects <Parameters>
```

Syntax for specific commands

- To show all configured dynamic objects and their ranges of IP addresses:

```
dynamic_objects -l
```

- To create a new dynamic object (and assign a range of IP addresses to it):

```
dynamic_objects -n <Object Name> [-r <FromIP1> <ToIP2> ...
[<FromIPx> <ToIPy>] -a]
```

- To add a new a range of IP addresses to the specific existing dynamic object:

```
dynamic_objects -o <Object Name> -r <FromIP1> <ToIP2> ...
[<FromIPx> <ToIPy>] -a
```

- To delete a range of IP addresses from the specific existing dynamic object:

```
dynamic_objects -o <Object Name> -r <FromIP1> <ToIP2> ...
[<FromIPx> <ToIPy>] -d
```

- To update the specific existing dynamic object (and assign a different range of IP addresses to it):

```
dynamic_objects -u <Object Name> [-r <FromIP1> <ToIP2> ...
[<FromIPx> <ToIPy>]]
```

- To compare the configured dynamic objects and objects configured in SmartConsole:

```
dynamic_objects -c
```

- To delete the specific existing dynamic object (and all ranges of IP addresses assigned to it):

```
dynamic_objects -do <Object Name>
```

- To delete all the existing dynamic objects (and all ranges of IP addresses assigned to them):

```
dynamic_objects -e
```

Parameters

Parameter	Description
<Object Name>	Specifies the name of the object: ■ As configured in SmartConsole ■ As configured with the "`dynamic_objects -n <object name>`" command

`-r <FromIP1> <ToIP2> ... [<FromIPx> <ToIPy>]`	Specifies the ranges of IP addresses in the format of pairs:
	`<From_IP_Address> <To_IP_Address>`
	For example, to specify two ranges, from 192.168.2.30 to 192.168.2.40 and from 192.168.2.50 to 192.168.2.60, enter these four IP addresses:
	`192.168.2.30 192.168.2.40 192.168.2.50 192.168.2.60`

`-a`	Adds the specified ranges of IP addresses to the specified dynamic object.
`-c`	Compare the dynamic objects in the dynamic objects database (`$FWDIR/database/dynamic_objects.db`) and in the `$FWDIR/conf/objects.C` file.
`-d`	Deletes range of IP addresses from the dynamic object.
`-do`	Deletes the specified dynamic object.
`-e`	Deletes all configured dynamic objects from the dynamic objects database (`$FWDIR/database/dynamic_objects.db`).
`-l`	Lists the configured dynamic objects in the dynamic objects database (`$FWDIR/database/dynamic_objects.db`).
`-n`	Creates a new dynamic object.
`-u`	Updates the specified dynamic object. If you specify a range of IP addresses, then the new range replaces all current ranges that are currently assigned to this dynamic object.

Example 1 - Create a new dynamic object named "bigserver" and assign to it the range of IP addresses 192.168.2.30-192.168.2.40

Run either these two commands:

```
dynamic_objects -n bigserver
```

```
dynamic_objects -o bigserver -r 192.168.2.30 192.168.2.40 -a
```

Or this single command:

```
dynamic_objects -n bigserver -r 192.168.2.20 192.168.2.40 -a
```

Example 2 - Update the ranges of IP addresses assigned to the dynamic object named "bigserver" from the current range to the new range 192.168.2.60-192.168.2.80

```
dynamic_objects -u bigserver -r 192.168.2.60 192.168.2.80
```

cpwd_admin

Description

The Check Point WatchDog (`cpwd`) is a process that invokes and monitors critical processes such as Check Point daemons on the local server, and attempts to restart them if they fail.

Among the processes monitored by Watchdog are `fwm`, `fwd`, `cpd`, `DAService`, and others.

The list of monitored processes depends on the installed and configured Check Point products and Software Blades.

The Check Point WatchDog writes monitoring information to the `$CPDIR/log/cpwd.elg` log file.

The `cpwd_admin` utility shows the status of the monitored processes, and configures the Check Point WatchDog.

There are two types of Check Point WatchDog monitoring

Monitoring	Description
Passive	WatchDog restarts the process only when the process terminates abnormally. In the output of the `cpwd_admin list` command, the `MON` column shows `N` for passively monitored processes.
Active	WatchDog checks the process status every predefined interval. WatchDog makes sure the process is alive, as well as properly functioning (not stuck on deadlocks, frozen, and so on). In the output of the `cpwd_admin list` command, the `MON` column shows `Y` for actively monitored processes. The list of actively monitored processes is predefined by Check Point. Users cannot change or configure it.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin
      config <options>
      del <options>
      detach <options>
      exist
      flist <options>
      getpid <options>
      kill
      list <options>
      monitor_list
      start <options>
      start_monitor
      stop <options>
      stop_monitor
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin
      config <options>
      del <options>
      detach <options>
      exist
      flist <options>
      getpid <options>
      kill
      list <options>
      monitor_list
      start <options>
      start_monitor
      stop <options>
      stop_monitor
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin
      config <options>
      del <options>
      detach <options>
      exist
      flist <options>
      getpid <options>
      kill
      list <options>
      monitor_list
      start <options>
      start_monitor
      stop <options>
      stop_monitor
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin
      config <options>
      del <options>
      detach <options>
      exist
      flist <options>
      getpid <options>
      kill
      list <options>
      monitor_list
      start <options>
      start_monitor
      stop <options>
      stop_monitor
```

Parameters

Parameter	Description
`config <options>`	Configures the Check Point WatchDog. See *"cpwd_admin config" on page 224*.

Parameter	Description
`del <options>`	Temporarily deletes a monitored process from the WatchDog database of monitored processes. See *"cpwd_admin del" on page 229*.
`detach <options>`	Temporarily detaches a monitored process from the WatchDog monitoring. See *"cpwd_admin detach" on page 231*.
`exist`	Checks whether the WatchDog process `cpwd` is alive. See *"cpwd_admin exist" on page 233*.
`flist <options>`	Saves the status of all monitored processes to a `$CPDIR/tmp/cpwd_list_<Epoch Timestamp>.lst` file. See *"cpwd_admin flist" on page 234*.
`getpid <options>`	Shows the PID of a monitored process. See *"cpwd_admin getpid" on page 236*.
`kill <options>`	Terminates the WatchDog process `cpwd`. See *"cpwd_admin kill" on page 237*. **Important** - Do **not** run this command unless explicitly instructed by Check Point Support or R&D to do so.
`list`	Prints the status of all monitored processes on the screen. See *"cpwd_admin list" on page 238*.
`monitor_list`	Prints the status of actively monitored processes on the screen. See *"cpwd_admin monitor_list" on page 243*.
`start <options>`	Starts a process as monitored by the WatchDog. See *"cpwd_admin start" on page 244*.
`start_monitor`	Starts the active WatchDog monitoring - WatchDog monitors the predefined processes actively. See *"cpwd_admin start_monitor" on page 247*.
`stop <options>`	Stops a monitored process. See *"cpwd_admin stop" on page 248*.
`stop_monitor`	Stops the active WatchDog monitoring - WatchDog monitors all processes only passively. See *"cpwd_admin stop_monitor" on page 250*.

cpwd_admin config

Description

Configures the Check Point WatchDog.

Important - After changing the WatchDog configuration parameters, you must restart the WatchDog process with the "`cpstop`" and "`cpstart`" commands (which restart *all* Check Point processes).

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin config
      -h
      -a <options>
      -d <options
      -p
      -r
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin config
      -h
      -a <options>
      -d <options
      -p
      -r
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin config
      -h
      -a <options>
      -d <options
      -p
      -r
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin config
      -h
      -a <options>
      -d <options
      -p
      -r
```

Parameters

Parameter	Description
`-h`	Shows built-in usage.
`-a <Configuration_Parameter_1>=<Value_1> <Configuration_Parameter_2>=<Value_2> ... <Configuration_Parameter_N>=<Value_N>`	Adds the WatchDog configuration parameters. **Note** - Spaces are not allowed between the name of the configuration parameter, the equal sign, and the value.
`-d <Configuration_Parameter_1> <Configuration_Parameter_2> ... <Configuration_Parameter_N>`	Deletes the WatchDog configuration parameters that user added with the "`cpwd_admin config -a`" command.
`-p`	Shows the WatchDog configuration parameters that user added with the "`cpwd_admin config -a`" command.
`-r`	Restores the default WatchDog configuration.

These are the available configuration parameters and the accepted values:

Configuration Parameter	Accepted Values	Description
`default_ctx`	Text string up to 128 characters	On a VSX Gateway, configures the CTX value that is assigned to monitored processes, for which no CTX is specified.
`display_ctx`	■ 0 (default) ■ 1	On a VSX Gateway, configures whether the WatchDog shows the `CTX` column in the output of the `cpwd_admin list` command (between the `APP` and the `PID` columns): ■ 0 - Does not show the `CTX` column ■ 1 - Shows the `CTX` column

Configuration Parameter	Accepted Values	Description
`no_limit`	■ Range: -1, 0, >0 ■ Default: 5	If `rerun_mode=1`, specifies the maximal number of times the WatchDog tries to restart a process. ■ -1 - Always tries to restart ■ 0 - Never tries to restart ■ >0 - Tries this number of times
`num_of_procs`	■ Range: 30 - 3000 ■ Default: 3000	Configures the maximal number of processes managed by the WatchDog.
`rerun_mode`	■ 0 ■ 1 (default)	Configures whether the WatchDog restarts processes after they fail: ■ 0 - Does not restart a failed process. Monitor and log only. ■ 1 - Restarts a failed process (this is the default).
`reset_ startups`	■ Range: > 0 ■ Default: 3600	Configures the time (in seconds) the WatchDog waits after the process starts and before the WatchDog resets the process's `startup_counter` to 0. To see the process's startup counter, in the output of the `cpwd_admin list` command, refer to the `#START` column.
`sleep_mode`	■ 0 ■ 1 (default)	Configures how the WatchDog restarts the process: ■ 0 - Ignores timeout and restarts the process immediately ■ 1 - Waits for the duration of `sleep_timeout`
`sleep_ timeout`	■ Range: 0 - 3600 ■ Default: 60	If `rerun_mode=1`, specifies how much time (in seconds) passes from a process failure until WatchDog tries to restart it.
`stop_timeout`	■ Range: > 0 ■ Default: 60	Configures the time (in seconds) the WatchDog waits for a process stop command to complete.

Configuration Parameter	Accepted Values	Description
`zero_timeout`	■ Range: > 0 ■ Default: 7200	After failing `no_limit` times to restart a process, the WatchDog waits `zero_timeout` seconds before it tries again. The value of the `zero_timeout` must be greater than the value of the `timeout`.

The WatchDog saves the user defined configuration parameters in the `$CPDIR/registry/HKLM_registry.data` file in the "`: (Wd_Config`" section:

```
("CheckPoint Repository Set"
  : (SOFTWARE
    : (CheckPoint
      : (CPshared
        :CurrentVersion (6.0)
        : (6.0
        ... ...
          : (reserved
          ... ...
            : (Wd
                : (Wd_Config
                    :Configuration_Parameter_1 ("[4]Value_1")
                    :Configuration_Parameter_2 ("[4]Value_2")
                )
            )
          ... ...
```

Example

```
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -a sleep_timeout=120 no_limit=12
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog Configuration parameters are:
sleep_timeout : 120
no_limit : 12
[Expert@HostName:0]#
[Expert@HostName:0]# cpstop ; cpstart
[Expert@HostName:0]#

[Expert@HostName:0]# cpwd_admin config -r
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
[Expert@HostName:0]# cpstop ; cpstart
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
```

Description

Configures the Check Point WatchDog.

Important - After changing the WatchDog configuration parameters, you must restart the WatchDog process with the `cpstop` and cpstart commands (which restart *all* Check Point processes).

Syntax

```
cpwd_admin config
      -h
      -a <options>
      -d <options
      -p
      -r
```

Parameters

Parameter	Description
`-h`	Shows built-in usage.
`-a <Configuration_Parameter_1>=<Value_1> <Configuration_Parameter_2>=<Value_2> ... <Configuration_Parameter_N>=<Value_N>`	Adds the WatchDog configuration parameters. **Note** - Spaces are not allowed between the name of the configuration parameter, the equal sign, and the value.
`-d <Configuration_Parameter_1> <Configuration_Parameter_2> ... <Configuration_Parameter_N>`	Deletes the WatchDog configuration parameters that user added with the `cpwd_admin config -a` command.
`-p`	Shows the WatchDog configuration parameters that user added with the `cpwd_admin config -a` command.
`-r`	Restores the default WatchDog configuration.

These are the available configuration parameters and the accepted values:

Configuration Parameter	Accepted Values	Description
`default_ctx`	Text string up to 128 characters	On a VSX Gateway, configures the CTX value that is assigned to monitored processes, for which no CTX is specified.
`display_ctx`	■ 0 (default) ■ 1	On a VSX Gateway, configures whether the WatchDog shows the `CTX` column in the output of the `cpwd_admin list` command (between the `APP` and the `PID` columns): ■ 0 - Does not show the `CTX` column ■ 1 - Shows the `CTX` column
`no_limit`	■ Range: -1, 0, >0 ■ Default: 5	If `rerun_mode=1`, specifies the maximal number of times the WatchDog tries to restart a process. ■ -1 - Always tries to restart ■ 0 - Never tries to restart ■ >0 - Tries this number of times
`num_of_procs`	■ Range: 30 - 2000 ■ Default: 2000	Configures the maximal number of processes managed by the WatchDog.
`rerun_mode`	■ 0 ■ 1 (default)	Configures whether the WatchDog restarts processes after they fail: ■ 0 - Does not restart a failed process. Monitor and log only. ■ 1 - Restarts a failed process (this is the default).
`reset_ startups`	■ Range: > 0 ■ Default: 3600	Configures the time (in seconds) the WatchDog waits after the process starts and before the WatchDog resets the process's `startup_counter` to 0. To see the process's startup counter, in the output of the `cpwd_admin list` command, refer to the `#START` column.
`sleep_mode`	■ 0 ■ 1 (default)	Configures how the WatchDog restarts the process: ■ 0 - Ignores timeout and restarts the process immediately ■ 1 - Waits for the duration of `sleep_timeout`

Configuration Parameter	Accepted Values	Description
`sleep_timeout`	■ Range: 0 - 3600 ■ Default: 60	If `rerun_mode=1`, specifies how much time (in seconds) passes from a process failure until WatchDog tries to restart it.
`stop_timeout`	■ Range: > 0 ■ Default: 60	Configures the time (in seconds) the WatchDog waits for a process stop command to complete.
`zero_timeout`	■ Range: > 0 ■ Default: 7200	After failing `no_limit` times to restart a process, the WatchDog waits `zero_timeout` seconds before it tries again. The value of the `zero_timeout` must be greater than the value of the `timeout`.

The WatchDog saves the user defined configuration parameters in the `$CPDIR/registry/HKLM_registry.data` file in the "`: (Wd_Config`" section:

```
("CheckPoint Repository Set"
  : (SOFTWARE
    : (CheckPoint
      : (CPshared
        :CurrentVersion (6.0)
        : (6.0
        ... ...
          : (reserved
          ... ...
            : (Wd
                : (Wd_Config
                    :Configuration_Parameter_1 ("[4]Value_1")
                    :Configuration_Parameter_2 ("[4]Value_2")
                )
            )
          ... ...
```

Example

```
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -a sleep_timeout=120 no_limit=12
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog Configuration parameters are:
sleep_timeout : 120
no_limit : 12
[Expert@HostName:0]#
[Expert@HostName:0]# cpstop ; cpstart
[Expert@HostName:0]#

[Expert@HostName:0]# cpwd_admin config -r
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
[Expert@HostName:0]# cpstop ; cpstart
[Expert@HostName:0]#
[Expert@HostName:0]# cpwd_admin config -p
cpWatchDog doesn't have configuration parameters
[Expert@HostName:0]#
```

cpwd_admin del

Description

Temporarily deletes a monitored process from the WatchDog database of monitored processes.

Notes:

- WatchDog stops monitoring the detached process, but the process stays alive.
- The *"cpwd_admin list" on page 238* command does not show the deleted process anymore.
- This change applies until all Check Point services restart during boot, or with the *"cpstart" on page 208* command.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin del -name <Application Name>
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin del -name <Application Name> [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin del -name <Application Name> [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin del -name <Application Name> [-ctx <VSID>]
```

Parameters

Parameter	Description
<Application Name>	Name of the monitored Check Point process as you see in the output of the *"cpwd_admin list" on page 238* command in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`
`-ctx <VSID>`	On a VSX Gateway, specifies the context of the applicable Virtual System.

Example

```
[Expert@HostName:0]# cpwd_admin del -name FWD
cpwd_admin:
successful Del operation
[Expert@HostName:0]#
```

cpwd_admin detach

Description

Temporarily detaches a monitored process from the WatchDog monitoring.

Notes:

- WatchDog stops monitoring the detached process, but the process stays alive.
- The *"cpwd_admin list" on page 238* command does not show the detached process anymore.
- This change applies until all Check Point services restart during boot, or with the *"cpstart" on page 208* command.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin detach -name <Application Name>
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin detach -name <Application Name> [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin detach -name <Application Name> [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin detach -name <Application Name> [-ctx <VSID>]
```

Parameters

Parameter	Description
<Application Name>	Name of the monitored Check Point process as you see in the output of the *"cpwd_admin list" on page 238* command in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`
`-ctx <VSID>`	On a VSX Gateway, specifies the context of the applicable Virtual System.

Example

```
[Expert@HostName:0]# cpwd_admin detach -name FWD
cpwd_admin:
successful Detach operation
[Expert@HostName:0]#
```

cpwd_admin exist

Description

Checks whether the WatchDog process `cpwd` is alive.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin exist
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin exist
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin exist
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin exist
```

Example

```
[Expert@HostName:0]# cpwd_admin exist
 cpwd_admin: cpWatchDog is running
[Expert@HostName:0]#
```

cpwd_admin flist

Description

Saves the status of all WatchDog monitored processes to a file.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin flist [-full]
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin flist [-full] [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin flist [-full] [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin flist [-full] [-ctx <VSID>]
```

Parameters

Parameter	Description
`-full`	Shows the verbose output.
`-ctx <VSID>`	On a VSX Gateway, specifies the context of the applicable Virtual System.

Output

Column	Description
APP	Shows the WatchDog name of the monitored process.
CTX	On a VSX Gateway, shows the VSID, in which the monitored process runs.
PID	Shows the PID of the monitored process.
STAT	Shows the status of the monitored process: ■ E - executing ■ T - terminated
#START	Shows how many times the WatchDog started the monitored process.
START_TIME	Shows the time when the WatchDog started the monitored process for the last time.
SLP/LIMIT	In verbose output, shows the values of the sleep_timeout and no_limit configuration parameters (see *"cpwd_admin config" on page 224*).
MON	Shows how the WatchDog monitors this process (see the explanation for the *"cpwd_admin" on page 220*): ■ Y - Active monitoring ■ N - Passive monitoring
COMMAND	Shows the command the WatchDog run to start this process.

Example

```
[Expert@HostName:0]# cpwd_admin flist
/opt/CPshrd-R81.20/tmp/cpwd_list_1564617600.lst
[Expert@HostName:0]#
```

cpwd_admin getpid

Description

Shows the PID of a WatchDog monitored process.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin getpid -name <Application Name>
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin getpid -name <Application Name> [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin getpid -name <Application Name> [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin getpid -name <Application Name> [-ctx <VSID>]
```

Parameters

Parameter	Description
<Application Name>	Name of the monitored Check Point process as you see in the output of the *"cpwd_admin list" on page 238* command in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`
`-ctx <VSID>`	On VSX Gateway, specifies the context of the applicable Virtual System.

Example

```
[Expert@HostName:0]# cpwd_admin getpid -name FWD
5640
[Expert@HostName:0]#
```

cpwd_admin kill

Description

Terminates the WatchDog process `cpwd`.

Important - Do **not** run this command unless explicitly instructed by Check Point Support or R&D to do so.
To restart the WatchDog process, you must restart all Check Point services with the *"cpstop" on page 219* and *"cpstart" on page 208* commands.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin kill
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin kill
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin kill
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin kill
```

cpwd_admin list

Description

Prints the status of all WatchDog monitored processes on the screen.

Note - By default, WatchDog monitors a maximum of 3000 processes.
To increase this threshold, use the command "`cpwd_admin config -a num_of_procs=<value>`".
See *"cpwd_admin config" on page 224*.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin list [-full]
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin list [-full] [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin list [-full] [-ctx <VSID>]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin list [-full] [-ctx <VSID>]
```

Parameters

Parameter	Description
`-full`	Shows the verbose output.
`-ctx <VSID>`	On a VSX Gateway, specifies the context of the applicable Virtual System.

Output

Column	Description
APP	Shows the WatchDog name of the monitored process.
CTX	On a VSX Gateway, shows the VSID, in which the monitored process runs.
PID	Shows the PID of the monitored process.
STAT	Shows the status of the monitored process: ■ E - executing ■ T - terminated
#START	Shows how many times the WatchDog started the monitored process.
START_TIME	Shows the time when the WatchDog started the monitored process for the last time.
SLP/LIMIT	In verbose output, shows the values of the sleep_timeout and no_limit configuration parameters (see "cpwd_admin config" on page 224).
MON	Shows how the WatchDog monitors this process (see the explanation for the "cpwd_admin" on page 220): ■ Y - Active monitoring ■ N - Passive monitoring
COMMAND	Shows the command the WatchDog run to start this process.

Examples

Example - Default output on a Management Server

```
[Expert@HostName:0]# cpwd_admin list
APP         PID    STAT  #START  START_TIME             MON  COMMAND
CPVIEWD     19738  E     1       [17:50:44] 31/5/2019   N    cpviewd
HISTORYD    0      T     0       [17:54:44] 31/5/2019   N    cpview_historyd
CPD         19730  E     1       [17:54:45] 31/5/2019   Y    cpd
SOLR        19935  E     1       [17:50:55] 31/5/2019   N    java_solr /opt/CPrt-
R81.20/conf/jetty.xml
RFL         19951  E     1       [17:50:55] 31/5/2019   N    LogCore
SMARTVIEW   19979  E     1       [17:50:55] 31/5/2019   N    SmartView
INDEXER     20032  E     1       [17:50:55] 31/5/2019   N    /opt/CPrt-R81.20/log_indexer/log_
indexer
SMARTLOG_SERVER 20100  E     1       [17:50:55] 31/5/2019   N    /opt/CPSmartLog-
R81.20/smartlog_server
CP3DLOGD    20237  E     1       [17:50:55] 31/5/2019   N    cp3dlogd
EPM         20251  E     1       [17:50:56] 31/5/2019   N    startEngine
DASERVICE   20404  E     1       [17:50:59] 31/5/2019   N    DAService_script
[Expert@HostName:0]#
```

Example - Default output on a Security Gateway

```
[Expert@HostName:0]# cpwd_admin list
APP         CTX         PID    STAT  #START  START_TIME             MON  COMMAND
FWK_FORKER  0           4180   E     1       [18:14:04] 23/5/2019   N    fwk_forker
FWK_WD      0           4182   E     1       [18:14:04] 23/5/2019   N    fwk_wd -i 1 -i6 0
CPSICDEMUX  0           5383   E     1       [18:14:14] 23/5/2019   N    cpsicdemux
CPVIEWD     0           5407   E     1       [18:14:15] 23/5/2019   N    cpviewd
HISTORYD    0           5410   E     1       [18:14:15] 23/5/2019   N    cpview_historyd
SXL_STATD   0           5413   E     1       [18:14:15] 23/5/2019   N    sxl_statd
CPD         0           5420   E     1       [18:14:15] 23/5/2019   Y    cpd
MPDAEMON    0           5436   E     1       [18:14:16] 23/5/2019   N    mpdaemon /opt/CPshrd-
R81.20/log/mpdaemon.elg /opt/CPshrd-R81.20/conf/mpdaemon.conf
CI_CLEANUP  0           5626   E     1       [18:14:26] 23/5/2019   N    avi_del_tmp_files
CIHS        0           5628   E     1       [18:14:26] 23/5/2019   N    ci_http_server -j -f
/opt/CPsuite-R81.20/fw1/conf/cihs.conf
FWD         0           5640   E     1       [18:14:26] 23/5/2019   N    fwd
RAD         0           6330   E     1       [18:14:28] 23/5/2019   N    rad
DASERVICE   0           8604   E     1       [18:14:43] 23/5/2019   N    DAService_script
[Expert@HostName:0]#
```

Example - Verbose output on a Management Server

```
[Expert@HostName:0]# cpwd_admin list -full
APP         PID    STAT  #START  START_TIME             SLP/LIMIT  MON
-------------------------------------------------------------------------------
CPVIEWD     19738  E     1       [17:50:44] 31/5/2019   60/5       N
            PATH = /opt/CPshrd-R81.20/bin/cpviewd
            COMMAND = cpviewd
-------------------------------------------------------------------------------
HISTORYD    0      T     0       [17:54:44] 31/5/2019   60/5       N
            PATH = /opt/CPshrd-R81.20/bin/cpview_historyd
            COMMAND = cpview_historyd
-------------------------------------------------------------------------------
CPD         19730  E     1       [17:54:45] 31/5/2019   60/5       Y
            PATH = /opt/CPshrd-R81.20/bin/cpd
            COMMAND = cpd
-------------------------------------------------------------------------------
SOLR        19935  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPrt-R81.20/bin/java_solr
            COMMAND = java_solr /opt/CPrt-R81.20/conf/jetty.xml
-------------------------------------------------------------------------------
RFL         19951  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPrt-R81.20/bin/LogCore
            COMMAND = LogCore
-------------------------------------------------------------------------------
SMARTVIEW   19979  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPrt-R81.20/bin/SmartView
            COMMAND = SmartView
-------------------------------------------------------------------------------
INDEXER     20032  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPrt-R81.20/log_indexer/log_indexer
            COMMAND = /opt/CPrt-R81.20/log_indexer/log_indexer
-------------------------------------------------------------------------------
SMARTLOG_SERVER 20100  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPSmartLog-R81.20/smartlog_server
            COMMAND = /opt/CPSmartLog-R81.20/smartlog_server
            ENV = LANG=C
-------------------------------------------------------------------------------
CP3DLOGD    20237  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPuepm-R81.20/bin/cp3dlogd
            COMMAND = cp3dlogd
-------------------------------------------------------------------------------
EPM         20251  E     1       [17:50:56] 31/5/2019   60/5       N
            PATH = /opt/CPuepm-R81.20/bin/startEngine
            COMMAND = startEngine
-------------------------------------------------------------------------------
DASERVICE   20404  E     1       [17:50:59] 31/5/2019   60/5       N
            PATH = /opt/CPda/bin/DAService_script
            COMMAND = DAService_script
[Expert@HostName:0]#
```

Example - Verbose output on a Security Gateway

```
[Expert@HostName:0]# cpwd_admin list -full
APP         CTX        PID    STAT  #START  START_TIME             SLP/LIMIT  MON
-------------------------------------------------------------------------------
FWK_FORKER 0           4180   E     1       [18:14:04] 23/5/2019   60/5       N
                       PATH = /opt/CPsuite-R81.20/fw1/bin/fwk_forker
                       COMMAND = fwk_forker
-------------------------------------------------------------------------------
FWK_WD     0           4182   E     1       [18:14:04] 23/5/2019   3/u        N
                       PATH = /opt/CPsuite-R81.20/fw1/bin/fwk_wd
                       COMMAND = fwk_wd -i 1 -i6 0
-------------------------------------------------------------------------------
CPSICDEMUX 0           5383   E     1       [18:14:14] 23/5/2019   60/5       N
                       PATH = /opt/CPshrd-R81.20/bin/cpsicdemux
                       COMMAND = cpsicdemux
-------------------------------------------------------------------------------
CPVIEWD    0           5407   E     1       [18:14:15] 23/5/2019   60/5       N
                       PATH = /opt/CPshrd-R81.20/bin/cpviewd
                       COMMAND = cpviewd
-------------------------------------------------------------------------------
HISTORYD   0           5410   E     1       [18:14:15] 23/5/2019   60/5       N
                       PATH = /opt/CPshrd-R81.20/bin/cpview_historyd
                       COMMAND = cpview_historyd
-------------------------------------------------------------------------------
SXL_STATD  0           5413   E     1       [18:14:15] 23/5/2019   60/5       N
                       PATH = /opt/CPsuite-R81.20/fw1/bin/sxl_statd
                       COMMAND = sxl_statd
-------------------------------------------------------------------------------
CPD        0           5420   E     1       [18:14:15] 23/5/2019   60/5       Y
                       PATH = /opt/CPshrd-R81.20/bin/cpd
                       COMMAND = cpd
-------------------------------------------------------------------------------
MPDAEMON   0           5436   E     1       [18:14:16] 23/5/2019   60/5       N
                       PATH = /opt/CPshrd-R81.20/bin/mpdaemon
                       COMMAND = mpdaemon /opt/CPshrd-R81.20/log/mpdaemon.elg /opt/CPshrd-
R81.20/conf/mpdaemon.conf
-------------------------------------------------------------------------------
CI_CLEANUP 0           5626   E     1       [18:14:26] 23/5/2019   60/5       N
                       PATH = /opt/CPsuite-R81.20/fw1/bin/avi_del_tmp_files
                       COMMAND = avi_del_tmp_files
-------------------------------------------------------------------------------
CIHS       0           5628   E     1       [18:14:26] 23/5/2019   60/5       N
                       PATH = /opt/CPsuite-R81.20/fw1/bin/ci_http_server
                       COMMAND = ci_http_server -j -f /opt/CPsuite-R81.20/fw1/conf/cihs.conf
-------------------------------------------------------------------------------
FWD        0           5640   E     1       [18:14:26] 23/5/2019   60/5       N
                       PATH = /opt/CPsuite-R81.20/fw1/bin/fw
                       COMMAND = fwd
-------------------------------------------------------------------------------
RAD        0           6330   E     1       [18:14:28] 23/5/2019   60/5       N
                       PATH = /opt/CPsuite-R81.20/fw1///bin/rad
                       COMMAND = rad
-------------------------------------------------------------------------------
DASERVICE  0           8604   E     1       [18:14:43] 23/5/2019   60/5       N
                       PATH = /opt/CPda/bin/DAService_script
                       COMMAND = DAService_script
[Expert@HostName:0]#
```

cpwd_admin monitor_list

Description

Prints the status of actively monitored processes on the screen.

See the explanation about the active monitoring in *"cpwd_admin" on page 220*.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin monitor_list
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin monitor_list
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin monitor_list
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin monitor_list
```

Example

```
[Expert@HostName:0]# cpwd_admin monitor_list
cpwd_admin:
APP        FILE_NAME                      NO_MSG_TIMES   LAST_MSG_TIME
CPD        CPD_5420_4714.mntr             0/10           [19:00:33] 31/5/2019
[Expert@HostName:0]#
```

cpwd_admin start

Description

Starts a process as monitored by the WatchDog.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin start -name <Application Name> -path "<Full Path to
Executable>" -command "<Command Syntax>" [-env {inherit | <Env_
Var>=<Value>] [-slp_timeout <Timeout>] [-retry_limit {<Limit> |
u}]
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin start -name <Application Name> [-ctx <VSID>] -path
"<Full Path to Executable>" -command "<Command Syntax>" [-env
{inherit | <Env_Var>=<Value>] [-slp_timeout <Timeout>] [-retry_
limit {<Limit> | u}]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin start -name <Application Name> [-ctx <VSID>] -path
"<Full Path to Executable>" -command "<Command Syntax>" [-env
{inherit | <Env_Var>=<Value>] [-slp_timeout <Timeout>] [-retry_
limit {<Limit> | u}]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin start -name <Application Name> [-ctx <VSID>] -
path "<Full Path to Executable>" -command "<Command Syntax>" [-env
{inherit | <Env_Var>=<Value>] [-slp_timeout <Timeout>] [-retry_
limit {<Limit> | u}]
```

Parameters

Parameter	Description
`-name <Application Name>`	Name, under which the `cpwd_admin list` command shows the monitored process in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`
`-ctx <VSID>`	On a VSX Gateway, specifies the context of the applicable Virtual System.
`-path "<Full Path to Executable>"`	The full path (with or without Check Point environment variables) to the executable including the executable name. Must enclose in double quotes. Examples: ■ For FWM: "`$FWDIR/bin/fwm`" ■ For FWD: "`/opt/CPsuite-R81.20/fw1/bin/fw`" ■ For CPD: "`$CPDIR/bin/cpd`" ■ For CPM: "`/opt/CPsuite-R81.20/fw1/scripts/cpm.sh`" ■ For SICTUNNEL: "`/opt/CPshrd-R81.20/bin/cptnl`"
`-command "<Command Syntax>"`	The command and its arguments to run. Must enclose in double quotes. Examples: ■ For FWM: "`fwm`" ■ For FWM on Multi-Domain Server: "`fwm mds`" ■ For FWD: "`fwd`" ■ For CPD: "`cpd`" ■ For CPM: "`/opt/CPsuite-R81.20/fw1/scripts/cpm.sh -s`" ■ For SICTUNNEL: "`/opt/CPshrd-R81.20/bin/cptnl -c "/opt/CPuepm-R81.20/engine/conf/cptnl_srv.conf"`"

Parameter	Description
`-env {inherit | <Env_ Var>=<Value>}`	Configures whether to inherit the environment variables from the shell. ■ `inherit` - Inherits all the environment variables (WatchDog supports up to 80 environment variables) ■ *<Env_Var>=<Value>* - Assigns the specified value to the specified environment variable
`-slp_timeout <Timeout>`	Configures the specified value of the "`sleep_timeout`" configuration parameter. See *"cpwd_admin config" on page 224*.
`-retry_limit {<Limit> | u}`	Configures the value of the "`retry_limit`" configuration parameter. See *"cpwd_admin config" on page 224*. ■ *<Limit>* - Tries to restart the process the specified number of times ■ `u` - Tries to restart the process unlimited number of times

Example

For the list of process and the applicable syntax, see sk97638.

cpwd_admin start_monitor

Description

Starts the active WatchDog monitoring. WatchDog monitors the predefined processes actively.

See the explanation for the *"cpwd_admin" on page 220* command.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin start_monitor
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin start_monitor
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin start_monitor
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin start_monitor
```

Example

```
[Expert@HostName:0]# cpwd_admin start_monitor
cpwd_admin:
CPWD has started to perform active monitoring on Check Point services/processes
[Expert@HostName:0]#
```

cpwd_admin stop

Description

Stops a WatchDog monitored process.

Important - This change does **not** survive reboot.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin stop -name <Application Name> [-path "<Full Path to
Executable>" -command "<Command Syntax>" [-env {inherit | <Env_
Var>=<Value>]
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin stop -name <Application Name> [-ctx <VSID>] [-path
"<Full Path to Executable>" -command "<Command Syntax>" [-env
{inherit | <Env_Var>=<Value>]
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin stop -name <Application Name> [-ctx <VSID>] [-path
"<Full Path to Executable>" -command "<Command Syntax>" [-env
{inherit | <Env_Var>=<Value>]
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin stop -name <Application Name> [-ctx <VSID>] [-
path "<Full Path to Executable>" -command "<Command Syntax>" [-env
{inherit | <Env_Var>=<Value>]
```

Parameters

Parameter	Description
`-name <Application Name>`	Name under which the `cpwd_admin list` command shows the monitored process in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`
`-ctx <VSID>`	On a VSX Gateway, specifies the context of the applicable Virtual System.
`-path "<Full Path to Executable>"`	The full path (with or without Check Point environment variables) to the executable including the executable name. Must enclose in double quotes. Examples: ■ For FWM: "`$FWDIR/bin/fwm`" ■ For FWD: "`/opt/CPsuite-R81.20/fw1/bin/fw`" ■ For CPD: "`$CPDIR/bin/cpd_admin`"
`-command "<Command Syntax>"`	The command and its arguments to run. Must enclose in double quotes. Examples: ■ For FWM: "`fw kill fwm`" ■ For FWD: "`fw kill fwd`" ■ For CPD: "`cpd_admin stop`"
`-env {inherit | <Env_Var>=<Value>}`	Configures whether to inherit the environment variables from the shell. ■ `inherit` - Inherits all the environment variables (WatchDog supports up to 80 environment variables) ■ `<Env_Var>=<Value>` - Assigns the specified value to the specified environment variable

Example

For the list of process and the applicable syntax, see sk97638.

cpwd_admin stop_monitor

Description

Stops the active WatchDog monitoring. WatchDog monitors all processes only passively.

See the explanation for the *"cpwd_admin" on page 220* command.

Syntax on a Management Server in Gaia Clish or the Expert mode

```
cpwd_admin stop_monitor
```

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpwd_admin stop_monitor
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
cpwd_admin stop_monitor
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all cpwd_admin stop_monitor
```

Example

```
[Expert@HostName:0]# cpwd_admin stop_monitor
cpwd_admin:
CPWD has stopped performing active monitoring on Check Point services/processes
[Expert@HostName:0]#
```

fw

Description

- Fetches and unloads Threat Prevention policy.
- Controls the Firewall module.
- Generates the Default Filter policy files.
- Fetches the policy from the Management Server, peer Cluster Member, or local directory.
- Fetches the specified Security or Audit log files from the specified Check Point server.
- Shows the list of interfaces and their IP addresses.
- Shows information about Check Point servers in High Availability configuration and their states.
- Controls ISP links in ISP Redundancy configuration.
- Kills the specified Check Point processes.
- Shows a list of hosts protected by the Security Gateway.
- Shows the content of Check Point log files.
- Switches the current active log file.
- Shows a list of Security or Audit log files.
- Merges several input log files into a single log file.
- Runs FW Monitor to capture the traffic that passes through the Security Gateway.
- Rebuilds pointer files for Security or Audit log files.
- Manages the Suspicious Activity Monitoring (SAM) rules.
- Manages the Suspicious Activity Policy editor.
- Shows the contents of the Unified Policy kernel tables.
- Fetches the SD-WAN policy from a local directory.
- Shows the currently installed policy.
- Shows and deletes the contents of the specified kernel tables.
- Executes the offline Unified Policy.
- Removes all policies from the Security Gateway or Cluster Member.
- Shows the Security Gateway major and minor version number and build number.

Syntax

```
fw [-d] [-i]
       amw <options>
       ctl <options>
       defaultgen
       fetch <options>
       fetchlogs <options>
       getifs
       hastat <options>
       isp_link <options>
       kill <options>
       lichosts <options>
       log <options>
       logswitch <options>
       lslogs <options>
       mergefiles <options>
       repairlog <options>
       sam <options>
       sam_policy <options>
       sdwan <options>
       showuptables <options>
       stat
       tab <options>
       unloadlocal
       up_execute <options>
       ver <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-i`	Specifies the CoreXL Firewall instance. See *"fw -i" on page 1073*.
`amw <options>`	Fetches and unloads Threat Prevention policy. See *"fw amw" on page 1074*.

Parameter	Description
`ctl`	Controls the Firewall module. See *"fw ctl" on page 1077*.
`defaultgen`	Generates the Default Filter policy files. See *"fw defaultgen" on page 1117*.
`fetch` *<options>*	Fetches the policy from the Management Server, peer Cluster Member, or local directory. See *"fw fetch" on page 1119*.
`fetchlogs` *<options>*	Fetches the specified Security log files (`$FWDIR/log/*.log*`) or Audit log files (`$FWDIR/log/*.adtlog*`) from the specified Check Point server. See *"fw fetchlogs" on page 1122*.
`getifs`	Shows the list with this information: ■ The name of interfaces, to which the Check Point Firewall kernel attached. ■ The IP addresses assigned to the interfaces. See *"fw getifs" on page 1126*.
`hastat` *<options>*	Shows information about Check Point servers in High Availability configuration and their states. See *"fw hastat" on page 1127*.
`isp_link` *<options>*	Controls ISP links in the ISP Redundancy configuration. See *"fw isp_link" on page 1128*.
`kill` *<options>*	Kills the specified Check Point processes. See *"fw kill" on page 1129*.
`lichosts` *<options>*	Shows a list of hosts protected by the Security Gateway. See *"fw lichosts" on page 1130*.
`log` *<options>*	Shows the content of Check Point log files - Security (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`). See *"fw log" on page 1131*.
`logswitch` *<options>*	Switches the current active log file - Security (`$FWDIR/log/fw.log`) or Audit (`$FWDIR/log/fw.adtlog`). See *"fw logswitch" on page 1141*.

Parameter	Description
`lslogs <options>`	Shows a list of Security log files (`$FWDIR/log/*.log*`) or Audit log files (`$FWDIR/log/*.adtlog*`) residing on the local server or a remote server. See *"fw lslogs" on page 1145*.
`mergefiles <options>`	Merges several input log files - Security (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`) - into a single log file. See *"fw mergefiles" on page 1148*.
`monitor <options>`	Runs FW Monitor to capture the traffic that passes through the Security Gateway. See *"fw monitor" on page 1151*.
`repairlog <options>`	Rebuilds pointer files for Security log files (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`) log files. See *"fw repairlog" on page 1186*.
`sam <options>`	Manages the Suspicious Activity Monitoring (SAM) rules. See *"fw sam" on page 1187*.
`sam_policy <options>`	Manages the Suspicious Activity Policy editor. See *"fw sam_policy" on page 1195*.
`sdwan <options>`	Shows the current installed SD-WAN policy. Fetches the SD-WAN policy from a local directory. See *"fw sdwan" on page 1222*.
`showuptables <options>`	Shows the contents of the Unified Policy kernel tables. See *"fw showuptables" on page 1224*.
`stat`	Shows the currently installed policy. See *"fw stat" on page 1225*.
`tab <options>`	Shows and deletes the contents of the specified kernel tables. See *"fw tab" on page 1228*.
`unloadlocal`	Uninstalls all policies from the Security Gateway or Cluster Member. See *"fw unloadlocal" on page 1242*.
`up_execute <options>`	Executes the offline Unified Policy. See *"fw up_execute" on page 1246*.
`ver <options>`	Shows the Security Gateway major and minor version number and build number. See *"fw ver" on page 1249*.

fw -i

Description

By default, the *"fw" on page 1068* commands apply to the entire Security Gateway.

The `fw` commands show aggregated information for all CoreXL Firewall instances.

The `fw -i` commands apply to the specified CoreXL Firewall instance.

Syntax

```
fw -i <ID of CoreXL Firewall instance> <Command>
```

Parameters

Parameter	Description
<ID of CoreXL Firewall instance>	Specifies the ID of the CoreXL Firewall instance. To see the available IDs, run the *"fw ctl multik stat" on page 1635* command.
<Command>	Only these commands support the `fw -i` syntax: ■ `fw -i <ID> conntab ...` ■ `fw -i <ID> ctl get ...` ■ `fw -i <ID> ctl leak ...` ■ `fw -i <ID> ctl pstat ...` ■ `fw -i <ID> ctl set ...` ■ `fw -i <ID> monitor ...` ■ `fw -i <ID> tab ...` For details and additional parameters for any of these commands, refer to the corresponding entry for each command.

Example 1 - Show the Connections table for CoreXL Firewall instance #1

```
fw -i 1 tab -t connections
```

Example 2 - Show various internal statistics for CoreXL Firewall instance #1

```
fw -i 1 ctl pstat
```

fw amw

Description

Fetches and unloads Threat Prevention policy.

Threat Prevention policy applies to these Software Blades:

- Anti-Bot
- Anti-Spam
- Anti-Virus
- IPS
- Threat Emulation
- Threat Extraction

Syntax

- To fetch the Threat Prevention policy from the Management Server:

```
fw [-d] amw fetch -f [-i] [-n] [-r]
```

- To fetch the Threat Prevention policy from a peer Cluster Member, and, if it fails, then from the Management Server:

```
fw [-d] amw fetch -f -c [-i] [-n] [-r]
```

- To fetch the Threat Prevention policy from the specified Check Point server(s):

```
fw [-d] amw fetch [-i] [-n] [-r] <Master 1> [<Master 2> ...]
```

- To fetch the Threat Prevention policy stored locally on the Security Gateway:

```
fw [-d] amw fetch local [-nu]
```

```
fw [-d] amw fetch localhost [-nu]
```

- To fetch the Threat Prevention policy stored locally on the Security Gateway in the specified directory:

```
fw [-d] amw fetchlocal [-lu] -d <Full Path to Directory>
```

- To unload the current Threat Prevention policy:

```
fw [-d] amw unload
```

Parameters

Parameter	Description
`fw -d amw ...`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`fw amw fetch`	Fetches the Threat Prevention policy from the specified Check Point server(s). These can be a Management Server, or a peer Cluster Member.
`fw amw fetch local` `fw amw fetch localhost`	Fetches the Threat Prevention policy that is stored locally on the Security Gateway in the `$FWDIR/state/local/AMW/` directory.
`fw amw fetchlocal`	Fetches the Threat Prevention policy that stored locally on the Security Gateway in the specified directory.
`fw amw unload`	Unloads the current Threat Prevention policy from the Security Gateway. **Important** - This significantly decreases the security on the Security Gateway. This is the same as if you disable the Threat Prevention Software Blades on the Security Gateway.
`-c`	Specifies that you fetch the policy from a peer Cluster Member. **Notes:** ■ Must also use the "`-f`" parameter. ■ Works only in cluster.
`-f`	Specifies that you fetch the policy from a Management Server listed in the `$FWDIR/conf/masters` file.
`-i`	On a Security Gateway with dynamically assigned IP address (DAIP), specifies to ignore the SIC name and object name.
`-lu`	Specifies to perform a late update - to load signatures just after the Security Gateway copies the policy files to the local directory `$FWDIR/state/local/AMW/`.
`-n`	Specifies not to load the fetched policy, if it is the same as the policy already located on the Security Gateway.
`-nu`	Specifies not to update the currently installed policy.

Parameter	Description
`-r`	On a Cluster Member, specifies to ignore this option in SmartConsole **Install Policy** window: **For gateway clusters, if installation on a cluster member fails, do not install on that cluster** **Best Practice** - Use this parameter if a peer Cluster Member is **Down**.
`<Master 1> [<Master 2> ...]`	Specifies the Check Point server(s), from which to fetch the Threat Prevention policy. You can fetch the Threat Prevention policy from the Management Server, or a peer Cluster Member. **Notes:** ■ If you fetch the Threat Prevention policy from the Management Server, you can enter one of these: • The main IP address of the Management Server object. • The object name of the Management Server. • The hostname that the Security Gateway resolves to the main IP address of the Management Server. ■ If you fetch the Threat Prevention policy from a peer Cluster Member, you can enter one of these: • The main IP address of the Cluster Member object. • The IP address of the Sync interface on the Cluster Member. ■ If the fetch from the first specified `<Master>` fails, the Security Gateway fetches the policy from the second specified `<Master>` , and so on. If the Security Gateway fails to connect to each specified `<Masters>`, the Security Gateway fetches the policy from the `localhost`. ■ If you do not specify the `<Masters>` explicitly, the Security Gateway fetches the policy from the `localhost`.
`-d <Full Path to Directory>`	Specifies local directory on the Security Gateway, from which to fetch the Threat Prevention policy files.

Example

```
[Expert@MyGW:0]# fw amw fetch local
Installing Threat Prevention policy from local
Fetching Threat Prevention policy succeeded
[Expert@MyGW:0]#
```

fw ctl

Description

Controls the Firewall kernel module.

Important - In a Cluster, you must configure all the Cluster Members in the same way.

Syntax

```
fw [-d] ctl
      arp <options>
      bench <options>
      block <options>
      chain
      conn
      conntab <options>
      cpasstat <options>
      debug <options>
      get <options>
      iflist
      install
      kdebug <options>
      pstat <options>
      set <options>
      tcpstrstat <options>
      uninstall
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`arp <options>`	Shows the configured Proxy ARP entries based on the `$FWDIR/conf/local.arp` file on the Security Gateway. See *"fw ctl arp" on page 1080*.

Parameter	Description
`bench <options>`	Runs the CPU benchmark tests that collect these statistics: ■ FireWall Lock Statistics ■ Outbound Packets Statistics ■ Inbound Packets Statistics See *"fw ctl bench" on page 1081*.
`block <options>`	Blocks all connections to, from, and through the Security Gateway. See *"fw ctl block" on page 1083*.
`chain`	Shows the list of Firewall Chain Modules. See *"fw ctl chain" on page 1084*.
`conn`	Shows the list of Firewall Connection Modules. See *"fw ctl conn" on page 1086*.
`conntab <options>`	Shows formatted list of current connections from the **Connections** kernel table (ID 8158). See *"fw ctl conntab" on page 1088*.
`cpasstat <options>`	Generates statistics report about Check Point Active Streaming (CPAS). See *"fw ctl cpasstat" on page 1097*.
`debug <options>`	Generates kernel debug messages from Check Point Firewall kernel to a debug buffer. See *"'fw ctl debug' and 'fw ctl kdebug'" on page 1098*.
`dlpkstat <options>`	Generates statistics report about Data Loss Prevention kernel module. See *"fw ctl dlpkstat" on page 1099*.
`get <options>`	Shows the value of the specified kernel parameter. See *"fw ctl get" on page 1100*.
`iflist`	Shows the list with this information: ■ The name of interfaces, to which the Check Point Firewall kernel attached. ■ The internal numbers of the interfaces in the Check Point Firewall kernel. See *"fw ctl iflist" on page 1102*.
`install`	Tells the operating system to start passing packets to Firewall. See *"fw ctl install" on page 1103*.

Parameter	Description
`kdebug <options>`	Generates kernel debug messages from Check Point Firewall kernel to a debug buffer. See *"'fw ctl debug' and 'fw ctl kdebug'" on page 1098*.
`leak <options>`	Generates leak detection report. See *"fw ctl leak" on page 1104*.
`pstat <options>`	Shows Security Gateway various internal statistics. See *"fw ctl pstat" on page 1107*.
`set <options>`	Configures the specified value for the specified kernel parameter. See *"fw ctl set" on page 1110*.
`tcpstrstat <options>`	Generates statistics report about TCP Streaming. See *"fw ctl tcpstrstat" on page 1114*.
`uninstall`	Tells the operating system to stop passing packets to Firewall, and unloads the current Security Policy. See *"fw ctl uninstall" on page 1116*.

fw ctl arp

Description

Shows the configured Proxy ARP entries based on the `$FWDIR/conf/local.arp` file on the Security Gateway.

For more information about the Proxy ARP, see sk30197.

Syntax

```
fw [-d] ctl arp
       [-h]
       [-n]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-h`	Shows the built-in help.
`-n`	Specifies not to resolve hostnames.

fw ctl bench

Description

The benchmark mechanism provides a way to measure the time spent in the code between two points.

This command runs the CPU benchmark tests that collect these statistics:

- FireWall Lock Statistics
- Outbound Packets Statistics
- Inbound Packets Statistics.

Note - This command writes the output of these tests to the `dmesg`.

Syntax

```
fw [-d] ctl bench
      -h
      lock
            [{ioctl | packet} [<Limit>]]
            [stop]
      packet [{<Limit> | stop}]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-h`	Shows the built-in help.

Parameter	Description
`lock [ioctl[ <Limit>]] [packet [<Limit>]] [stop]`	Runs the lock benchmark that collects the FireWall Lock Statistics. Available options: ■ No parameters - Starts the lock benchmark. ■ `ioctl` - Calculates the IOCTL flow statistics. ■ `packet` - Calculates the packet flow statistics. ■ *<Limit>* - Specifies the time limit (in seconds) for the benchmark to run. Default is 10 seconds. Maximum is 200 seconds. ■ `stop` - Stops the current lock benchmark.
`packet [{<Limit> | stop}]`	Runs the packet benchmark test that collects these statistics: ■ Outbound Packets Statistics ■ Inbound Packets Statistics Available options: ■ No parameters - Starts the packet benchmark. ■ *<Limit>* - Specifies the time limit (in seconds) for the benchmark to run. Default is 10 seconds. Maximum is 200 seconds. ■ `stop` - Stops the current packet benchmark.

fw ctl block

Description

Blocks all connections to, from, and through the Security Gateway.

Important - The "`fw ctl block on`" command immediately blocks all connections without a prompt and regardless the currently installed policy. To unblock the connections, you must either reboot the Security Gateway, or connect to the Security Gateway over a serial console (or Lights Out Management Card) and run the "`fw ctl block off`" command.

Syntax

```
fw [-d] ctl block
      off
      on
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`off`	Removes the block of all connections.
`on`	Blocks all connections.

fw ctl chain

Description

Shows the list of Firewall Chain Modules.

This list shows various inspection Chain Modules, through which the traffic passes on this Security Gateway.

The available Chain Modules depend on the configuration and enabled Software Blades.

Important - In Cluster, outputs of this command must be the same on all the Cluster Members.

Syntax

```
fw [-d] ctl chain
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.

Example

```
[Expert@MyGW:0]# fw ctl chain
in chain (23):
        0: -7fffffff (0000000000000000) (00000000) SecureXL inbound (sxl_in)
        1: -7ffffffe (0000000000000000) (00000000) SecureXL inbound CT (sxl_ct)
        2: -7f800000 (ffffffff8b6812b0) (ffffffff) IP Options Strip (in) (ipopt_strip)
        3: -7d000000 (ffffffff8a96ee80) (00000003) vpn multik forward in
        4: - 2000000 (ffffffff8a97d830) (00000003) vpn decrypt (vpn)
        5: - 1fffffa (ffffffff8a9533a0) (00000001) l2tp inbound (l2tp)
        6: - 1fffff8 (ffffffff8b67f0e0) (00000001) Stateless verifications (in) (asm)
        7: - 1fffff7 (ffffffff8b67ec00) (00000001) fw multik misc proto forwarding
        8: - 1fffff2 (ffffffff8a982aa0) (00000003) vpn tagging inbound (tagging)
        9: - 1fffff0 (ffffffff8a983460) (00000003) vpn decrypt verify (vpn_ver)
        10:         0 (ffffffff8b85a950) (00000001) fw VM inbound  (fw)
        11:         1 (ffffffff8a97ed70) (00000003) vpn policy inbound (vpn_pol)
        12:         2 (ffffffff8b681700) (00000001) fw SCV inbound (scv)
        13:         3 (ffffffff8a982130) (00000003) vpn before offload (vpn_in)
        14:         4 (ffffffff8b0fa5c0) (00000003) QoS inbound offload chain module
        15:         5 (ffffffff8b574730) (00000003) fw offload inbound (offload_in)
        16:        10 (ffffffff8b84c9c0) (00000001) fw post VM inbound  (post_vm)
        17:    100000 (ffffffff8b807970) (00000001) fw accounting inbound (acct)
        18:  22000000 (ffffffff8b0fbfc0) (00000003) QoS slowpath inbound chain mod (fg_sched)
        19:  7f730000 (ffffffff8b3d3aa0) (00000001) passive streaming (in) (pass_str)
        20:  7f750000 (ffffffff8b17dff0) (00000001) TCP streaming (in) (cpas)
        21:  7f800000 (ffffffff8b681260) (ffffffff) IP Options Restore (in) (ipopt_res)
        22:  7fb00000 (ffffffff8a9fe8a0) (00000001) Cluster Late Correction (ha_for)
out chain (19):
        0: -7f800000 (ffffffff8b6812b0) (ffffffff) IP Options Strip (out) (ipopt_strip)
        1: -78000000 (ffffffff8a96ee60) (00000003) vpn multik forward out
        2: - 1ffffff (ffffffff8a97fb70) (00000003) vpn nat outbound (vpn_nat)
        3: - 1fffff0 (ffffffff8b168640) (00000001) TCP streaming (out) (cpas)
        4: - 1ffff50 (ffffffff8b3d3aa0) (00000001) passive streaming (out) (pass_str)
        5: - 1ff0000 (ffffffff8a982aa0) (00000003) vpn tagging outbound (tagging)
        6: - 1f00000 (ffffffff8b67f0e0) (00000001) Stateless verifications (out) (asm)
        7:         0 (ffffffff8b85a950) (00000001) fw VM outbound (fw)
        8:        10 (ffffffff8b84c9c0) (00000001) fw post VM outbound  (post_vm)
        9:   2000000 (ffffffff8a982900) (00000003) vpn policy outbound (vpn_pol)
        10:  15000000 (ffffffff8b0fac30) (00000003) QoS outbound offload chain modul (fg_pol)
        11:  1ffffff0 (ffffffff8a951790) (00000001) l2tp outbound (l2tp)
        12:  20000000 (ffffffff8a978280) (00000003) vpn encrypt (vpn)
        13:  21000000 (ffffffff8b0fbfc0) (00000003) QoS slowpath outbound chain mod (fg_sched)
        14:  7f000000 (ffffffff8b807970) (00000001) fw accounting outbound (acct)
        15:  7f700000 (ffffffff8b17cb10) (00000001) TCP streaming post VM (cpas)
        16:  7f800000 (ffffffff8b681260) (ffffffff) IP Options Restore (out) (ipopt_res)
        17:  7f900000 (0000000000000000) (00000000) SecureXL outbound (sxl_out)
        18:  7fa00000 (0000000000000000) (00000000) SecureXL deliver (sxl_deliver)
[Expert@MyGW:0]#
```

fw ctl conn

Description

Shows the list of Firewall Connection Modules.

This list shows various inspection Connection Modules, through which the traffic passes on this Security Gateway.

The available Connection Modules depend on the configuration and enabled Software Blades.

Important - In Cluster, outputs of this command must be the same on all the Cluster Members.

Syntax

```
fw [-d] ctl conn
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.

Example

```
[Expert@MyGW:0]# fw ctl conn
Registered connections modules:
No. Name             Newconn          Packet           End              Reload           Dup
Type Dup Handler
Connectivity level 0:
1:  Accounting       1:  Accounting       0000000000000000 0000000000000000 FFFFFFFF8B8395A0
0000000000000000 Special  FFFFFFFF8B831720
2:  Authentication   2:  Authentication   FFFFFFFF8B3150A0 0000000000000000 0000000000000000
0000000000000000 Special  FFFFFFFF8B34FCC0
8:  NAT              8:  NAT              0000000000000000 0000000000000000 FFFFFFFF8B6D1AF0
0000000000000000 Special  FFFFFFFF8B6B8410
9:  RTM              9:  RTM              0000000000000000 0000000000000000 0000000000000000
0000000000000000 None
10:  RTM2             10:  RTM2             0000000000000000 0000000000000000 FFFFFFFF8B014970
0000000000000000 None
11:  SPII             11:  SPII             FFFFFFFF8B412060 0000000000000000 FFFFFFFF8B41AF40
FFFFFFFF8B4016A0 None
13:  VPN              13:  VPN              FFFFFFFF8A965440 0000000000000000 FFFFFFFF8AA4CC40
0000000000000000 Special  FFFFFFFF8AA60490
Connectivity level 1:
13:  VPN              13:  VPN              0000000000000000 0000000000000000 0000000000000000
0000000000000000 None
[Expert@MyGW:0]#
```

fw ctl conntab

Description

Shows formatted list of current connections from the **Connections** kernel table (ID 8158).

Use this command if you want to see the simplified information about the current connections.

Best Practices:

- Use the "`fw ctl conntab`" command to see the simplified information about the current connections.
- Use the "`fw tab -t connections -f`" command (*"fw tab" on page 1228*) to see the detailed (and more technical) information about the current connections.

Important:

- You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).
- On Scalable Platforms (Maestro and Chassis), you must connect to the applicable Security Group.

Syntax

Important - You can specify many parameters at the same time.

```
fw ctl conntab {-h | -help}
```

```
fw [-d] ctl conntab [-x [-y]]
      -sip=<Source IP Address in Decimal Format>
      -sport=<Port Number in Decimal Format>
      -dip=<Destination IP Address>
      -dport=<Port Number in Decimal Format>
      -proto=<Protocol Number in Decimal Format>
      -service=<Name of Service>
      -rule=<Rule Number in Decimal Format>
      -state=<State>
      -type=<Type>
      -flags=<Flags>
```

Parameters

Parameter	Description
`-h` `-help}`	Shows the built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-x [-y]`	Deletes entries that match the specified filters. Without this parameter "`-x`", the command only shows entries that match the specified filters. The parameter "`-y`" specifies not to show a prompt before Security Gateway executes this command.

`-sip=<`*`Source IP Address in Decimal Format`*`>`	Filters the output by the specified Source IP address.
	Note - The value can be a range of IP addresses: *<IP_address_1>-<IP_address_2>*
	Examples:
	`-sip=192.168.3.57`
	`-sip=192.168.3.55-192.168.3.66`

`-sport=<`*`Port Number in Decimal Format`*`>`	Filters the output by the specified Source Port number. See *IANA Service Name and Port Number Registry*. **Note** - The value can be a range of port numbers: *<port_1>-<port_2>* Examples: ▪ `-sport=35598` ▪ `-sport=33000-33320`
`-dip=<`*`Destination IP Address in Decimal Format`*`>`	Filters the output by the specified Destination IP address. **Note** - The value can be a range of IP addresses: *<IP_address_1>-<IP_address_2>* Examples: ▪ `-dip=192.168.3.57` ▪ `-dip=192.168.3.55-192.168.3.66`

Parameter	Description
`-dport=<Port Number in Decimal Format>`	Filters the output by the specified Destination Port number. See *IANA Service Name and Port Number Registry*. **Note** - The value can be a range of port numbers: *<port_1>-<port_2>* Examples: ■ `-dport=80` ■ `-dport=80-88`

`-proto=<Protocol Number in Decimal Format>`	Filters the output by the specified Protocol number.
	See *IANA Protocol Numbers*.
	Notes:
	■ For the protocols TCP, UDP, and ICMP, you can also specify the protocol name in all lowercase letters (`tcp`, `udp`, `icmp`) or all uppercase letters (`TCP`, `UDP`, `ICMP`).
	■ For protocols other than TCP, UDP, and ICMP, you must specify the protocol number.
	Examples:
	■ `-proto=6`
	`-proto=TCP`
	Filters the output for TCP.
	■ `-proto=11`
	`-proto=UDP`
	Filters the output for UDP.
	■ `-proto=1`
	`-proto=ICMP`
	Filters the output for ICMP.

Parameter	Description
`-service=<Name of Service>`	Filters the output by the specified Service name. **Notes:** ■ You must use the string that appears in the output of this command "`fw ctl conntab`" or the service name that appears in SmartConsole. ■ You can also use the service number that appears in the output of this command "`fw ctl conntab`". Examples: ■ `-service=http` ■ `-service=https` ■ `-service=391`
`-rule=<Rule Number in Decimal Format>`	See your Access Control Policy in SmartConsole, or in the output of the command. **Note** - The value can be a range of rule numbers: *<rule_1>-<rule_2>* Examples: ■ `-rule=1` ■ `-rule=5-8`

Parameter	Description
`-state=<State>`	Filters the output by the specified TCP State: ■ `-state=SYN_SENT` Filters the output for TCP connections with SYN. ■ `-state=SYN_ACK` Filters the output for TCP connections with SYN-ACK. ■ `-state=ESTABLISHED` Filters the output for established TCP connections. ■ `-state=SRC_FIN` Filters the output for TCP connections with SYN-FIN from a source. ■ `-state=DST_FIN` Filters the output for TCP connections with SYN-FIN from a destination. ■ `-state=BOTH_FIN` Filters the output for TCP connections with SYN-FIN from both a source and a destination. **Notes:** ■ You can specify the value in all lowercase letters or all uppercase letters. ■ The parameter "`-state`" is not supported together with the parameters "`-type`" or "`-flags`".

Parameter	Description

`-type=<Type>`	Filters the output by the specified Connection Type bitmask.
	Note - The parameter "`-type`" is not supported together with the parameter "`-state`".
	To see the Connection Type bitmask value of a connection entry:
	1. Run:
	`fw tab -u -t connections`
	2. Immediately after the tuple, after the semi-colon, refer to the first value.
	In sk65133, this value is denoted as "`R_CTYPE`".
	You must specify Type bitmask in this format:
	`-type=0x<Bits to Select>/0x<Value of 'R_CTYPE'>`
	Where:
	■ `0x<Value of 'R_CTYPE'>`
	Specifies the "`r_ctype`" value of a connection entry.
	■ `0x<Bits to Select>`
	Specifies the bits that should be selected out of the "`R_CTYPE`" value.

Parameter	Description

`-type=<Flags>`	Filters the output by the specified Connection Flag bitmask.
	Note - The parameter "`-flags`" is not supported together with the parameter "`-state`".
	To see the Connection Flag bitmask value of a connection entry:
	1. Run:
	`fw tab -u -t connections`
	2. Immediately after the tuple, after the semi-colon, refer to the second value.
	In sk65133, this value is denoted as "`R_CFLAGS`".
	You must specify Type bitmask in this format:
	`-type=0x<Bits to Select>/0x<Value of 'R_CFLAGS'>`
	Where:
	■ `0x<Value of 'R_CFLAGS'>`
	Specifies the "`R_CFLAGS`" value of a connection entry.
	■ `0x<Bits to Select>`
	Specifies the bits that should be selected out of the "`r_ctype`" value

Examples

Example 1 - Default output

```
[Expert@MyGW:0]# fw ctl conntab
<(inbound, src=[192.168.204.1,54201], dest=[192.168.204.40,22], TCP); 3593/3600, rule=2, tcp state=TCP_ESTABLISHED, service=ssh(481),
Ifncin=1, Ifncout=1, conn modules: Authentication, FG-1>
<(outbound, src=[192.168.204.40,59249], dest=[192.168.204.1,53], UDP); 20/40, rule=0, service=domain-udp(335), Ifnsout=1, conn
modules: Authentication, FG-1>
<(outbound, src=[192.168.204.40,37892], dest=[192.168.204.1,53], UDP); 20/40, rule=0, service=domain-udp(335), Ifnsin=1, Ifnsout=1,
conn modules: Authentication, FG-1>
[Expert@MyGW:0]#
```

Example 2 - Filter by a destination port

```
[Expert@MyGW:0]# fw ctl conntab -dport=22
<(inbound, src=[192.168.204.1,54201], dest=[192.168.204.40,22], TCP); 3594/3600, rule=2, tcp state=TCP_ESTABLISHED, service=ssh(481),
Ifncin=1, Ifncout=1, conn modules: Authentication, FG-1>
[Expert@MyGW:0]#
```

Example 3 - Filter by a destination port

```
[Expert@MyGW:0]# fw ctl conntab -dport=53
<(outbound, src=[192.168.204.40,33585], dest=[192.168.204.1,53], UDP); 39/40, rule=0, service=domain-udp(335), Ifnsout=1, conn
modules: Authentication, FG-1>
<(outbound, src=[192.168.204.40,56661], dest=[192.168.204.1,53], UDP); 39/40, rule=0, service=domain-udp(335), Ifnsin=1, Ifnsout=1,
conn modules: Authentication, FG-1>
[Expert@MyGW:0]#
```

Example 4 - Filter by a source port

```
[Expert@MyGW:0]# fw ctl conntab -sport=54201
<(inbound, src=[192.168.204.1,54201], dest=[192.168.204.40,22], TCP); 3600/3600, rule=2, tcp state=TCP_ESTABLISHED, service=ssh(481),
Ifncin=1, Ifncout=1, conn modules: Authentication, FG-1>
[Expert@MyGW:0]#
```

Example 5 - Filter by a protocol

```
[Expert@MyGW:0]# fw ctl conntab -proto=UDP
<(outbound, src=[192.168.204.40,44966], dest=[192.168.204.1,53], UDP); 37/40, rule=0, service=domain-udp(335), Ifnsin=1, Ifnsout=1,
conn modules: Authentication, FG-1>
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fw ctl conntab -proto=11
<(outbound, src=[192.168.204.40,44966], dest=[192.168.204.1,53], UDP); 37/40, rule=0, service=domain-udp(335), Ifnsin=1, Ifnsout=1,
conn modules: Authentication, FG-1>
[Expert@MyGW:0]#
```

Example 6 - Filter by a protocol

```
[Expert@MyGW:0]# fw ctl conntab -proto=TCP
<(inbound, src=[192.168.204.1,54201], dest=[192.168.204.40,22], TCP); 3596/3600, rule=2, tcp state=TCP_ESTABLISHED, service=ssh(481),
Ifncin=1, Ifncout=1, conn modules: Authentication, FG-1>
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fw ctl conntab -proto=6
<(inbound, src=[192.168.204.1,54201], dest=[192.168.204.40,22], TCP); 3596/3600, rule=2, tcp state=TCP_ESTABLISHED, service=ssh(481),
Ifncin=1, Ifncout=1, conn modules: Authentication, FG-1>
[Expert@MyGW:0]#
```

Example 7 - Filter by a service

```
[Expert@MyGW:0]# fw ctl conntab -service=domain-udp
<(outbound, src=[192.168.204.40,44966], dest=[192.168.204.1,53], UDP); 35/40, rule=0, service=domain-udp(335), Ifnsin=1, Ifnsout=1,
conn modules: Authentication, FG-1>
[Expert@MyGW:0]#
```

Example 8 - Filter by a rule number

```
[Expert@MyGW:0]# fw ctl conntab -rule=2
<(inbound, src=[192.168.204.1,54201], dest=[192.168.204.40,22], TCP); 3597/3600, rule=2, tcp state=TCP_ESTABLISHED, service=ssh(481),
Ifncin=1, Ifncout=1, conn modules: Authentication, FG-1>
[Expert@MyGW:0]#
```

Example 9 - Filter by a destination IP address, destination port, protocol, and service

```
[Expert@MyGW:0]# fw ctl conntab -dip=192.168.204.40 -dport=22 -proto=TCP -service=ssh
<(inbound, src=[192.168.204.1,54201], dest=[192.168.204.40,22], TCP); 3599/3600, rule=2, tcp state=TCP_ESTABLISHED, service=ssh(481),
Ifncin=1, Ifncout=1, conn modules: Authentication, FG-1>
[Expert@MyGW:0]#
```

Example 10 - Formatted detailed output from the Connections table (for comparison)

```
[Expert@MyGW:0]# fw tab -t connections -f

Formatting table's data - this might take a while...

localhost:
 Date: Sep 10, 2018
11:30:56 5 N/A N/A 192.168.204.40 > N/A LogId: <max_null>; ContextNum: <max_null>; OriginSicName: cn=cp_mgmt,o=MyGW..44jkyv; :
(+)==================================(+); Table_Name: connections; : (+); Attributes: dynamic, id 8158, attributes: keep, sync,
aggressive aging, kbufs 21 22 23 24 25 26 27 28 29 30 31 32 33 34, expires 25, refresh, , hashsize 2097152, unlimited;
LastUpdateTime: 10Sep2018 11:30:56; ProductName: VPN-1 & FireWall-1; ProductFamily: Network;

 11:30:56 5 N/A N/A 192.168.204.40 > N/A LogId: <max_null>; ContextNum: <max_null>; OriginSicName: cn=cp_mgmt,o=MyGW..44jkyv; : -----
------------------------------(+); Direction: 1; Source: 192.168.204.40; SPort: 54201; Dest: 192.168.204.1; DPort: 53; Protocol: udp;
CPTFMT_sep: ;; Type: 131073; Rule: 0; Timeout: 335; Handler: 0; Ifncin: -1; Ifncout: -1; Ifnsin: -1; Ifnsout: 1; Bits:
0000780000000000; Expires: 23/40; LastUpdateTime: 10Sep2018 11:30:56; ProductName: VPN-1 & FireWall-1; ProductFamily: Network;

 11:30:56 5 N/A N/A 192.168.204.40 > N/A LogId: <max_null>; ContextNum: <max_null>; OriginSicName: cn=cp_mgmt,o=MyGW..44jkyv; : -----
------------------------------(+); Direction: 0; Source: 192.168.204.1; SPort: 53; Dest: 192.168.204.40; DPort: 54201; Protocol: udp;
CPTFMT_sep_1: ->; Direction_1: 1; Source_1: 192.168.204.40; SPort_1: 54201; Dest_1: 192.168.204.1; DPort_1: 53; Protocol_1: udp; FW_
symval: 2054; LastUpdateTime: 10Sep2018 11:30:56; ProductName: VPN-1 & FireWall-1; ProductFamily: Network;

 11:30:56 5 N/A N/A 192.168.204.40 > N/A LogId: <max_null>; ContextNum: <max_null>; OriginSicName: cn=cp_mgmt,o=MyGW..44jkyv; : -----
------------------------------(+); Direction: 1; Source: 192.168.204.40; SPort: 22; Dest: 192.168.204.1; DPort: 54201; Protocol: tcp;
CPTFMT_sep_1: ->; Direction_2: 0; Source_2: 192.168.204.1; SPort_2: 54201; Dest_2: 192.168.204.40; DPort_2: 22; Protocol_2: tcp; FW_
symval: 2053; LastUpdateTime: 10Sep2018 11:30:56; ProductName: VPN-1 & FireWall-1; ProductFamily: Network;

 11:30:56 5 N/A N/A 192.168.204.40 > N/A LogId: <max_null>; ContextNum: <max_null>; OriginSicName: cn=cp_mgmt,o=MyGW..44jkyv; : -----
------------------------------(+); Direction: 0; Source: 192.168.204.1; SPort: 54201; Dest: 192.168.204.40; DPort: 22; Protocol: tcp;
CPTFMT_sep: ;; Type: 114689; Rule: 2; Timeout: 481; Handler: 0; Ifncin: 1; Ifncout: 1; Ifnsin: -1; Ifnsout: -1; Bits:
02007800000f9000; Expires: 3596/3600; LastUpdateTime: 10Sep2018 11:30:56; ProductName: VPN-1 & FireWall-1; ProductFamily: Network;

 11:30:56 5 N/A N/A 192.168.204.40 > N/A LogId: <max_null>; ContextNum: <max_null>; OriginSicName: cn=cp_mgmt,o=MyGW..44jkyv; : -----
------------------------------(+); Direction: 0; Source: 192.168.204.1; SPort: 53; Dest: 192.168.204.40; DPort: 44966; Protocol: udp;
CPTFMT_sep_1: ->; Direction_1: 1; Source_1: 192.168.204.40; SPort_1: 44966; Dest_1: 192.168.204.1; DPort_1: 53; Protocol_1: udp; FW_
symval: 2054; LastUpdateTime: 10Sep2018 11:30:56; ProductName: VPN-1 & FireWall-1; ProductFamily: Network;

 11:30:56 5 N/A N/A 192.168.204.40 > N/A LogId: <max_null>; ContextNum: <max_null>; OriginSicName: cn=cp_mgmt,o=MyGW..44jkyv; : -----
------------------------------(+); Direction: 1; Source: 192.168.204.40; SPort: 44966; Dest: 192.168.204.1; DPort: 53; Protocol: udp;
CPTFMT_sep: ;; Type: 131073; Rule: 0; Timeout: 335; Handler: 0; Ifncin: -1; Ifncout: -1; Ifnsin: 1; Ifnsout: 1; Bits:
0000780000000000; Expires: 23/40; LastUpdateTime: 10Sep2018 11:30:56; ProductName: VPN-1 & FireWall-1; ProductFamily: Network;

[Expert@MyGW:0]#
```

fw ctl cpasstat

Description

Generates statistics report about Check Point Active Streaming (CPAS).

Syntax

```
fw [-d] ctl cpasstat [-r]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-r`	Resets the counters.

'fw ctl debug' and 'fw ctl kdebug'

Description

These commands generate kernel debug messages from Check Point Firewall kernel to a debug buffer.

For more information, see the *R81.20 Security Gateway Guide* - Chapter *Kernel Debug on Security Gateway*.

fw ctl dlpkstat

Description

Generates statistics report about Data Loss Prevention, inspected HTTP requests, and Identity Awareness Captive Portal.

This report contains these statistics:

Category	Information
DLP Kernel Statistics Information	Emails and HTTP requests
User Mode Responses Statistics	Emails and HTTP requests
Identity Awareness - Captive Portal	HTTP requests redirected to the Captive Portal
Identity Awareness - Fetch Users Statistics	Synchronous and asynchronous Identity Awareness queries

Best Practice - This report is very useful when you:

- Debug problems with HTTP protocol that occur under traffic stress.
- Examine the traffic shape (for example, to know how many HTTP "POST" and HTTP "GET" requests pass through the Security Gateway).

Syntax

```
fw [-d] ctl dlpkstat [-r]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-r`	Resets the counters.

fw ctl get

Description

Shows the current value of the specified kernel parameter.

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- In VSX Gateway, the configured values of kernel parameters apply to all existing Virtual Systems and Virtual Routers.

Notes:

- Kernel parameters let you change the advanced behavior of your Security Gateway.
- There are two types of kernel parameters - *integer* and *string*.
- Security Gateway gets the names and the default values of the kernel parameters from these kernel module files:
  - `$FWDIR/boot/modules/fw_kern_64.o`
  - `$FWDIR/boot/modules/fw_kern_64_v6.o`
  - `$FWDIR/boot/modules/fw_kern_64_3_10_64.o`
  - `$FWDIR/boot/modules/fw_kern_64_3_10_64_v6.o`
  - `$PPKDIR/boot/modules/sim_kern_64.o`
  - `$PPKDIR/boot/modules/sim_kern_64_v6.o`
  - `$PPKDIR/boot/modules/sim_kern_64_3_10_64.o`
  - `$PPKDIR/boot/modules/sim_kern_64_3_10_64_v6.o`
- Refer to the related command *"fw ctl set" on page 1110*.
- Refer to the related article sk33156: Creating a file with all the kernel parameters and their values

Syntax

```
fw [-d] ctl get
      int <Name of Integer Kernel Parameter> [-a]
      str <Name of String Kernel Parameter> [-a]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
<Name of Integer Kernel Parameter>	Specifies the name of the integer kernel parameter.
<Name of String Kernel Parameter>	Specifies the name of the string kernel parameter.
`-a`	Specifies to search for this kernel parameter in this order: 1. In `$FWDIR/boot/modules/fw_*.o` 2. In `$PPKDIR/boot/modules/sim_*.o`

Example for an integer kernel parameter

```
[Expert@MyGW:0]# fw ctl get int fw_kdprintf_limit -a
FW:
fw_kdprintf_limit = 100
PPAK 0: fw_kdprintf_limit = 10
[Expert@MyGW:0]#
```

Example for a string kernel parameter

```
[Expert@MyGW:0]# fw ctl get str fileapp_default_encoding_charset -a
FW:
fileapp_default_encoding_charset = 'UTF-8'
PPAK 0: Get failed.
[Expert@MyGW:0]#
```

fw ctl iflist

Description

Shows the list with this information:

- The name of interfaces, to which the Check Point Firewall kernel attached.
- The internal numbers of the interfaces in the Check Point Firewall kernel.

Notes:

- This list shows all detected interfaces, even if there are no IP addresses assigned on them.
- You use this list when you analyze a kernel debug, which shows only the internal numbers of the interfaces (for example, `ifn=2`).
- Related *"cpstat" on page 1019* commands:
  - `cpstat -f ifconfig os`
  - `cpstat -f interfaces fw`

Syntax

```
fw [-d] ctl iflist
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.

Example

```
[Expert@MyGW:0]# fw ctl iflist
fw ctl iflist
1 : eth0
2 : eth1
3 : eth2
4 : eth3
5 : eth4
6 : eth5
7 : eth6
8 : eth7
[Expert@MyGW:0]#
```

fw ctl install

Description

Tells the operating system to start passing packets to Firewall.

This command runs automatically when the Security Gateway or an administrator runs the *"cpstart" on page 1018* command.

Warning - If you run the *"fw ctl uninstall" on page 1116* command and then the "`fw ctl install`" command, it does **not** restore the Security Policy.
You must run one of these commands: *"fw fetch" on page 1119*, or *"cpstart" on page 1018*.

Syntax

```
fw [-d] ctl install
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.

fw ctl leak

Description

Generates leak detection report. This report is for Check Point use only.

Important - This command save the report into the active `/var/log/messages` file and the `dmesg` buffer.

Syntax

```
fw [-d] ctl leak
      {-h | -help}
      [{-a | -A}] [-t <Internal Object Type>] [-o <Internal Object
ID>]
            [-d] [-l] [-p]
            [-s]
```

Parameters

Parameter	Description
`fw -d ctl leak ...`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{-h | -help}`	Shows the built-in help.
`-a`	Specifies to perform leak detection for potential leaks. This parameter is mutually exclusive with the parameter "`-A`".
`-A`	Specifies to perform leak detection for all leaks. This parameter is mutually exclusive with the parameter "`-a`".
`-d`	Dumps object data. This parameter is mutually exclusive with the parameter "`-s`".
`-l`	Prints the action log. This parameter is mutually exclusive with the parameter "`-s`".
`-o <Internal Object ID>`	Specifies to perform leak detection for the specified internal object ID.

Parameter	Description
`-p`	Purges the internal objects from the lists. This parameter is mutually exclusive with the parameter "`-s`".
`-s`	Shows summary only. This parameter is mutually exclusive with the parameters "`-d`", "`-l`", and "`-p`".
`-t <Internal Object Type>`	Specifies the internal object types, for which to perform leak detection. Available internal object types are: ■ `chain` ■ `connh` ■ `cookie` ■ `kbuf` ■ `num` If you do not specify the internal object type explicitly, the command performs leak detection for all internal object types.

Procedure

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Log in to the Expert mode.
3	Back up the current */var/log/messages* file: `[Expert@GW_HostName:0]# cp -v /var/log/messages{,_BKP}`
4	Delete the information from the current */var/log/messages* file: `[Expert@GW_HostName:0]# echo '' > /var/log/messages`
5	Delete the information from the current *dmesg* buffer: `[Expert@GW_HostName:0]# dmesg -c`
6	Generate the leak detection report (see the **Syntax** section above): `[Expert@GW_HostName:0]# fw [-d] ctl leak <options>`

Step	Instructions

7	Make sure the command generated the leak detection report:
	`[Expert@GW_HostName:0]# dmesg`
	`[Expert@GW_HostName:0]# cat /var/log/messages`

8	Collect the leak detection report: `[Expert@GW_HostName:0]# cp -v /var/log/messages{,_LEAK_DETECTION}`
9	Analyze the leak detection report: `/var/log/messages_LEAK_DETECTION`

Example

```
[Expert@MyGW:0]# cp -v /var/log/messages{,_BKP}
`/var/log/messages' -> `/var/log/messages_BKP'
[Expert@MyGW:0]#
[Expert@MyGW:0]# echo '' > /var/log/messages
[Expert@MyGW:0]#
[Expert@MyGW:0]# dmesg -c
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl leak -s
[Expert@MyGW:0]#
[Expert@MyGW:0]# dmesg
[fw4_0];fwleak_report: type chain - 0 objects
[fw4_0];fwleak_report: type cookie - 0 objects
[fw4_0];fwleak_report: type kbuf - 0 objects
[fw4_0];fwleak_report: type connh - 0 objects
[fw4_1];fwleak_report: type chain - 0 objects
[fw4_1];fwleak_report: type cookie - 0 objects
[fw4_1];fwleak_report: type kbuf - 0 objects
[fw4_1];fwleak_report: type connh - 0 objects
[fw4_2];fwleak_report: type chain - 0 objects
[fw4_2];fwleak_report: type cookie - 0 objects
[fw4_2];fwleak_report: type kbuf - 0 objects
[fw4_2];fwleak_report: type connh - 0 objects
[Expert@MyGW:0]#
[Expert@MyGW:0]# cat /var/log/messages
Sep 12 16:09:50 2019 MyGW kernel: [fw4_0];fwleak_report: type chain - 0 objects
Sep 12 16:09:50 2019 MyGW kernel: [fw4_0];fwleak_report: type cookie - 0 objects
Sep 12 16:09:50 2019 MyGW kernel: [fw4_0];fwleak_report: type kbuf - 0 objects
Sep 12 16:09:50 2019 MyGW kernel: [fw4_0];fwleak_report: type connh - 0 objects
Sep 12 16:09:50 2019 MyGW kernel: [fw4_1];fwleak_report: type chain - 0 objects
Sep 12 16:09:50 2019 MyGW kernel: [fw4_1];fwleak_report: type cookie - 0 objects
Sep 12 16:09:50 2019 MyGW kernel: [fw4_1];fwleak_report: type kbuf - 0 objects
Sep 12 16:09:50 2019 MyGW kernel: [fw4_1];fwleak_report: type connh - 0 objects
Sep 12 16:09:50 2019 MyGW kernel: [fw4_2];fwleak_report: type chain - 0 objects
Sep 12 16:09:50 2019 MyGW kernel: [fw4_2];fwleak_report: type cookie - 0 objects
Sep 12 16:09:50 2019 MyGW kernel: [fw4_2];fwleak_report: type kbuf - 0 objects
Sep 12 16:09:50 2019 MyGW kernel: [fw4_2];fwleak_report: type connh - 0 objects
[Expert@MyGW:0]
[Expert@MyGW:0]# cp -v /var/log/messages{,_LEAK_DETECTION}
`/var/log/messages' -> `/var/log/messages_LEAK_DETECTION'
[Expert@MyGW:0]#
```

fw ctl pstat

Description

Shows Security Gateway various internal statistics:

- System Capacity Summary
- Hash kernel memory (hmem) statistics
- System kernel memory (smem) statistics
- Kernel memory (kmem) statistics
- Cookies
- Connections
- Fragments
- NAT
- Handles

Syntax

Important - You can specify many parameters at the same time.

```
fw [-d] ctl pstat [-c] [-h] [-k] [-l] [-m] [-o] [-s] [-v {4 | 6}]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-c`	Shows detailed CoreXL Dispatcher statistics: ■ `fwmultik_global_stats` splits for each CoreXL Firewall instance. ■ `fwmultik_gconn_stats` for each CPU. ■ `fwmultik_stats` for each CPU.
`-h`	Shows additional Hash kernel memory (hmem) statistics.
`-k`	Shows additional Kernel memory (kmem) statistics.

Parameter	Description
`-l`	Shows Handles statistics.
`-m`	Shows general CoreXL Dispatcher statistics.
`-o`	Shows additional Cookies statistics.
`-s`	Shows additional System kernel memory (smem) statistics.
`-v 4` `-v 6`	Shows statistics for IPv4 (`-v 4`) traffic only, or for IPv6 (`-v 4`) traffic only. Default is to show statistics for both IPv4 and IPv6 traffic.

Examples

Example 1 - fw ctl pstat

```
[Expert@MyGW:0]# fw ctl pstat

System Capacity Summary:
  Memory used: 3% (265 MB out of 7117 MB) - below watermark
  Concurrent Connections: Not Available
  Aggressive Aging is enabled, not active

Hash kernel memory (hmem) statistics:
  Total memory allocated: 742391808 bytes in 181248 (4096 bytes) blocks using 1 pool
  Total memory bytes  used:        0   unused: 742391808 (100.00%)   peak: 68247020
  Total memory blocks used:        0   unused:   181248 (100%)   peak:    17227
  Allocations: 2193027 alloc, 0 failed alloc, 2154121 free

System kernel memory (smem) statistics:
  Total memory  bytes  used: 913975068   peak: 1165010872
  Total memory bytes wasted:  7883999
    Blocking  memory  bytes   used:  4896272   peak:  6916084
    Non-Blocking memory bytes used: 909078796   peak: 1158094788
  Allocations: 13217 alloc, 0 failed alloc, 10027 free, 0 failed free
  vmalloc bytes  used: 908585924 expensive: no

Kernel memory (kmem) statistics:
  Total memory  bytes  used: 185761552   peak: 486615148
  Allocations: 2204456 alloc, 0 failed alloc
               2162587 free, 0 failed free
  External Allocations: 0 for packets, 7303643 for SXL

Cookies:
        91808 total, 0 alloc, 0 free,
        2 dup, 91808 get, 0 put,
        182258 len, 909 cached len, 0 chain alloc,
        0 chain free

Connections:
        0 total, 0 TCP, 0 UDP, 0 ICMP,
        0 other, 0 anticipated, 0 recovered, -3 concurrent,
        0 peak concurrent

Fragments:
        0 fragments, 0 packets, 0 expired, 0 short,
        0 large, 0 duplicates, 0 failures

NAT:
        0/0 forw, 0/0 bckw, 0 tcpudp,
        0 icmp, 0-0 alloc

Sync: Run "cphaprob syncstat" for cluster sync statistics.

[Expert@MyGW:0]#
```

fw ctl set

Description

Configures the specified value for the specified kernel parameter.

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- In a VSX Gateway, the configured values of kernel parameters apply to all existing Virtual Systems and Virtual Routers.
- The configuration made with this command **without** the "`-f`" flag does **not** survive reboot.
  To make this configuration permanent, you must edit one of the applicable configuration files:
  - `$FWDIR/boot/modules/fwkern.conf`
  - `$PPKDIR/conf/simkern.conf`
- For the complete procedure, see *"Working with Kernel Parameters" on page 2021*.

Notes:

- Kernel parameters control the advanced behavior of your Security Gateway.
- There are two types of kernel parameters - *integer* and *string*.
- Security Gateway gets the names and the default values of the kernel parameters from these kernel module files:
  - `$FWDIR/boot/modules/fw_kern_64_3_10_64.o`
  - `$FWDIR/boot/modules/fw_kern_64_3_10_64_v6.o`
  - `$FWDIR/boot/modules/fw_kern_64_3_10_64_sp.o`
  - `$FWDIR/boot/modules/fw_kern_64_3_10_64_sp_v6.o`
  - `$PPKDIR/boot/modules/adp_kern_64_3_10_64.o`
  - `$PPKDIR/boot/modules/sim_kern_64_3_10_64.o`
  - `$PPKDIR/boot/modules/sim_kern_64_3_10_64_v6.o`
- Refer to the related command *"fw ctl get" on page 1100*.
- Refer to the related article sk33156: Creating a file with all the kernel parameters and their values.

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
fw [-d] ctl set [-f] int <Name of Integer Kernel Parameter>
<Integer Value>
```

```
fw [-d] ctl set [-f] str <Name of String Kernel Parameter>
'<String Value>'
```

Syntax on a Scalable Platform Security Group in the Expert mode

On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

- To make the change only in the current session (does not survive reboot):

```
g_fw [-d] ctl set int <Name of Integer Kernel Parameter>
<Integer Value>
```

```
g_fw [-d] ctl set str <Name of String Kernel Parameter>
'<String Value>'
```

- To make the change that survives reboot:

```
g_update_conf_file <Path to File> <Name of Integer Kernel
Parameter>=<Integer Value>
```

```
g_update_conf_file <Path to File> <Name of String Kernel
Parameter>='<String Value>'
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-f`	Automatically makes the required changes in the corresponding configuration file to survive reboot: ■ `$FWDIR/boot/modules/fwkern.conf` ■ `$PPKDIR/conf/simkern.conf` This flag does not apply to Scalable Platforms.
<Name of Integer Kernel Parameter>	Specifies the name of the integer kernel parameter.
<Integer Value>	Specifies the integer value for the integer kernel parameter.
<Name of String Kernel Parameter>	Specifies the name of the string kernel parameter.
'<String Value>'	Specifies the string value for the string kernel parameter.
<Path to File>	Specifies the path to the configuration file on Scalable Platforms: ■ `$FWDIR/boot/modules/fwkern.conf` ■ `$PPKDIR/conf/simkern.conf`

Example for an integer kernel parameter (does not survive reboot)

```
[Expert@MyGW:0]# fw ctl get int fw_kdprintf_limit
fw_kdprintf_limit = 100
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl set int fw_kdprintf_limit 50
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl get int fw_kdprintf_limit
fw_kdprintf_limit = 50
[Expert@MyGW:0]#
```

Example for an integer kernel parameter (survives reboot)

```
[Expert@MyGW:0]# fw ctl get int fw_kdprintf_limit
fw_kdprintf_limit = 100
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl set -f int fw_kdprintf_limit 50
"fwkern.conf" was updated successfully
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl get int fw_kdprintf_limit
fw_kdprintf_limit = 50
[Expert@MyGW:0]#
```

Example for a string kernel parameter

```
[Expert@MyGW:0]# fw ctl set str icap_unwrap_append_header_str '__print__'
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl get str icap_unwrap_append_header_str
icap_unwrap_append_header_str = '__print__'
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl set str icap_unwrap_append_header_str ''
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl get str icap_unwrap_append_header_str
icap_unwrap_append_header_str = ''
[Expert@MyGW:0]#
```

fw ctl tcpstrstat

Description

Generates statistics report about TCP Streaming.

Syntax

```
fw [-d] ctl tcpstrstat
       [-p]
       [-r]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-p`	Shows verbose statistics.
`-r`	Resets the counters.

Example 1 - Default output

```
[Expert@MyGW:0]# fw ctl tcpstrstat

General Counters:
=================
 Connections:
   Concurrent num of connections .............  0
   Concurrent num of si connections ..........  0
 Packets:
   Total num of packets ......................  2567
   Total packets in bytes ....................  202394
   Concurrent num of async packets ...........  0
 Memory:
   Allocated memory in bytes .................  0
   Referenced skbuffs num ....................  0
   Referenced skbuffs size in bytes ..........  0
   External packet references.................  0
   Allocated memory per connection ...........  0
 Rejected packets/connections:
   Total num of rejected packets .............  0
 Dropped packets/connections:
   Total num of dropped packets ..............  0
 Stripped/Truncated packets:
   Total num of stripped packets .............  0
   Total num of truncated packets ............  0
 Paused packets:
   Total num of c2s|s2c paused packets .......  0 | 0
   Concurrent num of UDP held packets ........  0

Applications Counters:
======================
 Application Name: ASPII_MT
  Connections:
   Total num of connections ..................  954
   Concurrent num of connections .............  0
   Total num of c2s|s2c connections ..........  954 | 954
   Concurrent num of c2s|s2c connections .....  0 | 0
  Packets:
   Total num of c2s|s2c data packets .........  2567 | 0
   Total c2s|s2c data packets in bytes .......  130518 | 0

FastForward Counters:
=====================
  FF connection:
   Total num of c2s|s2c FFconns ..............  0 | 0
   Total num of c2s|s2c saved packets ........  0 | 0
   Total num of c2s|s2c bytes requests .......  0 | 0
   Total num of c2s|s2c saved bytes ..........  0 | 0

[Expert@MyGW:0]#
```

fw ctl uninstall

Description

1. Tells the operating system to stop passing packets to Firewall.
2. Unloads the current Security Policy.
3. Unloads the current Firewall Chain Modules (see *"fw ctl chain" on page 1084*).
4. Unloads the current Firewall Connection Modules except for `RTM` (see *"fw ctl conn" on page 1086*).

Warnings:

1. If you run the "`fw ctl uninstall`" command, the networks behind the Security Gateway become unprotected.
2. If you run the "`fw ctl uninstall`" command and then the *"fw ctl install" on page 1103* command, it does not restore the Security Policy.
   You must run one of these commands: *"fw fetch" on page 1119*, or *"cpstart" on page 1018*.

Syntax

```
fw [-d] ctl uninstall
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.

fw defaultgen

Description

Manually generates the Default Filter policy files.

Refer to these related commands:

- *"comp_init_policy" on page 965*
- *"control_bootsec" on page 973*
- *"fwboot default" on page 1266*
- *"fwboot bootconf" on page 1253*

Syntax

```
fw [-d] defaultgen
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.

`defaultgen`	Generates the Default Filter policy files:
	■ For IPv4 traffic:
	`$FWDIR/state/default.bin`
	■ For IPv6 traffic:
	`$FWDIR/state/default.bin6`
	If the Default Filter policy file already exists, the command creates a backup copy (`$FWDIR/state/default.bin.bak` and `$FWDIR/state/default.bin6.bak`).

Example

```
[Expert@MyGW:0]# fw defaultgen
Generating default filter
defaultfilter:
Compiled OK.
defaultfilter:
Compiled OK.
 Backing up default.bin as default.bin.bak
 hostaddr(MyGW) failed
 Backing up default.bin6 as default.bin6.bak
[Expert@MyGW:0]#
```

fw fetch

Description

Fetches the Security Policy from the specified host and installs it to the kernel.

Syntax

- To fetch the policy from the Management Server:

```
fw [-d] fetch -f [-i] [-n] [-r]
```

- To fetch the policy from a peer Cluster Member, and, if it fails, then from the Management Server:

```
fw [-d] fetch -f -c [-i] [-n] [-r]
```

- To fetch the policy from the specified Check Point server(s):

```
fw [-d] fetch [-i] [-n] [-r] <Master 1> [<Master 2> ...]
```

- To fetch the policy stored locally on the Security Gateway in the default directory `$FWDIR/state/`:

```
fw [-d] fetch local [-nu]
fw [-d] fetch localhost [-nu]
```

- To fetch the policy stored locally on the Security Gateway in the specified directory:

```
fw [-d] fetchlocal -d <Full Path to Directory>
```

Parameters

Parameter	Description
`fw -d fetch...`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.

Parameter	Description
`-c`	Specifies that you fetch the policy from a peer Cluster Member. **Notes:** ■ Must also use the "`-f`" parameter. ■ Works only in cluster.
`-f`	Specifies that you fetch the policy from a Management Server listed in the `$FWDIR/conf/masters` file.
`-i`	On a Security Gateway with dynamically assigned IP address (DAIP), specifies to ignore the SIC name and object name.
`-n`	Specifies not to load the fetched policy, if it is the same as the policy already located on the Security Gateway.
`-nu`	Specifies not to update the currently installed policy.
`-r`	On a Cluster Member, specifies to ignore this option in SmartConsole **Install Policy** window: **For gateway clusters, if installation on a cluster member fails, do not install on that cluster** **Best Practice** - Use this parameter if a peer Cluster Member is **Down**.

Parameter	Description
`<Master 1> [<Master 2> ...]`	Specifies the Check Point server(s), from which to fetch the policy. You can fetch the policy from the Management Server, or a peer Cluster Member. **Notes:** ■ If you fetch the policy from the Management Server, you can enter one of these: • The main IP address of the Management Server object. • The object name of the Management Server. • The hostname that the Security Gateway resolves to the main IP address of the Management Server. ■ If you fetch the policy from a peer Cluster Member, you can enter one of these: • The main IP address of the Cluster Member object. • The IP address of the Sync interface on the Cluster Member. ■ If the fetch from the first specified `<Master>` fails, the Security Gateway fetches the policy from the second specified `<Master>` , and so on. If the Security Gateway fails to connect to each specified `<Masters>`, the Security Gateway fetches the policy from the `localhost`. ■ If you do not specify the `<Masters>` explicitly, the Security Gateway fetches the policy from the `localhost`.
`-d <Full Path to Directory>`	Specifies the local directory on the Security Gateway, from which to fetch the policy files.

fw fetchlogs

Description

Fetches the specified Security log files (`$FWDIR/log/*.log*`) or Audit log files (`$FWDIR/log/*.adtlog*`) from the specified Check Point server.

Important - You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).

Syntax

```
fw [-d] fetchlogs [-f <Name of Log File 1>] [-f <Name of Log File 2>]... [-f <Name of Log File N>] <Target>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-f <Name of Log File N>`	Specifies the name of the log file to fetch. Need to specify name only. **Notes:** ■ If you do not specify the log file name explicitly, the command transfers all Security log files (`$FWDIR/log/*.log*`) and all Audit log files (`$FWDIR/log/*.adtlog*`). ■ The specified log file name can include wildcards * and ? (for example, `2017-0?-*.log`). If you enter a wildcard, you must enclose it in double quotes or single quotes. ■ You can specify multiple log files in one command. You must use the `-f` parameter for each log file name pattern. ■ This command also transfers the applicable log pointer files.
`<Target>`	Specifies the remote Check Point server, with which this local Check Point server has established SIC trust. **Notes:** ■ The local and the remote servers must have established SIC trust. ■ The local server can be a Security Management Server, a Log Server, a Cluster Member. ■ The remote server can be a Security Gateway, a Cluster Member, a Log Server, or a Security Management Server in High Availability deployment. ■ You can specify the remote managed server by its main IP address or Object Name as configured in SmartConsole.

Notes:

- This command moves the specified log files from the `$FWDIR/log/` directory on the specified Check Point server.

  Meaning, it deletes the specified log files on the specified Check Point server after it copies them successfully.

- This command moves the specified log files to the `$FWDIR/log/` directory on the local Check Point server, on which you run this command.

- This command cannot fetch the *active* log files `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`.

  To fetch these active log files:

  1. Perform the log switch on the applicable Check Point server:

     See *"fw logswitch" on page 284*.

     ```
     fw logswitch [-audit] [-h <IP Address or Hostname>]
     ```

  2. Fetch the rotated log file from the applicable Check Point server:

     ```
     fw fetchlogs -f <Log File Name> <IP Address or Hostname>
     ```

- This command renames the log files it fetched from the specified Check Point server.

  The new log file name is the concatenation of these:

  - The Check Point server's name (as configured in SmartConsole).
  - Two underscore (_) characters.
  - The original log file name

  Example: `MyGW__2019-06-01_000000.log`

Example - Fetching log files from a Management Server

```
[Expert@HostName:0]# fw lslogs MyGW
     Size Log file name
        23KB 2019-05-16_000000.log
         9KB 2019-05-17_000000.log
        11KB 2019-05-18_000000.log
      5796KB 2019-06-01_000000.log
      4610KB fw.log
[Expert@HostName:0]#

[Expert@HostName:0]# fw fetchlogs -f 2019-06-01_000000 MyGW
File fetching in process. It may take some time...
File MyGW__2019-06-01_000000.log was fetched successfully
[Expert@HostName:0]#

[Expert@HostName:0]# ls $FWDIR/log/MyGW*
/opt/CPsuite-R81.20/fw1/log/MyGW__2019-06-01_000000.log
/opt/CPsuite-R81.20/fw1/log/MyGW__2019-06-01_000000.logaccount_ptr
/opt/CPsuite-R81.20/fw1/log/MyGW__2019-06-01_000000.loginitial_ptr
/opt/CPsuite-R81.20/fw1/log/MyGW__2019-06-01_000000.logptr
[Expert@HostName:0]#

[Expert@HostName:0]# fw lslogs MyGW
     Size Log file name
        23KB 2019-05-16_000000.log
         9KB 2019-05-17_000000.log
        11KB 2019-05-18_000000.log
      4610KB fw.log
[Expert@HostName:0]#
```

fw getifs

Description

Shows the list with this information:

- The name of interfaces, to which the Check Point Firewall kernel attached.
- The IP addresses assigned to the interfaces.

Notes:

- This list shows only interfaces that have IP addresses assigned on them.
- Related *"cpstat" on page 1019* commands:
  - `cpstat -f ifconfig os`
  - `cpstat -f interfaces fw`

Syntax

```
fw [-d] getifs
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.

Example

```
[Expert@MyGW:0]# fw getifs
localhost eth0 192.168.30.40 255.255.255.0
localhost eth1 172.30.60.80 255.255.255.0
[Expert@MyGW:0]#
```

fw hastat

Description

Shows information about Check Point computers in High Availability configuration and their states.

Note - This command is outdated. On cluster members, run the Gaia Clish command "`show cluster state`", or the Expert mode command "`cphaprob state`".

Note - This command is outdated. On Management Servers, run the *"cpstat" on page 209* command.

Syntax

```
fw hastat [<Target1>] [<Target2>] ... [<TargetN>]
```

Parameters

Parameter	Description
<Target1> *<Target2>* ... *<TargetN>*	Specifies the Check Point computers to query. If you run this command on the Management Server, you can enter the applicable IP address, or the resolvable HostName of the managed Security Gateway or Cluster Member. If you do not specify the target, the command queries the local computer.

Example - Querying the cluster members from the Management Server

```
[Expert@MGMT:0]# fw hastat 192.168.3.52
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.52 1 active OK
[Expert@MGMT:0]#

[Expert@MGMT:0]# fw hastat 192.168.3.53
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.53 2 stand-by OK
[Expert@MGMT:0]#

[Expert@MGMT:0]# fw hastat 192.168.3.52 192.168.3.53
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.52 1 active OK
192.168.3.53 2 stand-by OK
[Expert@MGMT:0]#
```

Example - Querying the local Cluster Member

```
[Expert@Member1:0]# fw hastat
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.52 1 active OK
[Expert@Member1:0]#
```

fw isp_link

Description

Controls the state of ISP Links in the ISP Redundancy configuration on Security Gateway.

See the *R81.20 Security Gateway Guide*.

Syntax

```
fw [-d] isp_link
      {-h | -help}
      [<Name of Object>] <Name of ISP Link>
      down
      up
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{-h | -help}`	Shows the built-in usage.
<Name of Object>	Only when you run this command on a Management Server: The name of the Security Gateway or Cluster Member object as defined in SmartConsole (from the left navigation panel, click **Gateways & Servers**).
<Name of ISP Link>	The name of the ISP Link as defined in the Security Gateway or Cluster object: 1. In SmartConsole, from the left navigation panel, click **Gateways & Servers**. 2. Open the Security Gateway or Cluster object. 3. From the left tree, click **Other > ISP Redundancy**.
`down`	Changes the state of the specified ISP Link to DOWN.
`up`	Changes the state of the specified ISP Link to UP.

fw kill

Description

Kills the specified Check Point processes.

Important:

- Make sure the killed process is restarted, or restart it manually. See sk97638.
- You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).

Syntax

```
fw [-d] kill [-t <Signal Number>] <Name of Process>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-t <Signal Number>`	Specifies which signal to send to the Check Point process. For the list of available signals and their numbers, run the `kill -l` command. For information about the signals, see the manual pages for the `kill` and `signal`. If you do not specify the signal explicitly, the command sends Signal 15 (`SIGTERM`). **Note** - Processes can ignore some signals.
`<Name of Process>`	Specifies the name of the Check Point process to kill. To see the names of the processes, run the `ps auxwf` command.

Example

```
fw kill fwd
```

fw lichosts

Description

Shows IP addresses of internal hosts that Security Gateway detected and counted based on the installed license.

Syntax

```
fw [-d] lichosts [-l] [-x]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-l`	Shows the output in the long format.
`-x`	Shows the output in the hexadecimal format.

Example

```
[Expert@MyGW:0]# fw lichosts
License allows an unlimited number of hosts
[Expert@MyGW:0]
```

Related SK article

sk10200 - 'too many internal hosts' error in /var/log/messages on Security Gateway.

fw log

Description

Shows the content of Check Point log files - Security (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`).

Important - You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).

Syntax

```
fw log {-h | -help}
```

```
fw [-d] log [-a] [-b "<Start Timestamp>" "<End Timestamp>"] [-c
<Action>] [{-f | -t}] [-g] [-H] [-h <Origin>] [-i] [-k {<Alert
Name> | all}] [-l] [-m {initial | semi | raw}] [-n] [-o] [-p] [-q]
[-S] [-s "<Start Timestamp>"] [-e "<End Timestamp>"] [-u
<Unification Scheme File>] [-w] [-x <Start Entry Number>] [-y <End
Entry Number>] [-z] [-#] [<Log File>]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the built-in usage. **Note** - The built-in usage does not show some of the parameters described in this table.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-a`	Shows only Account log entries.

Parameter	Description
`-b "<Start Timestamp>" "<End Timestamp>"`	Shows only entries that were logged between the specified start and end times. ■ The *<Start Timestamp>* and *<End Timestamp>* may be a date, a time, or both. ■ If date is omitted, then the command assumes the current date. ■ Enclose the "*<Start Timestamp>*" and "*<End Timestamp>* in single or double quotes (`-b 'XX' 'YY'`", or `-b "XX" "YY`). ■ You cannot use the "`-b`" parameter together with the "`-s`" or "`-e`" parameters. ■ See the date and time format below.
`-c <Action>`	Shows only events with the specified action. One of these: ■ `accept` ■ `drop` ■ `reject` ■ `encrypt` ■ `decrypt` ■ `vpnroute` ■ `keyinst` ■ `authorize` ■ `deauthorize` ■ `authcrypt` ■ `ctl` **Notes:** ■ The `fw log` command always shows the **Control** (`ctl`) actions. ■ For *login* action, use the `authcrypt`.
`-e "<End Timestamp>"`	Shows only entries that were logged before the specified time. **Notes:** ■ The *<End Timestamp>* may be a date, a time, or both. ■ Enclose the *<End Timestamp>* in single or double quotes (`-e '...'`, or `-e "..."`). ■ You cannot use the "`-e`" parameter together with the "`-b`" parameter. ■ See the date and time format below.

Parameter	Description
`-f`	This parameter: 1. Shows the saved entries that match the specified conditions. 2. After the command reaches the end of the currently opened log file, it continues to monitor the log file indefinitely and shows the new entries that match the specified conditions. **Note** - Applies only to the *active* log file `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`
`-g`	Does not show delimiters. The default behavior is: ■ Show a colon (`:`) after a field name ■ Show a semi-colon (`;`) after a field value
`-H`	Shows the High Level Log key.
`-h <Origin>`	Shows only logs that were generated by the Security Gateway with the specified IP address or object name (as configured in SmartConsole).
`-i`	Shows log UID.
`-k {<Alert Name> | all}`	Shows entries that match a specific alert type: ■ *<Alert Name>* - Show only entries that match a specific alert type: • `alert` • `mail` • `snmp_trap` • `spoof` • `user_alert` • `user_auth` ■ `all` - Show entries that match all alert types (this is the default).
`-l`	Shows both the date and the time for each log entry. The default is to show the date only once above the relevant entries, and then specify the time for each log entry.

Parameter	Description
`-m`	Specifies the log unification mode: ■ `initial` - Complete unification of log entries. The command shows one unified log entry for each ID. This is the default. If you also specify the `-f` parameter, then the output does not show any updates, but shows only entries that relate to the start of new connections. To shows updates, use the `semi` parameter. ■ `semi` - Step-by-step unification of log entries. For each log entry, the output shows an entry that unifies this entry with all previously encountered entries with the same ID. ■ `raw` - No log unification. The output shows all log entries.
`-n`	Does not perform DNS resolution of the IP addresses in the log file (this is the default behavior). This significantly speeds up the log processing.
`-o`	Shows detailed log chains - shows all the log segments in the log entry.
`-p`	Does not perform resolution of the port numbers in the log file (this is the default behavior). This significantly speeds up the log processing.
`-q`	Shows the names of log header fields.
`-S`	Shows the Sequence Number.
`-s "<Start Timestamp>"`	Shows only entries that were logged after the specified time. **Notes:** ■ The *<Start Timestamp>* may be a date, a time, or both. ■ If the date is omitted, then the command assumed the current date. ■ Enclose the *<Start Timestamp>* in single or double quotes (`-s '...'`, or `-s "..."`). ■ You cannot use the "`-s`" parameter together with the "`-b`" parameter. ■ See the date and time format below.

Parameter	Description
`-t`	This parameter: 1. Does not show the saved entries that match the specified conditions. 2. After the command reaches the end of the currently opened log file, it continues to monitor the log file indefinitely and shows the new entries that match the specified conditions. **Note** - Applies only to the *active* log file `$FWDIR/log/fw.log` or `$FWDIR/log/fw.adtlog`
`-u <Unification Scheme File>`	Specifies the path and name of the log unification scheme file. The default log unification scheme file is: `$FWDIR/conf/log_unification_scheme.C`
`-w`	Shows the flags of each log entry (different bits used to specify the "nature" of the log - for example, control, audit, accounting, complementary, and so on).
`-x <Start Entry Number>`	Shows only entries from the specified log entry number and below, counting from the beginning of the log file.
`-y <End Entry Number>`	Shows only entries until the specified log entry number, counting from the beginning of the log file.
`-z`	In case of an error (for example, wrong field value), continues to show log entries. The default behavior is to stop.
`-#`	Show confidential logs in clear text.
`<Log File>`	Specifies the log file to read. If you do not specify the log file explicitly, the command opens the `$FWDIR/log/fw.log` log file. You can specify a switched log file.

Date and Time format

Part of timestamp	Format	Example
Date only	`MMM DD, YYYY`	`June 11, 2018`
Time only Note - In this case, the command assumes the current date.	`HH:MM:SS`	`14:20:00`
Date and Time	`MMM DD, YYYY HH:MM:SS`	`June 11, 2018 14:20:00`

Output

Each output line consists of a single log entry, whose fields appear in this format:

Note - The fields that show depends on the connection type.

```
HeaderDateHour ContentVersion HighLevelLogKey Uuid SequenceNum
Flags Action Origin IfDir InterfaceName LogId ...
```

This table describes some of the fields.

Field Header	Description	Example
`HeaderDateHour`	Date and Time	`12Jun2018 12:56:42`
`ContentVersion`	Version	`5`
`HighLevelLogKey`	High Level Log Key	`<max_null>`, or empty
`Uuid`	Log UUID	`(0x5b1f99cb,0x0,0x3403a8c0,0xc0000000)`
`SequenceNum`	Log Sequence Number	`1`

Field Header	Description	Example
`Flags`	Internal flags that specify the "nature" of the log - for example, control, audit, accounting, complementary, and so on	`428292`
`Action`	Action performed on this connection	■ `accept` ■ `dropreject` ■ `encrypt` ■ `decrypt` ■ `vpnroute` ■ `keyinst` ■ `authorize` ■ `deauthorize` ■ `authcrypt` ■ `ctl`
`Origin`	Object name of the Security Gateway that generated this log	`MyGW`
`IfDir`	Traffic direction through interface: ■ `<` - Outbound (sent by a Security Gateway) ■ `>` - Inbound (received by a Security Gateway)	■ `<` ■ `>`

Field Header	Description	Example
`InterfaceName`	Name of the Security Gateway interface, on which this traffic was logged If a Security Gateway performed some internal action (for example, log switch), then the log entry shows `daemon`	■ `eth0` ■ `daemon` ■ `N/A`
`LogId`	Log ID	`0`
`Alert`	Alert Type	■ `alert` ■ `mail` ■ `snmp_trap` ■ `spoof` ■ `user_alert` ■ `user_auth`
`OriginSicName`	SIC name of the Security Gateway that generated this log	`CN=MyGW,O=MyDomain_ Server.checkpoint.com.s6t98x`
`inzone`	Inbound Security Zone	`Local`
`outzone`	Outbound Security Zone	`External`
`service_id`	Name of the service used to inspect this connection	`ftp`
`src`	Object name or IP address of the connection's source server	`MyHost`

Field Header	Description	Example
dst	Object name or IP address of the connection's destination server	MyFTPServer
proto	Name of the connection's protocol	tcp
sport_svc	Source port of the connection	64933
ProductName	Name of the Check Point product that generated this log	■ VPN-1 & FireWall-1 ■ Application Control ■ FloodGate-1
ProductFamily	Name of the Check Point product family that generated this log	Network

Examples

Example 1 - Show all log entries with both the date and the time for each log entry

```
fw log -l
```

Example 2 - Show all log entries that start after the specified timestamp

```
[Expert@MyGW:0]# fw log -l -s "June 12, 2018 12:33:00"
 12Jun2018 12:33:00 5 N/A 1 accept MyGW > N/A LogId: <max_null>; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; fg-1_client_in_rule_name: Default; fg-1_client_out_rule_name: Default; fg-1_server_in_rule_name: Host
Redirect; fg-1_server_out_rule_name: ; ProductName: FG; ProductFamily: Network;

 12Jun2018 12:33:39 5 N/A 1 drop MyGW < eth0 LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; inzone: Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_
table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid: 4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_
uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_table: TABLE_END; UP_action_table: TABLE_START; ROW_
START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc: ftp; sport_svc: 64933;
ProductFamily: Network;

... ... ...

[Expert@MyGW:0]#
```

Example 3 - Show all log entries between the specified timestamps

```
[Expert@MyGW:0]# fw log -l -b "June 12, 2018 12:33:00" 'June 12, 2018 12:34:00'
 12Jun2018 12:33:00 5 N/A 1 accept MyGW > N/A LogId: <max_null>; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; fg-1_client_in_rule_name: Default; fg-1_client_out_rule_name: Default; fg-1_server_in_rule_name: Host
Redirect; fg-1_server_out_rule_name: ; ProductName: FG; ProductFamily: Network;

 12Jun2018 12:33:39 5 N/A 1 drop MyGW < eth0 LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; inzone: Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_
table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid: 4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_
uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_table: TABLE_END; UP_action_table: TABLE_START; ROW_
START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc: ftp; sport_svc: 64933;
ProductFamily: Network;

 12Jun2018 12:33:45 5 N/A 1 ctl MyGW > LogId: <max_null>; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; description: Contracts; reason: Could not reach
"https://productcoverage.checkpoint.com/ProductCoverageService". Check DNS and Proxy configuration on the gateway.; Severity: 2;
status: Failed; version: 1.0; failure_impact: Contracts may be out-of-date; update_service: 1; ProductName: Security
Gateway/Management; ProductFamily: Network;
[Expert@MyGW:0]#
```

Example 4 - Show all log entries with action "drop"

```
[Expert@MyGW:0]# fw log -l -c drop
 12Jun2018 12:33:39 5 N/A 1 drop MyGW < eth0 LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; inzone: Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_
table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid: 4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_
uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_table: TABLE_END; UP_action_table: TABLE_START; ROW_
START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc: ftp; sport_svc: 64933;
ProductFamily: Network;
[Expert@MyGW:0]#
```

Example 5 - Show all log entries with action "drop", show all field headers, and show log flags

```
[Expert@MyGW:0]# fw log -l -q -w -c drop
 HeaderDateHour: 12Jun2018 12:33:39; ContentVersion: 5; HighLevelLogKey: <max_null>; LogUid: ; SequenceNum: 1; Flags: 428292; Action:
drop; Origin: MyGW; IfDir: <; InterfaceName: eth0; Alert: ; LogId: 0; ContextNum: <max_null>; OriginSicName: CN=MyGW,O=MyDomain_
Server.checkpoint.com.s6t98x; inzone: Local; outzone: External; service_id: ftp; src: MyGW; dst: MyFTPServer; proto: tcp; UP_match_
table: TABLE_START; ROW_START: 0; match_id: 2; layer_uuid: 4e26fc30-b345-4c96-b8d7-9db6aa7cdd89; layer_name: MyPolicy Network; rule_
uid: 802020d9-5cdc-4c74-8e92-47e1b0eb72e5; rule_name: ; ROW_END: 0; UP_match_table: TABLE_END; UP_action_table: TABLE_START; ROW_
START: 0; action: 0; ROW_END: 0; UP_action_table: TABLE_END; ProductName: VPN-1 & FireWall-1; svc: ftp; sport_svc: 64933;
ProductFamily: Network;
[Expert@MyGW:0]#
```

Example 6 - Show only log entries from 0 to 10 (counting from the beginning of the log file)

```
[Expert@MyGW:0]# fw log -l -x 0 -y 10
... ...
[Expert@MyGW:0]#
```

fw logswitch

Description

Switches the current active log file:

1. Closes the current active log file.
2. Renames the current active log file.
3. Creates a new active log file with the default name.

Notes:

- By default, this command switches the active Security log file - `$FWDIR/log/fw.log`
- You can specify to switch the active Audit log file - `$FWDIR/log/fw.adtlog`

Important You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).

Syntax

```
fw [-d] logswitch
      [-audit] [<Name of Switched Log>]
      -h <Target> [[+ | -]<Name of Switched Log>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-audit`	Specifies to switch the active Audit log file (`$FWDIR/log/fw.adtlog`). You can use this parameter only on a Management Server.

Parameter	Description
`-h <Target>`	Specifies the remote server, on which to switch the log. **Notes:** ■ The local and the remote servers must have established SIC trust. ■ The local server can be a Security Management Server, a Log Server. ■ The remote server can be a Security Gateway, a Log Server, or a Security Management Server in High Availability deployment. ■ You can specify the remote managed server by its main IP address or Object Name as configured in SmartConsole.

`<Name of Switched Log>`	Specifies the name of the switched log file.
	Notes:
	■ If you do not specify this parameter, then a default name is:
	`<YYYY-MM-DD_HHMMSS>.log`
	`<YYYY-MM-DD_HHMMSS>.adtlog`
	For example, *2018-03-26_174455.log*
	■ If you specify the name of the switched log file, then the name of the switch log file is:
	`<Specified_Log_Name>.log`
	`<Specified_Log_Name>.adtlog`
	■ The log switch operation fails if the specified name for the switched log matches the name of an existing log file.
	■ The maximum length of the specified name of the switched log file is 230 characters.

`+`	Specifies to *copy* the active log from the remote server to the local server.
	Notes:
	■ If you specify the name of the switched log file, you must write it immediately after *this* + (plus) parameter.
	■ The command copies the active log from the remote server and saves it in the `$FWDIR/log/` directory on the local server.
	■ The default name of the saved log file is:
	`<Gateway_Object_Name>__<YYYY-MM-DD_HHMMSS>.log`
	For example, *MyGW__2018-03-26_174455.log*
	■ If you specify the name of the switched log file, then the name of the saved log file is:
	`<Gateway_Object_Name>__<Specified_Log_Name>.log`
	■ When this command copies the log file from the remote server, it compresses the file.

Parameter	Description
-	Specifies to *transfer* the active log from the remote server to the local server. **Notes:** ■ The command saves the copied active log file in the `$FWDIR/log/` directory on the local server and then deletes the switched log file on the remote server. ■ If you specify the name of the switched log file, you must write it immediately after this - (minus) parameter. ■ The default name of the saved log file is: `<Gateway_Object_Name>__<YYYY-MM-DD_HHMMSS>.log` For example, *MyGW__2018-03-26_174455.log* ■ If you specify the name of the switched log file, then the name of the saved log file is: `<Gateway_Object_Name>__<Specified_Log_Name>.log` ■ When this command transfers the log file from the remote server, it compresses the file. ■ As an alternative, you can use the *"fw fetchlogs" on page 268* command.

Compression

When this command transfers the log files from the remote server, it compresses the file with the `gzip` command (see RFC 1950 to RFC 1952 for details). The algorithm is a variation of LZ77 method. The compression ratio varies with the content of the log file and is difficult to predict. Binary data are not compressed. Text data, such as user names and URLs, are compressed.

Example - Switching the active Security log on a Security Management Server or Security Gateway

```
[Expert@MGMT:0]# fw logswitch
Log file has been switched to: 2018-06-13_182359.log
[Expert@MGMT:0]#
```

Example - Switching the active Audit log on a Security Management Server

```
[Expert@MGMT:0]# fw logswitch -audit
Log file has been switched to: 2018-06-13_185711.adtlog
[Expert@MGMT:0]#
```

Example - Switching the active Security log on a managed Security Gateway and copying the switched log

```
[Expert@MGMT:0]# fw logswitch -h MyGW +
Log file has been switched to: 2018-06-13_185451.log
[Expert@MGMT:0]#
[Expert@MGMT:0]# ls $FWDIR/log/*.log
/opt/CPsuite-R81.20/fw1/log/fw.log
/opt/CPsuite-R81.20/fw1/log/MyGW__2018-06-13_185451.log
[Expert@MGMT:0]#

[Expert@MyGW:0]# ls $FWDIR/log/*.log
/opt/CPsuite-R81.20/fw1/log/fw.log
/opt/CPsuite-R81.20/fw1/log/2018-06-13_185451.log
[Expert@MyGW:0]#
```

fw lslogs

Description

Shows a list of Security log files (`$FWDIR/log/*.log`) and Audit log files (`$FWDIR/log/*.adtlog`) residing on the local server or a remote server.

Important - You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).

Syntax

```
fw [-d] lslogs [-f <Name of Log File 1>] [-f <Name of Log File 2>]
... [-f <Name of Log File N>] [-e] [-r] [-s {name | size | stime |
etime}] [<Target>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-f <Name of Log File>`	Specifies the name of the log file to show. Need to specify only the name. **Notes:** ■ If the log file name is not specified explicitly, the command shows all Security log files (`$FWDIR/log/*.log`). ■ File names may include `*` and `?` as wildcards (for example, `2019-0?-*`). If you enter a wildcard, you must enclose it in double quotes or single quotes. ■ You can specify multiple log files in one command. You must use the "`-f`" parameter for each log file name pattern: `-f <Name of Log File 1> -f <Name of Log File 2> ... -f <Name of Log File N>`

Parameter	Description
`-e`	Shows an extended file list. It includes the following information for each log file: ■ `Size` - The total size of the log file and its related pointer files ■ `Creation Time` - The time the log file was created ■ `Closing Time` - The time the log file was closed ■ `Log File Name` - The file name
`-r`	Reverses the sort order (descending order).
`-s {name | size | stime | etime}`	Specifies the sort order of the log files using one of the following sort options: ■ `name` - The file name ■ `size` - The file size ■ `stime` - The time the log file was created (this is the default option) ■ `etime` - The time the log file was closed
<Target>	Specifies the remote Check Point server, with which this local Check Point server has established SIC trust. **Notes:** ■ The local and the remote servers must have established SIC trust. ■ The local server can be a Security Management Server, a Log Server, a Security Gateway, a Cluster Member. ■ The remote server can be a Security Gateway, a Cluster Member, a Log Server, or a Security Management Server in High Availability deployment. ■ You can specify the remote managed server by its main IP address or Object Name as configured in SmartConsole.

Example 1 - Default output

```
[Expert@HostName:0]# fw lslogs
     Size Log file name
         9KB 2019-06-14_000000.log
        11KB 2019-06-15_000000.log
         9KB 2019-06-16_000000.log
        10KB 2019-06-17_000000.log
         9KB fw.log
[Expert@HostName:0]#
```

Example 2 - Showing all log files

```
[Expert@HostName:0]# fw lslogs -f "*"
     Size Log file name
          9KB fw.adtlog
          9KB fw.log
          9KB 2019-05-29_000000.adtlog
          9KB 2019-05-29_000000.log
          9KB 2019-05-20_000000.adtlog
          9KB 2019-05-20_000000.log
[Expert@HostName:0]#
```

Example 3 - Showing only log files specified by the patterns

```
[Expert@HostName:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*'
     Size Log file name
          9KB 2019-06-14_000000.adtlog
          9KB 2019-06-14_000000.log
         11KB 2019-06-15_000000.adtlog
         11KB 2019-06-15_000000.log
[Expert@HostName:0]#
```

Example 4 - Showing only log files specified by the patterns and their extended information

```
[Expert@HostName:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*'
     Size Log file name
          9KB 2019-06-14_000000.adtlog
          9KB 2019-06-14_000000.log
         11KB 2019-06-15_000000.adtlog
         11KB 2019-06-15_000000.log
[Expert@HostName:0]#
```

Example 5 - Showing only log files specified by the patterns, sorting by name in reverse order

```
[Expert@HostName:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*' -e -s name -r
     Size Creation Time Closing Time Log file name
        11KB 14Jun2018 0:00:00 15Jun2018 0:00:00 2019-06-15_000000.log
        11KB 14Jun2018 0:00:00 15Jun2018 0:00:00 2019-06-15_000000.adtlog
         9KB 13Jun2018 18:23:59 14Jun2018 0:00:00 2019-06-14_000000.log
         9KB 13Jun2018 0:00:00 14Jun2018 0:00:00 2019-06-14_000000.adtlog
[Expert@HostName:0]#
```

Example 6 - Showing only log files specified by the patterns, from a managed Security Gateway with main IP address 192.168.3.53

```
[Expert@MGMT:0]# fw lslogs -f "2019-06-14*" -f '2019-06-15*' 192.168.3.53
     Size Log file name
        11KB 2019-06-15_000000.adtlog
        11KB 2019-06-15_000000.log
         9KB 2019-06-14_000000.log
         9KB 2019-06-14_000000.adtlog
[Expert@MGMT:0]#
```

fw mergefiles

Description

Merges several Security log files (`$FWDIR/log/*.log`) into a single log file.

Merges several Audit log files (`$FWDIR/log/*.adtlog`) into a single log file.

Important:

- Do **not** merge the *active* Security file `$FWDIR/log/fw.log` with other Security switched log files.
  Switch the active Security file `$FWDIR/log/fw.log` (with the *"fw logswitch" on page 1141* command) and only then merge it with other Security switched log files.
- Do **not** merge the *active* Audit file `$FWDIR/log/fw.adtlog` with other Audit switched log files.
  Switch the active Audit file `$FWDIR/log/fw.adtlog` (with the *"fw logswitch" on page 1141* command) and only then merge it with other Audit switched log files.
- This command unifies logs entries with the same Unique-ID (UID). If you rotate the current active log file before all the segments of a specific log arrive, this command merges the records with the same Unique ID from two different files, into one fully detailed record.
- If the size of the final merged log file exceeds 2GB, this command creates a list of merged files, where the size of each merged file size is not more than 2GB.
  The user receives this warning:

  ```
  Warning: The size of the files you have chosen to merge
  is greater than 2GB. The merge will produce two or more
  files.
  ```

  The names of merged files are:
  - *<Name of Merged Log File>*`.log`
  - *<Name of Merged Log File>*`_1.log`
  - *<Name of Merged Log File>*`_2.log`
  - `... ...`
  - *<Name of Merged Log File>*`_N.log`

Important - You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).

Syntax

```
fw [-d] mergefiles {-h | -help}
```

```
fw [-d] mergefiles [-r] [-s] [-t <Time Conversion File>] <Name of Log File 1> <Name of Log File 2> ... <Name of Log File N> <Name of Merged Log File>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`{-h | -help}`	Shows the built-in usage.
`-r`	Removes duplicate entries.
`-s`	Sorts the merged file by the **Time** field in log records.

`-t <Time Conversion File>`	Specifies a full path and name of a file that instructs this command how to adjust the times during the merge.
	This is required if you merge log files from Log Servers configured with different time zones.
	The file format is:
	`<IP Address of Log Server #1> <Signed Date Time #1 in Seconds>`
	`<IP Address of Log Server #2> <Signed Date Time #2 in Seconds>`
	`... ...`
	Notes
	■ You must specify the absolute path and the file name.
	■ The name of the time conversion file cannot exceed 230 characters.

Parameter	Description
<Name of Log File 1> ... <Name of Log File N>	Specifies the log files to merge. **Notes:** ■ You must specify the absolute path and the name of the input log files. ■ The name of the input log file cannot exceed 230 characters.
<Name of Merged Log File>	Specifies the output merged log file. **Notes:** ■ The name of the merged log file cannot exceed 230 characters. ■ If a file with the specified name already exists, the command stops and asks you to remove the existing file, or to specify another name. ■ The size of the merged log file cannot exceed 2 GB. In such scenario, the command creates several merged log files, each not exceeding the size limit.

Example - Merging Security log files

```
[Expert@HostName:0]# ls -l $FWDIR/*.log
-rw-rw-r-- 1 admin root 189497 Sep  7 00:00 2019-09-07_000000.log
-rw-rw-r-- 1 admin root  14490 Sep  9 09:52 2019-09-09_000000.log
-rw-rw-r-- 1 admin root  30796 Sep 10 10:56 2019-09-10_000000.log
-rw-rw-r-- 1 admin root  24503 Sep 10 13:08 fw.log
[Expert@HostName:0]#
[Expert@HostName:0]# fw mergefiles -s $FWDIR/2019-09-07_000000.log $FWDIR/2019-09-09_000000.log
$FWDIR/2019-09-10_000000.log /var/log/2019-Sep-Merged.log
[Expert@HostName:0]#
[Expert@HostName:0]# ls -l /var/log/2019-Sep-Merged.log*
-rw-rw---- 1 admin root 213688 Sep 10 13:18 /var/log/2019-Sep-Merged.log
-rw-rw---- 1 admin root   8192 Sep 10 13:18 /var/log/2019-Sep-Merged.logLuuidDB
-rw-rw---- 1 admin root     80 Sep 10 13:18 /var/log/2019-Sep-Merged.logaccount_ptr
-rw-rw---- 1 admin root   2264 Sep 10 13:18 /var/log/2019-Sep-Merged.loginitial_ptr
-rw-rw---- 1 admin root   4448 Sep 10 13:18 /var/log/2019-Sep-Merged.logptr
[Expert@HostName:0]#
```

fw monitor

Description

Firewall Monitor is the Check Point traffic capture tool.

In a Security Gateway, traffic passes through different inspection points - Chain Modules in the Inbound direction and then in the Outbound direction (see *"fw ctl chain" on page 1084*).

The FW Monitor tool captures the traffic at each Chain Module in both directions.

You can later analyze the captured traffic with the same FW Monitor tool, or with special tools like Wireshark.

Notes:

- Only one instance of "`fw monitor`" can run at a time.
- You can stop the "`fw monitor`" instance in one of these ways:
  - In the shell, in which the "`fw monitor`" instance runs, press **CTRL + C** keys
  - In another shell, run this command: `fw monitor -U`
- Each time you run the FW Monitor, it compiles its temporary policy files (`$FWDIR/tmp/monitorfilter.*`).
- The FW Monitor also show the traffic accelerated with SecureXL.
- For more information, see sk30583.

Syntax for IPv4

```
fw monitor {-h | -help}
```

```
fw monitor [-d] [-D] [-ci <Number of Inbound Packets>] [-co
<Number of Outbound Packets>] [-e <INSPECT Expression> | -f
{<INSPECT Filter File> | -}] [-F "<Source IP>,<Source Port>,<Dest
IP>,<Dest Port>,<Protocol Number>"] [-i] [-l <Length>] [-m
{i,I,o,O,e,E}] [-o <Output File> [-w]] [[-pi <Position>] [-pI
<Position>] [-po <Position>] [-pO <Position>] | -p all [-a]] [-T]
[-u | -s] [-U] [-v <VSID>] [-x <Offset>[,<Length>] [-w]] [-b <Size
of Buffer>]
```

Syntax for IPv6

```
fw6 monitor {-h | -help}
```

```
fw6 monitor [-d] [-D] [-ci <Number of Inbound Packets>] [-co
<Number of Outbound Packets>] [-e <INSPECT Expression> | -f
{<INSPECT Filter File> | -}] [-F "<Source IP>,<Source Port>,<Dest
IP>,<Dest Port>,<Protocol Number>"] [-i] [-l <Length>] [-m
{i,I,o,O,e,E}] [-o <Output File> [-w]] [[-pi <Position>] [-pI
<Position>] [-po <Position>] [-pO <Position>] | -p all [-a]] [-T]
[-u | -s] [-U] [-v <VSID>] [-x <Offset>[,<Length>] [-w]] [-b <Size
of Buffer>]
```

Parameters

Parameter	Description
`{-h | -help}`	Shows the built-in usage.
`-b <Size of Buffer>`	Specifies the size of the memory buffer for FW Monitor. An approximate formula for total required RAM memory: `(4) x (Number of active CoreXL Firewall instances) x (Size of Buffer)` The default FW Monitor algorithm for allocating the memory buffer required to capture traffic: 1. Try to allocate the memory buffer with the default size. 2. If the available RAM is not enough, try allocate the memory buffer with a smaller size. If the available RAM is not enough on a Security Gateway, FW Monitor can fail to allocate the required memory buffer. With this parameter, you can specify the size of the memory buffer to "help" FW Monitor in its caculations. **Note** - Each CoreXL Firewall instance has two internal buffers, and there is one general buffer that merges the data from all CoreXL Firewall instances. **Default:** 8192 (in kilobytes) **Range:** 128 - 8192 (in kilobytes)

Parameter	Description
`-d` `-D`	Runs the command in debug mode and shows some information about how the FW Monitor starts and compiles the specified INSPECT filter: ■ `-d` Simple debug output. ■ `-D` Verbose output. **Note** - You can specify both parameters to show more information.
`-ci <Number of Inbound Packets>` `-co <Number of Outbound Packets>`	Specifies how many packets to capture. The FW Monitor stops the traffic capture if it counted the specified number of packets. ■ `-ci` Specifies the number of inbound packets to count. ■ `-co` Specifies the number of outbound packets to count **Best Practice** - You can use the "`-ci`" and the "`-co`" parameters together. This is especially useful during large volumes of traffic. In such scenarios, FW Monitor may bind so many resources (for writing to the console, or to a file) that recognizing the break sequence (**CTRL+C**) might take a very long time.

Parameter	Description

`-e <INSPECT Expression>`
or
`-f {<INSPECT Filter File> | -}`
	Captures only specific packets of non-accelerated traffic:
	■ "`-e <INSPECT Expression>`"
	Defines the INSPECT filter expression on the command line.
	■ "`-f <INSPECT Filter File>`"
	Reads the INSPECT filter expression from the specified file. You must enter the full path and name of the plain-text file that contains the INSPECT filter expression.
	■ "`-f -`"
	Reads the INSPECT filter expression from the standard input. After you enter the INSPECT filter expression, you must enter the `^D` (**CTRL+D**) as the EOF (End Of File) character.
	
	Warning - These INSPECT filters do **not** apply to the accelerated traffic.
	Important - Make sure to enclose the INSPECT filter expression correctly in single quotes (ASCII value 39) or double quotes (ASCII value 34).
	Notes:
	■ Refer to the `$FWDIR/lib/fwmonitor.def` file for useful macro definitions.
	■ See syntax examples below (*"Examples for the "-e" parameter" on page 1169*).

`-F "<Source IP>,<Source Port>,<Dest IP>,<Dest Port>,<Protocol Number>"`	Specifies the capture filter (for both accelerated and non-accelerated traffic): ■ `<Source IP>` - Specifies the source IP address ■ `<Source Port>` - Specifies the source Port Number (see *IANA Service Name and Port Number Registry*) ■ `<Dest IP>` - Specifies the destination IP address ■ `<Dest Port>` - Specifies the destination Port Number (see *IANA Service Name and Port Number Registry*) ■ `<Protocol Number>` - Specifies the Protocol Number (see *IANA Protocol Numbers*)

Parameter	Description

	Notes:
	■ See syntax examples below (*"Examples for the "-F" parameter" on page 1183*).
	■ The "`-F`" parameter uses these Kernel Debug Filters.
	For more information, see the *R81.20 Security Gateway Guide* - Chapter *Kernel Debug on Security Gateway* - Section *Kernel Debug Filters*.
	• For the Source IP address:
	`simple_debug_filter_saddr_<N> "<IP Address>"`
	• For the Source Ports:
	`simple_debug_filter_sport_<N> <1-65535>`
	• For the Destination IP address:
	`simple_debug_filter_daddr_<N> "<IP Address>"`
	• For the Destination Ports:
	`simple_debug_filter_dport_<N> <1-65535>`
	• For the Protocol Number:
	`simple_debug_filter_proto_<N> <0-254>`
	■ Value 0 means "`any`".
	■ This parameter supports up to 5 capture filters (up to 5 instances of the "`-F`" parameter in the syntax).
	The FW Monitor performs the logical "OR" between all specified simple capture filters.

`-H`	Creates an IP address filter. For more information, see the *R81.20 Security Gateway Guide* - Chapter *Kernel Debug on Security Gateway* - Section *Kernel Debug Filters*. This parameter supports up to 3 capture filters (up to 3 instances of the "`-H`" parameter in the syntax). Example - Capture only HTTP traffic to and from the Host 1.1.1.1: `fw ctl debug -H "1.1.1.1"`

Parameter	Description
`-i`	Flushes the standard output. **Note** - This parameter is valid only with the "`-v <VSID>`" parameter. **Best Practice** - Use this parameter to make sure FW Monitor immediately writes the captured data for each packet to the standard output. This is especially useful if you want to kill a running FW Monitor process, and want to be sure that FW Monitor writes all the data to the specified file.
`-l <Length>`	Specifies the maximal length of the captured packets. FW Monitor reads only the specified number of bytes from each packet. **Notes:** ■ This parameter is optional. ■ With this parameter you can capture only the headers from each packet (for example, IP and TCP) and omit the payload. This decreases the size of the output file. This also helps the internal FW Monitor buffer not to fill too fast. ■ Make sure to capture the minimal required number of bytes, to capture the Layer 3 IP header and Layer 4 Transport header.

Parameter	Description
`-m {i, I, o, O, e, E}`	Specifies the capture mask (inspection point) in relation to Chain Modules, in which the FW Monitor captures the traffic. These are the inspection points, through which each packet passes on a Security Gateway. ■ `-m i` Pre-Inbound only (before the packet enters a Chain Module in the inbound direction) ■ `-m I` Post-Inbound only (after the packet passes a Chain Module in the inbound direction) ■ `-m o` Pre-Outbound only (before the packet enters a Chain Module in the outbound direction) ■ `-m O` Post-Outbound only (after the packet passes through a Chain Module in the outbound direction) ■ `-m e` Pre-Outbound VPN only (before the packet enters a VPN Chain Module in the outbound direction) ■ `-m E` Post-Outbound VPN only (after the packet passes through a VPN Chain Module in the outbound direction)

Parameter	Description
	Notes: ■ You can specify several capture masks (for example, to see NAT on the egress packets, enter "`... -m o O ...`"). ■ You can use this capture mask parameter "`-m {i, I, o, O, e, E}`" together with the chain module position parameter "`-p{i | I | o | O}`". ■ In the inbound direction: • All chain positions *before* the FireWall Virtual Machine module are Pre-Inbound (the *"fw ctl chain" on page 1084* command shows this module as "`fw VM inbound`"). • All chain modules *after* the FireWall Virtual Machine module are Post-Inbound. ■ In the outbound direction: • All chain position *before* the FireWall Virtual Machine module are Pre-Outbound. • All chain modules *after* the FireWall Virtual Machine module are Post-Outbound. ■ By default, the FW Monitor captures the traffic only in the FireWall Virtual Machine module. ■ The packet direction relates to each specific packet, and not to the connection's direction. ■ The letters "`q`" and "`Q`" after the inspection point mean that the QoS policy is applied to the interface.

	Example packet flows:
	■ From a Client to a Server through the FireWall Virtual Machine module:
	`[Client] --> ("i") {FW VM attached to eth1} ("I") [Security Gateway] ("o") {FW VM attached to eth2} ("O") --> [Server]`
	■ From a Server to a Client through the FireWall Virtual Machine module:
	`[Client] <-- ("O") {FW VM attached to eth1} ("o") [Security Gateway] ("I") {FW VM attached to eth2} ("i") <-- [Server]`

Parameter	Description
`-o <Output File>`	Specifies the output file, to which FW Monitor writes the captured raw data. **Important** - If you do not specify the path explicitly, FW Monitor creates this output file in the current working directory. Because this output file can grow very fast to very large size, we always recommend to specify the full path to the largest partition `/var/log/`. The format of this output file is the same format used by tools like `snoop` (refer to RFC 1761). You can later analyze the captured traffic with the same FW Monitor tool, or with special tools like Wireshark.

`-pi <Position>`
`-pI <Position>`
`-po <Position>`
`-pO <Position>`
or
`-p all [-a]`
	Inserts the FW Monitor Chain Module at the specified position between the kernel Chain Modules (see the *"fw ctl chain" on page 1084*).
	If the FW Monitor writes the captured data to the specified output file (with the parameter "`-o <Output File>`"), it also writes the position of the FW Monitor chain module as one of the fields.
	You can insert the FW Monitor Chain Module in these positions only:
	■ `-pi <Position>`
	Inserts the FW Monitor Chain Module in the specified Pre-Inbound position.
	■ `-pI <Position>`
	Inserts the FW Monitor Chain Module in the specified Post-Inbound position.
	■ `-po <Position>`
	Inserts the FW Monitor Chain Module in the specified Pre-Outbound position.
	■ `-pO <Position>`
	Inserts the FW Monitor Chain Module in the specified Post-Outbound position
	■ `-p all [-a]`
	Inserts the FW Monitor Chain Module at all positions (both Inbound and Outbound).
	Warning - This parameter causes very high load on the CPU, but provides the most complete traffic capture.
	The "`-a`" parameter specifies to use absolute chain positions. This parameter changes the chain ID from a relative value (which only makes sense with the matching output from the *"fw ctl chain" on page 1084* command) to an absolute value.

Parameter	Description
	Notes: ■ *<Position>* can be one of these: • A relative position number In the output of the *"fw ctl chain" on page 1084* command, refer to the numbers in the leftmost column (for example, 0, 5, 14). • A relative position alias In the output of the *"fw ctl chain" on page 1084* command, refer to the internal chain module names in the rightmost column in the parentheses (for example, `sxl_in`, `fw`, `cpas`). • An absolute position In the output of the *"fw ctl chain" on page 1084* command, refer to the numbers in the second column from the left (for example, -7fffffff, -1fffff8, 7f730000). In the syntax, you must write these numbers in the hexadecimal format (for example, -0x7fffffff, -0x1fffff8, 0x7f730000). ■ You can use this chain module position parameter "`-p{i | I| o | O} ...`" together with the capture mask parameter "`-m {i, I, o, O, e, E}`". ■ In the inbound direction: • All chain positions *before* the FireWall Virtual Machine module are Pre-Inbound (the *"fw ctl chain" on page 1084* command shows this module as "`fw VM inbound`"). • All chain modules *after* the FireWall Virtual Machine module are Post-Inbound. ■ In the outbound direction: • All chain position *before* the FireWall Virtual Machine module are Pre-Outbound. • All chain modules *after* the FireWall Virtual Machine module are Post-Outbound. ■ By default, the FW Monitor captures the traffic only in the FireWall Virtual Machine module. ■ The chain module position parameters "`-p{i | I| o | O} ...`" parameters do **not** apply to the accelerated traffic, which is still monitored at the default inbound and outbound positions. ■ For more information about the inspection points, see the applicable table below.

Parameter	Description
`-T`	Shows the timestamp for each packet: `DDMMMYYYY HH:MM:SS.mmmmmm` **Best Practice** - Use this parameter if you do not save the output to a file, but print it on the screen.

`-u`
or
`-s`
	Shows UUID for each packet (it is only possible to print either the UUID, or the SUUID - not both):
	■ `-u`
	Prints connection's Universal-Unique-ID (UUID) for each packet
	■ `-s`
	Prints connection's Session UUID (SUUID) for each packet

`-U`	Removes the simple capture filters specified with this parameter: `-F "<Source IP>,<Source Port>,<Dest IP>,<Dest Port>,<Protocol Number>"`
`-v <VSID>`	On a VSX Gateway or VSX Cluster Member, captures the packets on the specified Virtual System or Virtual Router. By default, FW Monitor captures the packets on all Virtual Systems and Virtual Routers. Example: `fw monitor -v 4 -e "accept;" -o /var/log/fw_mon.cap`
`-w`	Captures the entire packet, instead of only the header. Must be used together with one of these parameters: ■ `-o <Output File>` ■ `-x <Offset>[,<Length>]`

Parameter	Description
`-x <Offset> [,<Length>]`	Specifies the position in each packet, where the FW Monitor starts to capture the data from each packet. Optionally, it is also possible to limit the amount of data the FW Monitor captures. ■ *<Offset>* Specifies how many bytes to skip from the beginning of each packet. FW Monitor starts to capture the data from each packet only after the specified number of bytes. ■ *<Length>* Specifies the maximal length of the captured packets. FW Monitor reads only the specified number of bytes from each packet. For example, to skip over the IP header and TCP header, enter "`-x 52,96`"

Inspection points in Security Gateway and in the FW Monitor output

Note - The Inbound and Outbound traffic direction relates to each specific packet, and not to the connection.

- *Inbound*

Name of inspection point	Relation to the FireWall Virtual Machine	Notion of inspection point in the FW Monitor output
Pre-Inbound	Before the inbound FireWall VM	i (for example, `eth4:i`)
Post-Inbound	After the inbound FireWall VM	I (for example, `eth4:I`)
Pre-Inbound VPN	Inbound before decrypt	id (for example, `eth4:id`)
Post-Inbound VPN	Inbound after decrypt	ID (for example, `eth4:ID`)
Pre-Inbound QoS	Inbound before QoS	iq (for example, `eth4:iq`)
Post-Inbound QoS	Inbound after QoS	IQ (for example, `eth4:IQ`)

- *Outbound*

Name of inspection point	Relation to the FireWall Virtual Machine	Notion of inspection point in the FW Monitor output
Pre-Outbound	Before the outbound FireWall VM	o (for example, `eth4:o`)
Post-Outbound	After the outbound FireWall VM	O (for example, `eth4:O`)
Pre-Outbound VPN	Outbound before encrypt	e (for example, `eth4:e`)
Post-Outbound VPN	Outbound after encrypt	E (for example, `eth4:E`)
Pre-Outbound QoS	Outbound before QoS	oq (for example, `eth4:oq`)
Post-Outbound QoS	Outbound after QoS	OQ (for example, `eth4:OQ`)

Generic Examples

Example 1 - Default syntax

```
[Expert@MyGW:0]# fw monitor
 monitor: getting filter (from command line)
 monitor: compiling
monitorfilter:
Compiled OK.
 monitor: loading
 monitor: monitoring (control-C to stop)
[vs_0][fw_1] eth0:i[40]: 192.168.204.1 -> 192.168.204.40 (TCP) len=40 id=31789
TCP: 53901 -> 22 ....A. seq=761113cd ack=f92e2a13
[vs_0][fw_1] eth0:I[40]: 192.168.204.1 -> 192.168.204.40 (TCP) len=40 id=31789
TCP: 53901 -> 22 ....A. seq=761113cd ack=f92e2a13
[vs_0][fw_1] eth0:i[40]: 192.168.204.1 -> 192.168.204.40 (TCP) len=40 id=31790
TCP: 53901 -> 22 ....A. seq=761113cd ack=f92e2a47
... ... ...
 monitor: caught sig 2
 monitor: unloading
[Expert@MyGW:0]#
```

Example 2 - Showing timestamps in the output for each packet

```
[Expert@MyGW:0]# fw monitor -T
 monitor: getting filter (from command line)
 monitor: compiling
monitorfilter:
Compiled OK.
 monitor: loading
 monitor: monitoring (control-C to stop)
[vs_0][fw_1] 12Sep2018 19:08:05.453947 eth0:oq[124]: 192.168.3.53 -> 172.20.168.16 (TCP)
len=124 id=38414
TCP: 22 -> 64424 ...PA. seq=1c23924a ack=3c951092
[vs_0][fw_1] 12Sep2018 19:08:05.453960 eth0:OQ[124]: 192.168.3.53 -> 172.20.168.16 (TCP)
len=124 id=38414
TCP: 22 -> 64424 ...PA. seq=1c23924a ack=3c951092
[vs_0][fw_1] 12Sep2018 19:08:05.454059 eth0:oq[252]: 192.168.3.53 -> 172.20.168.16 (TCP)
len=252 id=38415
TCP: 22 -> 64424 ...PA. seq=1c23929e ack=3c951092
[vs_0][fw_1] 12Sep2018 19:08:05.454064 eth0:OQ[252]: 192.168.3.53 -> 172.20.168.16 (TCP)
len=252 id=38415
TCP: 22 -> 64424 ...PA. seq=1c23929e ack=3c951092
[vs_0][fw_1] 12Sep2018 19:08:05.454072 eth0:oq[252]: 192.168.3.53 -> 172.20.168.16 (TCP)
len=252 id=38416
TCP: 22 -> 64424 ...PA. seq=1c239372 ack=3c951092
[vs_0][fw_1] 12Sep2018 19:08:05.454074 eth0:OQ[252]: 192.168.3.53 -> 172.20.168.16 (TCP)
len=252 id=38416
TCP: 22 -> 64424 ...PA. seq=1c239372 ack=3c951092
[vs_0][fw_1] 12Sep2018 19:08:05.463165 eth0:iq[40]: 172.20.168.16 -> 192.168.3.53 (TCP)
len=40 id=17398
TCP: 64424 -> 22 ....A. seq=3c951092 ack=1c239446
[vs_0][fw_1] 12Sep2018 19:08:05.463177 eth0:IQ[40]: 172.20.168.16 -> 192.168.3.53 (TCP)
len=40 id=17398
TCP: 64424 -> 22 ....A. seq=3c951092 ack=1c239446
 monitor: unloading
[Expert@MyGW:0]#
```

Example 3 - Capturing only three Pre-Inbound packets at the FireWall Virtual Machine module

```
[Expert@MyGW:0]# fw monitor -m i -ci 3
 monitor: getting filter (from command line)
 monitor: compiling
monitorfilter:
Compiled OK.
 monitor: loading
 monitor: monitoring (control-C to stop)
[vs_0][fw_1] eth0:i[40]: 192.168.204.1 -> 192.168.204.40 (TCP) len=40 id=31905
TCP: 53901 -> 22 ....A. seq=76111bb5 ack=f92e683b
[vs_0][fw_1] eth0:i[40]: 192.168.204.1 -> 192.168.204.40 (TCP) len=40 id=31906
TCP: 53901 -> 22 ....A. seq=76111bb5 ack=f92e68ef
[vs_0][fw_1] eth0:i[40]: 192.168.204.1 -> 192.168.204.40 (TCP) len=40 id=31907
TCP: 53901 -> 22 ....A. seq=76111bb5 ack=f92e69a3
 monitor: unloading
Read 3 inbound packets and 0 outbound packets
[Expert@MyGW:0]#
```

Example 4 - Inserting the FW Monitor chain is before the chain #2 and capture only three Pre-Inbound packets

```
[Expert@MyGW:0]# fw ctl chain
in chain (15):
        0: -7fffffff (0000000000000000) (00000000) SecureXL inbound (sxl_in)
        1: -7ffffffe (0000000000000000) (00000000) SecureXL inbound CT (sxl_ct)
        2: -7f800000 (ffffffff8b6718c0) (ffffffff) IP Options Strip (in) (ipopt_strip)
        3: - 1fffff8 (ffffffff8b66f6f0) (00000001) Stateless verifications (in) (asm)
        4: - 1fffff7 (ffffffff8b66f210) (00000001) fw multik misc proto forwarding
        5:         0 (ffffffff8b8506a0) (00000001) fw VM inbound  (fw)
        6:         2 (ffffffff8b671d10) (00000001) fw SCV inbound (scv)
        7:         4 (ffffffff8b061ed0) (00000003) QoS inbound offload chain module
        8:         5 (ffffffff8b564d30) (00000003) fw offload inbound (offload_in)
        9:        10 (ffffffff8b842710) (00000001) fw post VM inbound  (post_vm)
        10:    100000 (ffffffff8b7fd6c0) (00000001) fw accounting inbound (acct)
        11:  22000000 (ffffffff8b0638d0) (00000003) QoS slowpath inbound chain mod (fg_sched)
        12:  7f730000 (ffffffff8b3c40b0) (00000001) passive streaming (in) (pass_str)
        13:  7f750000 (ffffffff8b0e5b40) (00000001) TCP streaming (in) (cpas)
        14:  7f800000 (ffffffff8b671870) (ffffffff) IP Options Restore (in) (ipopt_res)
out chain (14):
        0: -7f800000 (ffffffff8b6718c0) (ffffffff) IP Options Strip (out) (ipopt_strip)
        1: - 1fffff0 (ffffffff8b0d0190) (00000001) TCP streaming (out) (cpas)
        2: - 1ffff50 (ffffffff8b3c40b0) (00000001) passive streaming (out) (pass_str)
        3: - 1f00000 (ffffffff8b66f6f0) (00000001) Stateless verifications (out) (asm)
        4: -     1ff (ffffffff8aeec0a0) (00000001) NAC Packet Outbound (nac_tag)
        5:         0 (ffffffff8b8506a0) (00000001) fw VM outbound (fw)
        6:        10 (ffffffff8b842710) (00000001) fw post VM outbound  (post_vm)
        7:  15000000 (ffffffff8b062540) (00000003) QoS outbound offload chain modul (fg_pol)
        8:  21000000 (ffffffff8b0638d0) (00000003) QoS slowpath outbound chain mod (fg_sched)
        9:  7f000000 (ffffffff8b7fd6c0) (00000001) fw accounting outbound (acct)
        10:  7f700000 (ffffffff8b0e4660) (00000001) TCP streaming post VM (cpas)
        11:  7f800000 (ffffffff8b671870) (ffffffff) IP Options Restore (out) (ipopt_res)
        12:  7f900000 (0000000000000000) (00000000) SecureXL outbound (sxl_out)
        13:  7fa00000 (0000000000000000) (00000000) SecureXL deliver (sxl_deliver)
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw monitor -pi 2 -ci 3
 monitor: getting filter (from command line)
 monitor: compiling
monitorfilter:
Compiled OK.
 monitor: loading
in chain (17):
        0: -7fffffff (0000000000000000) (00000000) SecureXL inbound (sxl_in)
        1: -7ffffffe (0000000000000000) (00000000) SecureXL inbound CT (sxl_ct)
        2: -7f800001 (ffffffff8b6774d0) (ffffffff) fwmonitor (i/f side)
        3: -7f800000 (ffffffff8b6718c0) (ffffffff) IP Options Strip (in) (ipopt_strip)
        4: - 1fffff8 (ffffffff8b66f6f0) (00000001) Stateless verifications (in) (asm)
        5: - 1fffff7 (ffffffff8b66f210) (00000001) fw multik misc proto forwarding
        6:         0 (ffffffff8b8506a0) (00000001) fw VM inbound  (fw)
        7:         2 (ffffffff8b671d10) (00000001) fw SCV inbound (scv)
        8:         4 (ffffffff8b061ed0) (00000003) QoS inbound offload chain module
        9:         5 (ffffffff8b564d30) (00000003) fw offload inbound (offload_in)
        10:        10 (ffffffff8b842710) (00000001) fw post VM inbound  (post_vm)
        11:    100000 (ffffffff8b7fd6c0) (00000001) fw accounting inbound (acct)
        12:  22000000 (ffffffff8b0638d0) (00000003) QoS slowpath inbound chain mod (fg_sched)
        13:  70000000 (ffffffff8b6774d0) (ffffffff) fwmonitor (IP  side)
        14:  7f730000 (ffffffff8b3c40b0) (00000001) passive streaming (in) (pass_str)
        15:  7f750000 (ffffffff8b0e5b40) (00000001) TCP streaming (in) (cpas)
        16:  7f800000 (ffffffff8b671870) (ffffffff) IP Options Restore (in) (ipopt_res)
out chain (16):
        0: -7f800000 (ffffffff8b6718c0) (ffffffff) IP Options Strip (out) (ipopt_strip)
        1: -70000000 (ffffffff8b6774d0) (ffffffff) fwmonitor (i/f side)
        2: - 1fffff0 (ffffffff8b0d0190) (00000001) TCP streaming (out) (cpas)
        3: - 1ffff50 (ffffffff8b3c40b0) (00000001) passive streaming (out) (pass_str)
        4: - 1f00000 (ffffffff8b66f6f0) (00000001) Stateless verifications (out) (asm)
        5: -     1ff (ffffffff8aeec0a0) (00000001) NAC Packet Outbound (nac_tag)
        6:         0 (ffffffff8b8506a0) (00000001) fw VM outbound (fw)
        7:        10 (ffffffff8b842710) (00000001) fw post VM outbound  (post_vm)
        8:  15000000 (ffffffff8b062540) (00000003) QoS outbound offload chain modul (fg_pol)
        9:  21000000 (ffffffff8b0638d0) (00000003) QoS slowpath outbound chain mod (fg_sched)
        10:  70000000 (ffffffff8b6774d0) (ffffffff) fwmonitor (IP side)
        11:  7f000000 (ffffffff8b7fd6c0) (00000001) fw accounting outbound (acct)
        12:  7f700000 (ffffffff8b0e4660) (00000001) TCP streaming post VM (cpas)
```

```
        13:  7f800000 (ffffffff8b671870) (ffffffff) IP Options Restore (out) (ipopt_res)
        14:  7f900000 (0000000000000000) (00000000) SecureXL outbound (sxl_out)
        15:  7fa00000 (0000000000000000) (00000000) SecureXL deliver (sxl_deliver)
 monitor: monitoring (control-C to stop)
[vs_0][fw_1] eth0:oq1 (TCP streaming (out))[1228]: 192.168.204.40 -> 192.168.204.1 (TCP)
len=1228 id=37575
TCP: 22 -> 51702 ...PA. seq=34e2af31 ack=e6c995ce
[vs_0][fw_1] eth0:OQ10 (TCP streaming post VM)[1228]: 192.168.204.40 -> 192.168.204.1 (TCP)
len=1228 id=37575
TCP: 22 -> 51702 ...PA. seq=34e2af31 ack=e6c995ce
[vs_0][fw_1] eth0:iq2 (IP Options Strip (in))[40]: 192.168.204.1 -> 192.168.204.40 (TCP)
len=40 id=32022
TCP: 51702 -> 22 ....A. seq=e6c995ce ack=34e2af31
[vs_0][fw_1] eth0:IQ13 (TCP streaming (in))[40]: 192.168.204.1 -> 192.168.204.40 (TCP) len=40
id=32022
TCP: 51702 -> 22 ....A. seq=e6c995ce ack=34e2af31
[vs_0][fw_1] eth0:oq1 (TCP streaming (out))[1356]: 192.168.204.40 -> 192.168.204.1 (TCP)
len=1356 id=37576
TCP: 22 -> 51702 ...PA. seq=34e2b3d5 ack=e6c995ce
[vs_0][fw_1] eth0:OQ10 (TCP streaming post VM)[1356]: 192.168.204.40 -> 192.168.204.1 (TCP)
len=1356 id=37576
TCP: 22 -> 51702 ...PA. seq=34e2b3d5 ack=e6c995ce
[vs_0][fw_1] eth0:iq2 (IP Options Strip (in))[40]: 192.168.204.1 -> 192.168.204.40 (TCP)
len=40 id=32023
TCP: 51702 -> 22 ....A. seq=e6c995ce ack=34e2b8f9
[vs_0][fw_1] eth0:IQ13 (TCP streaming (in))[40]: 192.168.204.1 -> 192.168.204.40 (TCP) len=40
id=32023
TCP: 51702 -> 22 ....A. seq=e6c995ce ack=34e2b8f9
[vs_0][fw_1] eth0:oq1 (TCP streaming (out))[1356]: 192.168.204.40 -> 192.168.204.1 (TCP)
len=1356 id=37577
TCP: 22 -> 51702 ...PA. seq=34e2b8f9 ack=e6c995ce
[vs_0][fw_1] eth0:OQ10 (TCP streaming post VM)[1356]: 192.168.204.40 -> 192.168.204.1 (TCP)
len=1356 id=37577
TCP: 22 -> 51702 ...PA. seq=34e2b8f9 ack=e6c995ce
[vs_0][fw_1] eth0:oq1 (TCP streaming (out))[412]: 192.168.204.40 -> 192.168.204.1 (TCP)
len=412 id=37578
TCP: 22 -> 51702 ...PA. seq=34e2be1d ack=e6c995ce
[vs_0][fw_1] eth0:OQ10 (TCP streaming post VM)[412]: 192.168.204.40 -> 192.168.204.1 (TCP)
len=412 id=37578
TCP: 22 -> 51702 ...PA. seq=34e2be1d ack=e6c995ce
[vs_0][fw_1] eth0:iq2 (IP Options Strip (in))[40]: 192.168.204.1 -> 192.168.204.40 (TCP)
len=40 id=32024
TCP: 51702 -> 22 ....A. seq=e6c995ce ack=34e2bf91
[vs_0][fw_1] eth0:IQ13 (TCP streaming (in))[40]: 192.168.204.1 -> 192.168.204.40 (TCP) len=40
id=32024
TCP: 51702 -> 22 ....A. seq=e6c995ce ack=34e2bf91
[vs_0][fw_1] eth0:oq1 (TCP streaming (out))[716]: 192.168.204.40 -> 192.168.204.1 (TCP)
len=716 id=37579
TCP: 22 -> 51702 ...PA. seq=34e2bf91 ack=e6c995ce
[vs_0][fw_1] eth0:OQ10 (TCP streaming post VM)[716]: 192.168.204.40 -> 192.168.204.1 (TCP)
len=716 id=37579
TCP: 22 -> 51702 ...PA. seq=34e2bf91 ack=e6c995ce
 monitor: unloading
Read 3 inbound packets and 5 outbound packets
[Expert@MyGW:0]#
```

Example 5 - Showing list of Chain Modules with the FW Monitor, when you do not change the default capture positions

```
[Expert@MyGW:0]# fw ctl chain
in chain (17):
        0: -7fffffff (0000000000000000) (00000000) SecureXL inbound (sxl_in)
        1: -7ffffffe (0000000000000000) (00000000) SecureXL inbound CT (sxl_ct)
        2: -7f800000 (ffffffff8b6718c0) (ffffffff) IP Options Strip (in) (ipopt_strip)
        3: -70000000 (ffffffff8b6774d0) (ffffffff) fwmonitor (i/f side)
        4: - 1fffff8 (ffffffff8b66f6f0) (00000001) Stateless verifications (in) (asm)
        5: - 1fffff7 (ffffffff8b66f210) (00000001) fw multik misc proto forwarding
        6:         0 (ffffffff8b8506a0) (00000001) fw VM inbound  (fw)
        7:         2 (ffffffff8b671d10) (00000001) fw SCV inbound (scv)
        8:         4 (ffffffff8b061ed0) (00000003) QoS inbound offload chain module
        9:         5 (ffffffff8b564d30) (00000003) fw offload inbound (offload_in)
        10:        10 (ffffffff8b842710) (00000001) fw post VM inbound  (post_vm)
        11:    100000 (ffffffff8b7fd6c0) (00000001) fw accounting inbound (acct)
        12:  22000000 (ffffffff8b0638d0) (00000003) QoS slowpath inbound chain mod (fg_sched)
        13:  70000000 (ffffffff8b6774d0) (ffffffff) fwmonitor (IP  side)
        14:  7f730000 (ffffffff8b3c40b0) (00000001) passive streaming (in) (pass_str)
        15:  7f750000 (ffffffff8b0e5b40) (00000001) TCP streaming (in) (cpas)
        16:  7f800000 (ffffffff8b671870) (ffffffff) IP Options Restore (in) (ipopt_res)
out chain (16):
        0: -7f800000 (ffffffff8b6718c0) (ffffffff) IP Options Strip (out) (ipopt_strip)
        1: -70000000 (ffffffff8b6774d0) (ffffffff) fwmonitor (i/f side)
        2: - 1fffff0 (ffffffff8b0d0190) (00000001) TCP streaming (out) (cpas)
        3: - 1ffff50 (ffffffff8b3c40b0) (00000001) passive streaming (out) (pass_str)
        4: - 1f00000 (ffffffff8b66f6f0) (00000001) Stateless verifications (out) (asm)
        5: -     1ff (ffffffff8aeec0a0) (00000001) NAC Packet Outbound (nac_tag)
        6:         0 (ffffffff8b8506a0) (00000001) fw VM outbound (fw)
        7:        10 (ffffffff8b842710) (00000001) fw post VM outbound  (post_vm)
        8:  15000000 (ffffffff8b062540) (00000003) QoS outbound offload chain modul (fg_pol)
        9:  21000000 (ffffffff8b0638d0) (00000003) QoS slowpath outbound chain mod (fg_sched)
        10:  70000000 (ffffffff8b6774d0) (ffffffff) fwmonitor (IP side)
        11:  7f000000 (ffffffff8b7fd6c0) (00000001) fw accounting outbound (acct)
        12:  7f700000 (ffffffff8b0e4660) (00000001) TCP streaming post VM (cpas)
        13:  7f800000 (ffffffff8b671870) (ffffffff) IP Options Restore (out) (ipopt_res)
        14:  7f900000 (0000000000000000) (00000000) SecureXL outbound (sxl_out)
        15:  7fa00000 (0000000000000000) (00000000) SecureXL deliver (sxl_deliver)
[Expert@MyGW:0]#
```

Examples for the "-e" parameter

Example 1 - Capture everything

```
[Expert@HostName]# fw monitor -e "accept;" -o /var/log/fw_
mon.cap
```

Example 2 - Capture traffic to / from specific hosts

To specify a host, you can use one of these expressions:

- Use "`host(<IP_Address_in_Doted_Decimal_format>)`", which applies to both Source IP address and Destination IP address
- Use a specific Source IP address "`src=<IP_Address_in_Doted_Decimal_format>`" and a specific Destination IP address "`dst=<IP_Address_in_Doted_Decimal_format>`"

Example filters:

- Capture everything between host X and host Y:

```
[Expert@HostName]# fw monitor -e "host(x.x.x.x) and host
(y.y.y.y), accept;" -o /var/log/fw_mon.cap
```

```
[Expert@HostName]# fw monitor -e "((src=x.x.x.x ,
dst=y.y.y.y) or (src=y.y.y.y , dst=x.x.x.x)), accept;" -o
/var/log/fw_mon.cap
```

- Capture everything between hosts X,Z and hosts Y,Z in *all* Firewall kernel chains:

```
[Expert@HostName]# fw monitor -p all -e "((src=x.x.x.x or
dst=z.z.z.z) and (src=y.y.y.y or dst=z.z.z.z)), accept ;" -o
/var/log/fw_mon.cap
```

- Capture everything to/from host X or to/from host Y or to/from host Z:

```
[Expert@HostName]# fw monitor -e "host(x.x.x.x) or host
(y.y.y.y) or host(z.z.z.z), accept;" -o /var/log/fw_mon.cap
```

```
[Expert@HostName]# fw monitor -e "((src=x.x.x.x or
dst=x.x.x.x) or (src=y.y.y.y or dst=y.y.y.y) or (src=z.z.z.z
or dst=z.z.z.z)), accept;" -o /var/log/fw_mon.cap
```

Example 3 - Capture traffic to / from specific ports

Note - You must specify port numbers in Decimal format. Refer to the `/etc/services` file on the Security Gateway, or to *IANA Service Name and Port Number Registry*.

To specify a port, you can use one of these expressions:

- Use "`port(<IANA_Port_Number>)`", which applies to both Source Port and Destination Port
- Use a specific Source Port "`sport=<IANA_Port_Number>`" and a specific Destination Port "`dport=<IANA_Port_Number>`"
- In addition:
  - For specific TCP port, you can use "`tcpport(<IANA_Port_Number>)`", which applies to both Source TCP Port and Destination TCP Port
  - For specific UDP port, you can use "`udpport(<IANA_Port_Number>)`", which applies to both Source UDP Port and Destination UDP Port

Example filters:

- Capture everything to/from port X:

```
[Expert@HostName]# fw monitor -e "port(x), accept;" -o
/var/log/fw_mon.cap
```

```
[Expert@HostName]# fw monitor -e "(sport=x or dport=x),
accept;" -o /var/log/fw_mon.cap
```

- Capture everything except port X:

```
[Expert@HostName]# fw monitor -e "((sport=!x) or
(dport=!x)), accept;" -o /var/log/fw_mon.cap
```

```
[Expert@HostName]# fw monitor -e "not (sport=x or dport=x),
accept;" -o /var/log/fw_mon.cap
```

- Capture everything except SSH:

```
[Expert@HostName]# fw monitor -e "((sport!=22) or
(dport!=22)), accept;" -o /var/log/fw_mon.cap
```

```
[Expert@HostName]# fw monitor -e "not (sport=22 or
dport=22), accept;" -o /var/log/fw_mon.cap
```

```
[Expert@HostName]# fw monitor -e "not tcpport(22), accept;"
-o /var/log/fw_mon.cap
```

- Capture everything to/from host X except SSH:

```
[Expert@HostName]# fw monitor -e "(host(x.x.x.x) and
(sport!=22 or dport!=22)), accept;" -o /var/log/fw_mon.cap
```

```
[Expert@HostName]# fw monitor -e "((src=x.x.x.x or
dst=x.x.x.x) and (not (sport=22 or dport=22))), accept;" -o
/var/log/fw_mon.cap
```

```
[Expert@HostName]# fw monitor -e "(host(x.x.x.x) and not
tcpport(22)), accept;" -o /var/log/fw_mon.cap
```

- Capture everything except NTP:

```
[Expert@HostName]# fw monitor -e "not udpport(123), accept;"
-o /var/log/fw_mon.cap
```

Example 4 - Capture traffic over specific protocol

Note - You must specify protocol numbers in Decimal format. Refer to the `/etc/protocols` file on the Security Gateway, or to *IANA Protocol Numbers*.

To specify a protocol, you can use one of these expressions:

- Use "`ip_p=<IANA_Protocol_Number>`"

  Examples:

  - To specify TCP protocol with byte offset, use "`ip_p=6`"
  - To specify UDP protocol with byte offset, use "`ip_p=11`"
  - To specify ICMP protocol with byte offset, use "`ip_p=1`"

- Use "`accept [9:1]=<IANA_Protocol_Number>`"

  Examples:

  - To specify TCP protocol with byte offset, use "`accept [9:1]=6`"
  - To specify UDP protocol with byte offset, use "`accept [9:1]=11`"
  - To specify ICMP protocol with byte offset, use "`accept [9:1]=1`"

- In addition, you can explicitly use these expressions to specify protocols:

  Summary Table

Which protocol to specify	On which port(s) traffic is captured	Expression
TCP	N / A	`"tcp, accept;"`
UDP	N / A	`"udp, accept;"`
ICMPv4	N / A	`"icmp, accept;"` or `"icmp4, accept;"`
ICMPv6	N / A	`"icmp6, accept;"`
HTTP	TCP 80	`"http, accept;"`
HTTPS	TCP 443	`"https, accept;"`
PROXY	TCP 8080	`"proxy, accept;"`
DNS	UDP 53	`"dns, accept;"`
IKE	UDP 500	`"ike, accept;"`
NAT-T	UDP 4500	`"natt, accept;"`
ESP and IKE	IP proto 50 and UDP 500	`"vpn, accept;"`

Which protocol to specify	On which port(s) traffic is captured	Expression
All VPN-related data: a. ESP b. IPsec over UDP c. IKE d. NAT-T e. CRL f. RDP g. Tunnel Test h. Topology i. L2TP j. SCV k. Multi-Portal l. and so on	a. IP proto 50 b. UDP 2746 c. UDP 500 d. UDP 4500 e. TCP 18264 f. UDP 259 g. UDP 18234 h. TCP 264 i. TCP 1701 j. UDP 18233 k. TCP 443 + TCP 444 l. and so on	`"vpnall, accept;"`
Multi-Portal connections	TCP 443 and TCP 444	`"multi, accept;"`
SSH	TCP 22	`"ssh, accept;"`
FTP	TCP 20 and TCP 21	`"ftp, accept;"`
Telnet	TCP 23	`"telnet, accept;"`
SMTP	TCP 25	`"smtp, accept;"`
POP3	TCP 110	`"pop3, accept;"`

Example filters:

- Filter to capture everything on protocol X:

```
[Expert@HostName]# fw monitor -e "ip_p=X, accept;" -o
/var/log/fw_mon.cap
```

- Filter to capture rverything on protocol X and port Z on protocol Y:

```
[Expert@HostName]# fw monitor -e "(ip_p=X) or (ip_p=Y, port
(Z)), accept;" -o /var/log/fw_mon.cap
```

- Filter to capture capture everything TCP between host X and host Y:

```
[Expert@HostName]# fw monitor -e "ip_p=6, host(x.x.x.x) or
host(y.y.y.y), accept;" -o /var/log/fw_mon.cap
```

```
[Expert@HostName]# fw monitor -e "tcp, host(x.x.x.x) or host
(y.y.y.y), accept;" -o /var/log/fw_mon.cap
```

```
[Expert@HostName]# fw monitor -e "accept [9:1]=6 ,
((src=x.x.x.x , dst=y.y.y.y) or (src=y.y.y.y ,
dst=x.x.x.x));"
```

```
[Expert@HostName]# fw monitor -e "ip_p=6, ((src=x.x.x.x ,
dst=y.y.y.y) or (src=y.y.y.y , dst=x.x.x.x)), accept;" -o
/var/log/fw_mon.cap
```

Example 5 - Capture traffic with specific protocol options

Note - Refer to the `$FWDIR/lib/tcpip.def` file on Security Gateway.

Summary Table for IPv4

Option Description	Expression	Example
Source IPv4 address of the IPv4 packet	`ip_src = <IPv4_Address>`	`fw monitor -e "ip_src = 192.168.22.33, accept;"`
Destination IPv4 address of the IPv4 packet	`ip_dst = <IPv4_Address>`	`fw monitor -e "ip_dst = 192.168.22.33, accept;"`
Time To Live of the IPv4 packet	`ip_ttl = <Number>`	`fw monitor -e "ip_ttl = 255, accept;"`
Total Length of the IPv4 packet in bytes	`ip_len = <Length_in_Bytes>`	`fw monitor -e "ip_len = 64, accept;"`

Option Description	Expression	Example
TOS field of the IPv4 packet	`ip_tos = <Number>`	`fw monitor -e "ip_ tos = 0, accept;"`

IANA Protocol Number (either in Dec or in Hex) encapsulated in the IPv4 packet	`ip_p = <IANA_ Protocol_ Number>`	Example for TCP:
		`fw monitor -e "ip_p = 6, accept;"`
		Examples for UDP:
		`fw monitor -e "ip_p = 17, accept;"`
		`fw monitor -e "ip_p = 0x11, accept;"`
		Example for ICMPv4:
		`fw monitor -e "ip_p = 1, accept;"`

Summary Table for IPv6

Option Description	Expression	Example
Source IPv6 address of the IPv6 packet	ip_src6p = <IPv6_ Address>	`fw monitor -e "ip_src6p = 0:0:0:0:0:ffff:c0a8:1621, accept;"`
Destination IPv6 address of the IPv6 packet	ip_dst6p = <IPv6_ Address>	`fw monitor -e "ip_dst6p = 0:0:0:0:0:ffff:c0a8:1621, accept;"`
Payload Length of the IPv6 packet in bytes	ip_len6 = <Length_in_ Bytes>	`fw monitor -e "ip_len6 = 1000, accept;"`
Hop Limit ("Time To Live") of the IPv6 packet	ip_ttl6 = <Number>	`fw monitor -e "ip_ttl6 = 255, accept;"`
Next Header of the IPv6 packet - encapsulated IANA Protocol Number	ip_p6 = <IANA_ Protocol_ Number>	`fw monitor -e "ip_p6 = 6, accept;"`

Summary Table for TCP

Option Description	Expression	Example
SYN flag is set in TCP packet	`syn`	`fw monitor -e "ip_p = 6, syn, accept;"`
ACK flag is set in TCP packet	`ack`	`fw monitor -e "ip_p = 6, ack, accept;"`
RST flag is set in TCP packet	`rst`	`fw monitor -e "ip_p = 6, rst, accept;"`
FIN flag is set in TCP packet	`fin`	`fw monitor -e "ip_p = 6, fin, accept;"`
First packet of TCP connection (SYN flag is set, but ACK flag is not set in TCP packet)	`first`	`fw monitor -e "ip_p = 6, first, accept;"`
Not the first packet of TCP connection (SYN flag is not set in TCP packet)	`not_first`	`fw monitor -e "ip_p = 6, not_first, accept;"`
Established TCP connection (either ACK flag is set, or SYN flag is not set in TCP packet)	`established`	`fw monitor -e "ip_p = 6, established, accept;"`
Last packet of TCP connection (both ACK flag and FIN flag are set in TCP packet)	`last`	`fw monitor -e "ip_p = 6, last, accept;"`
End of TCP connection (either RST flag is set, or FIN flag is set in TCP packet)	`tcpdone`	`fw monitor -e "ip_p = 6, tcpdone, accept;"`

<table>
<tr><th>Option Description</th><th>Expression</th><th>Example</th></tr>
<tr><td>General way to match the flags inside in TCP packets</td><td><code>th_flags = <<i>Sum_of_Flags_Hex_Values</i>></code></td><td>
<table>
<tr><th>TCP Flag</th><th>Example</th></tr>
<tr><td>SYN (0x2)</td><td><code>fw monitor -e "th_ flags = 0x2, accept;"</code></td></tr>
<tr><td>ACK (0x10)</td><td><code>fw monitor -e "th_ flags = 0x10, accept;"</code></td></tr>
<tr><td>PSH (0x8)</td><td><code>fw monitor -e "th_ flags = 0x8, accept;"</code></td></tr>
<tr><td>FIN (0x1)</td><td><code>fw monitor -e "th_ flags = 0x1, accept;"</code></td></tr>
<tr><td>RST (0x4)</td><td><code>fw monitor -e "th_ flags = 0x4, accept;"</code></td></tr>
<tr><td>URG (0x20)</td><td><code>fw monitor -e "th_ flags = 0x20, accept;"</code></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Option Description</th><th>Expression</th><th>Example</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>TCP Flag</th><th>Example</th></tr>
<tr><td>SYN + ACK</td><td><code>fw monitor -e "th_ flags = 0x12, accept;"</code></td></tr>
<tr><td>PSH + ACK</td><td><code>fw monitor -e "th_ flags = 0x18, accept;"</code></td></tr>
<tr><td>FIN + ACK</td><td><code>fw monitor -e "th_ flags = 0x11, accept;"</code></td></tr>
<tr><td>RST + ACK</td><td><code>fw monitor -e "th_ flags = 0x14, accept;"</code></td></tr>
</table>
</td></tr>
<tr><td>TCP source port</td><td><code>th_sport = <<i>Port_Number</i>></code></td><td><code>fw monitor -e "th_ sport = 59259, accept;"</code></td></tr>
<tr><td>TCP destination port</td><td><code>th_dport = <<i>Port_Number</i>></code></td><td><code>fw monitor -e "th_ dport = 22, accept;"</code></td></tr>
<tr><td>TCP sequence number (either in Dec or in Hex)</td><td><code>th_seq = <<i>Number</i>></code></td><td>Example for Dec format:
<code>fw monitor -e "th_seq = 3937833514, accept;"</code>
Example for Hex format:
<code>fw monitor -e "th_seq = 0xeab6922a, accept;"</code></td></tr>
</table>

Option Description	Expression	Example

TCP acknowledged number (either in Dec or in Hex)	`th_ack = <Number>`	Example for Dec format:
		`fw monitor -e "th_ack = 509054325, accept;"`
		Example for Hex format:
		`fw monitor -e "th_ack = 0x1e578d75, accept;"`

Summary Table for UDP

Option Description	Expression	Example
UDP source port	`uh_sport = <Port_Number>`	`fw monitor -e "uh_sport = 53, accept;"`
UDP destination port	`uh_dport = <Port_Number>`	`fw monitor -e "uh_dport = 53, accept;"`

Summary Table for ICMPv4

Option Description	Expression	Example
ICMPv4 packets with specified Type	`icmp_type = <Number>`	`fw monitor -e "icmp_type = 0, accept;"`
ICMPv4 packets with specified Code	`icmp_code = <Number>`	`fw monitor -e "icmp_code = 0, accept;"`
ICMPv4 packets with specified Identifier	`icmp_id = <Number>`	`fw monitor -e "icmp_id = 20583, accept;"`
ICMPv4 packets with specified Sequence number	`icmp_seq = <Number>`	`fw monitor -e "icmp_seq = 1, accept;"`
ICMPv4 Echo Request packets (Type 8, Code 0)	`echo_req`	`fw monitor -e "echo_req, accept;"`
ICMPv4 Echo Reply packets (Type 0, Code 0)	`echo_reply`	`fw monitor -e "echo_reply, accept;"`
ICMPv4 Echo Request and ICMPv4 Echo Reply packets	`ping`	`fw monitor -e "ping, accept;"`

Option Description	Expression	Example
Traceroute packets as implemented in Unix OS (UDP packets on ports above 30000 and with TTL<30; or ICMP Time exceeded packets)	`traceroute`	`fw monitor -e "traceroute, accept;"`
Traceroute packets as implemented in Windows OS (ICMP Request packets with TTL<30; or ICMP Time exceeded packets)	`tracert`	`fw monitor -e "tracert, accept;"`
Length of ICMPv4 packets	`icmp_ip_len = <length>`	`fw monitor -e "icmp_ip_len = 84, accept;"`

Summary Table for ICMPv6

Option Description	Expression	Example
ICMPv6 packets with specified Type	`icmp6_type = <Number>`	`fw monitor -e "icmp6_type = 1, accept;"`
ICMPv6 packets with specified Code	`icmp6_code = <Number>`	`fw monitor -e "icmp6_code = 3, accept;"`

Example 6 - Capture specific bytes in packets

Syntax:

```
fw monitor -e "accept [ <Offset> : <Length> , <Byte Order> ]
<Relational-Operator> <Value>;"
```

Parameters:

Parameter	Explanation
<Offset>	Specifies the offset relative to the beginning of the IP packet from where the value should be read.

Parameter	Explanation
<Length>	Specifies the number of bytes: ■ `1` = byte ■ `2` = word ■ `4` = dword If length is not specified, FW Monitor assumes 4 (dword).
<Byte Order>	Specifies the byte order: ■ `b` = big endian, or network order ■ `l` = little endian, or host order If order is not specified, FW Monitor assumes little endian byte order.
<Relational-Operator	Relational operator to express the relation between the packet data and the value: ■ `<` - less than ■ `>` - greater than ■ `<=` - less than or equal to ■ `>=` - greater than ■ `=` or `is` - equal to ■ `!=` or `is not` - not equal to
<Value>	One of the data types known to INSPECT (for example, an IP address, or an integer).

Explanations:

- The IP-based protocols are stored in the IP packet as a byte at offset 9.
  - To filter based on a Protocol encapsulated into IP, use this syntax:

    ```
    [Expert@HostName]# fw monitor -e "accept [9:1]=<IANA_
    Protocol_Number>;"
    ```

- The Layer 3 IP Addresses are stored in the IP packet as double words at offset 12 (Source address) and at offset 16 (Destination address).

- To filter based on a Source IP address, use this syntax:

```
[Expert@HostName]# fw monitor -e "accept [12:4,b]=<IP_
Address_in_Doted_Decimal_format>;"
```

- To filter based on a Destination IP address, use this syntax:

```
[Expert@HostName]# fw monitor -e "accept [16:4,b]=<IP_
Address_in_Doted_Decimal_format>;"
```

- The Layer 4 Ports are stored in the IP packet as a word at offset 20 (Source port) and at offset 22 (Destination port).
  - To filter based on a Source port, use this syntax:

```
[Expert@HostName]# fw monitor -e "accept
[20:2,b]=<Port_Number_in_Decimal_format>;"
```

  - To filter based on a Destination port, use this syntax:

```
[Expert@HostName]# fw monitor -e "accept
[22:2,b]=<Port_Number_in_Decimal_format>;"
```

Example filters:

- Capture everything between host X and host Y:

```
[Expert@HostName]# fw monitor -e "accept (([12:4,b]=x.x.x.x
, [16:4,b]=y.y.y.y) or ([12:4,b]=y.y.y.y ,
[16:4,b]=x.x.x.x));"
```

- Capture everything on port X:

```
[Expert@HostName]# fw monitor -e "accept [20:2,b]=x or
[22:2,b]=x;" -o /var/log/fw_mon.cap
```

Example 7 - Capture traffic to/from specific network

You must specify the *network address* and *length of network mask* (number of bits).

There are 3 options:

Traffic direction	Expression
To or From a network	"net(<*Network_IP_Address*>, <*Mask_Length*>), accept;"

Traffic direction	Expression
To a network	`"to_net(<Network_IP_Address>, <Mask_Length>), accept;"`
From a network	`"from_net(<Network_IP_Address>, <Mask_Length>), accept;"`

Example filters:

- Capture everything to/from network 192.168.33.0 / 24:

```
[Expert@HostName]# fw monitor -e "net(192.168.33.0, 24), accept;"
```

- Capture everything sent to network 192.168.33.0 / 24:

```
[Expert@HostName]# fw monitor -e "to_net(192.168.33.0, 24), accept;"
```

- Capture everything sent from network 192.168.33.0 / 24:

```
[Expert@HostName]# fw monitor -e "from_net(192.168.33.0, 24), accept;"
```

Example 8 - Filter out irrelevant "noise"

Filter in only TCP protocol, and HTTP and HTTPS ports

Filter out the SSH and FW Logs

```
[Expert@HostName]# fw monitor -e "accept (ip_p=6) and (not (sport=22 or dport=22)) and (not (sport=257 or dport=257)) and ((dport=80 or dport=443) or (sport=80 or sport=443);" -o /var/log/fw_mon.cap
```

Examples for the "-F" parameter

You can specify up to 5 capture filters with this parameter (up to 5 instances of the "`-F`" parameter in the syntax).

The FW Monitor performs the logical "OR" between all specified simple capture filters.

Value 0 is used as "`any`".

Example 1 - Capture everything

```
[Expert@HostName]# fw monitor -F "0,0,0,0,0" -o /var/log/fw_
mon.cap
```

Example 2 - Capture traffic to / from specific hosts

- Capture all traffic from Source IP x.x.x.x (any port) to Destination IP y.y.y.y (any port), over all protocols:

  ```
  [Expert@HostName]# fw monitor -F "x.x.x.x,0,y.y.y.y,0,0" -o
  /var/log/fw_mon.cap
  ```

- Capture all traffic between Host x.x.x.x (any port) and Host y.y.y.y (any port), over all protocols:

  ```
  [Expert@HostName]# fw monitor -F "x.x.x.x,0,y.y.y.y,0,0" -F
  "y.y.y.y,0, x.x.x.x ,0,0" -o /var/log/fw_mon.cap
  ```

Example 3 - Capture traffic to / from specific ports

- Capture traffic from any Source IP from Source Port X to any Destination IP to Destination Port Y, over all protocols:

  ```
  [Expert@HostName]# fw monitor -F "0,x,0,y,0" -o /var/log/fw_
  mon.cap
  ```

- Capture traffic between all hosts, between Port X and Port Y, over all protocols:

  ```
  [Expert@HostName]# fw monitor -F "0,x,0,y,0" -F "0,y,0,x,0"
  -o /var/log/fw_mon.cap
  ```

Example 4 - Capture traffic over specific protocol

- Capture traffic between all hosts, between all ports, over a Protocol with assigned number X:

  ```
  [Expert@HostName]# fw monitor -F "0,0,0,0,x" -o /var/log/fw_
  mon.cap
  ```

Example 5 - Capture traffic between specific hosts between specific ports over specific protocol

```
[Expert@HostName]# fw monitor -F "a.a.a.a,b,c.c.c.c,d,e" -F
"c.c.c.c,d,a.a.a.a,b,e" -o /var/log/fw_mon.cap
```

To capture only HTTP traffic between the Client 1.1.1.1 and the Server 2.2.2.2:

```
fw montior -F "1.1.1.1,0,2.2.2.2,80,6" -F
"2.2.2.2,80,1.1.1.1,0,6" -o /var/log/fw_mon.cap
```

fw repairlog

Description

Check Point Security log file (`$FWDIR/log/*.log`) and Audit log files (`$FWDIR/log/*.adtlog`) are databases, with special pointer files.

If these log pointer files become corrupted (which causes the inability to read the log file), this command can rebuild them.

Log File Type	Log File Location	Log Pointer Files

Security log	`$FWDIR/log/*.log`	`*.logptr`
		`*.logaccount_ptr`
		`*.loginitial_ptr`
		`*.logLuuidDB`

Audit log	`$FWDIR/log/*.adtlog`	`*.adtlogptr`
		`*.adtlogaccount_ptr`
		`*.adtloginitial_ptr`
		`*.adtlogLuuidDB`

Important - You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).

Syntax

```
fw [-d] repairlog [-u] <Name of Log File>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-u`	Specifies to rebuild the unification chains in the log file.
<Name of Log File>	The name of the log file to repair.

Example - Repairing the Audit log file

```
fw repairlog -u 2019-06-17_000000.adtlog
```

fw sam

Description

Manages the Suspicious Activity Monitoring (SAM) rules. You can use the SAM rules to block connections to and from IP addresses without the need to change or reinstall the Security Policy. For more information, see sk112061.

You can create the Suspicious Activity Rules in two ways:

- In SmartConsole from Monitoring Results
- In CLI with the `fw sam` command

Notes:

- VSX Gateways and VSX Cluster Members do not support Suspicious Activity Monitoring (SAM) Rules. See sk79700.
- See the "`fw sam_policy`" and "`sam_alert`" commands.
- SAM rules consume some CPU resources on Security Gateway.

  Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.
- Logs for enforced SAM rules (configured with the `fw sam` command) are stored in the `$FWDIR/log/sam.dat` file.
  By design, the file is purged when the number of stored entries reaches 100,000.
  This data log file contains the records in one of these formats:

  ```
  <type>,<actions>,<expire>,<ipaddr>
  ```

  ```
  <type>,<actions>,<expire>,<src>,<dst>,<dport>,<ip_p>
  ```
- SAM Requests are stored on the Security Gateway in the kernel table `sam_requests`.
- IP Addresses that are blocked by SAM rules, are stored on the Security Gateway in the kernel table `sam_blocked_ips`.

Note - To configure SAM Server settings for a Security Gateway or Cluster:

1. Connect with SmartConsole to the applicable Security Management Server or Domain Management Server.
2. From the left navigation panel, click Gateways & Servers.
3. Open the Security Gateway or Cluster object.
4. From the left tree, click **Other > SAM**.
5. Configure the settings.
6. Click **OK**.
7. Install the Access Control Policy on this Security Gateway or Cluster object.

Syntax

- **To add or cancel a SAM rule according to criteria:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM
Server>] [-f <Security Gateway>] [-t <Timeout>] [-l <Log
Type>] [-C] [-e <key=val>]+ [-r] -{n|i|I|j|J} <Criteria>
```

- **To delete all SAM rules:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM
Server>] [-f <Security Gateway>] -D
```

- **To monitor all SAM rules:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM
Server>] [-f <Security Gateway>] [-r] -M -{i|j|n|b|q} all
```

- **To monitor SAM rules according to criteria:**

```
fw [-d] sam [-v] [-s <SAM Server>] [-S <SIC Name of SAM
Server>] [-f <Security Gateway>] [-r] -M -{i|j|n|b|q}
<Criteria>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-v`	Enables verbose mode. In this mode, the command writes one message to *stderr* for each Security Gateway, on which the command is enforced. These messages show whether the command was successful or not.
`-s <SAM Server>`	Specifies the IP address (in the X.X.X.X format) or resolvable HostName of the Security Gateway that enforces the command. The default is `localhost`.

Parameter	Description
`-S <SIC Name of SAM Server>`	Specifies the SIC name for the SAM server to be contacted. It is expected that the SAM server has this SIC name, otherwise the connection fails. **Notes:** ■ If you do not explicitly specify the SIC name, the connection continues without SIC names comparison. ■ For more information about enabling SIC, refer to the OPSEC API Specification. ■ On VSX Gateway, run the *fw vsx showncs -vs <VSID>* command to show the SIC name for the applicable Virtual System.
`-f <Security Gateway>`	Specifies the Security Gateway, on which to enforce the action. `<Security Gateway>` can be one of these: ■ *All* - Default. Specifies to enforce the action on all managed Security Gateways, where SAM Server runs. You can use this syntax only on Security Management Server or Domain Management Server. ■ *localhost* - Specifies to enforce the action on this local Check Point server (on which the `fw sam` command is executed). You can use this syntax only on Security Gateway or StandAlone. ■ *Gateways* - Specifies to enforce the action on all objects defined as Security Gateways, on which SAM Server runs. You can use this syntax only on Security Management Server or Domain Management Server. ■ *Name of Security Gateway object* - Specifies to enforce the action on this specific Security Gateway object. You can use this syntax only on Security Management Server or Domain Management Server. ■ *Name of Group object* - Specifies to enforce the action on all specific Security Gateways in this Group object. **Notes:** ■ You can use this syntax only on Security Management Server or Domain Management Server. ■ VSX Gateways and VSX Cluster Members do not support Suspicious Activity Monitoring (SAM) Rules. See sk79700.
`-D`	Cancels all inhibit ("`-i`", "`-j`", "`-I`", "`-J`") and notify ("`-n`") parameters. **Notes:** ■ To "uninhibit" the inhibited connections, run the `fw sam` command with the "`-C`" or "`-D`" parameters. ■ It is also possible to use this command for active SAM requests.

Parameter	Description
`-C`	Cancels the `fw sam` command to inhibit connections with the specified parameters. **Notes:** ■ These connections are no longer inhibited (no longer rejected or dropped). ■ The command parameters must match the parameters in the original `fw sam` command, except for the `-t <Timeout>` parameter.
`-t <Timeout>`	Specifies the time period (in seconds), during which the action is enforced. The default is forever, or until you cancel the `fw sam` command.
`-l <Log Type>`	Specifies the type of the log for enforced action: ■ `nolog` - Does not generate Log / Alert at all ■ `short_noalert` - Generates a Log ■ `short_alert` - Generates an Alert ■ `long_noalert` - Generates a Log ■ `long_alert` - Generates an Alert (this is the default)
`-e <key=val>+`	Specifies rule information based on the keys and the provided values. Multiple keys are separated by the plus sign (+). Available keys are (each is limited to 100 characters): ■ `name` - Security rule name ■ `comment` - Security rule comment ■ `originator` - Security rule originator's username
`-r`	Specifies not to resolve IP addresses.
`-n`	Specifies to generate a "Notify" long-format log entry. **Notes:** ■ This parameter generates an alert when connections that match the specified services or IP addresses pass through the Security Gateway. ■ This action does not inhibit / close connections.
`-i`	Inhibits (drops or rejects) new connections with the specified parameters. **Notes:** ■ Each inhibited connection is logged according to the log type. ■ Matching connections are rejected.

Parameter	Description
`-I`	Inhibits (drops or rejects) new connections with the specified parameters, and closes all existing connections with the specified parameters. **Notes:** ■ Matching connections are rejected. ■ Each inhibited connection is logged according to the log type.
`-j`	Inhibits (drops or rejects) new connections with the specified parameters. **Notes:** ■ Matching connections are dropped. ■ Each inhibited connection is logged according to the log type.
`-J`	Inhibits new connections with the specified parameters, and closes all existing connections with the specified parameters. **Notes:** ■ Matching connections are dropped. ■ Each inhibited connection is logged according to the log type.
`-b`	Bypasses new connections with the specified parameters.
`-q`	Quarantines new connections with the specified parameters.
`-M`	Monitors the active SAM requests with the specified actions and criteria.
`all`	Gets all active SAM requests. This is used for monitoring purposes only.
`<Criteria>`	Criteria are used to match connections. The criteria and are composed of various combinations of the following parameters: ■ Source IP Address ■ Source Netmask ■ Destination IP Address ■ Destination Netmask ■ Port (see *IANA Service Name and Port Number Registry*) ■ Protocol Number (see *IANA Protocol Numbers*)

Parameter	Description
	Possible combinations are (see the explanations below this table): ■ src *<IP>* ■ dst *<IP>* ■ any *<IP>* ■ subsrc *<IP> <Netmask>* ■ subdst *<IP> <Netmask>* ■ subany *<IP> <Netmask>* ■ srv *<Src IP> <Dest IP> <Port> <Protocol>* ■ subsrv *<Src IP> <Src Netmask> <Dest IP> <Dest Netmask> <Port> <Protocol>* ■ subsrvs *<Src IP> <Src Netmask> <Dest IP> <Port> <Protocol>* ■ subsrvd *<Src IP> <Dest IP> <Dest Netmask> <Port> <Protocol>* ■ dstsrv *<Dest IP> <Port> <Protocol>* ■ subdstsrv *<Dest IP> <Dest Netmask> <Port> <Protocol>* ■ srcpr *<IP> <Protocol>* ■ dstpr *<IP> <Protocol>* ■ subsrcpr *<IP> <Netmask> <Protocol>* ■ subdstpr *<IP> <Netmask> <Protocol>* ■ generic *<key=val>*

Explanation for the *<Criteria>* syntax

Parameter	Description
src *<IP>*	Matches the Source IP address of the connection.
dst <IP>	Matches the Destination IP address of the connection.
any *<IP>*	Matches either the Source IP address or the Destination IP address of the connection.
subsrc *<IP> <Netmask>*	Matches the Source IP address of the connections according to the netmask.
subdst *<IP> <Netmask>*	Matches the Destination IP address of the connections according to the netmask.

Parameter	Description
`subany <IP> <Netmask>`	Matches either the Source IP address or Destination IP address of connections according to the netmask.
`srv <Src IP> <Dest IP> <Port> <Protocol>`	Matches the specific Source IP address, Destination IP address, Service (port number) and Protocol.
`subsrv <Src IP> <Netmask> <Dest IP> <Netmask> <Port> <Protocol>`	Matches the specific Source IP address, Destination IP address, Service (port number) and Protocol. Source and Destination IP addresses are assigned according to the netmask.
`subsrvs <Src IP> <Src Netmask> <Dest IP> <Port> <Protocol>`	Matches the specific Source IP address, source netmask, destination netmask, Service (port number) and Protocol.
`subsrvd <Src IP> <Dest IP> <Dest Netmask> <Port> <Protocol>`	Matches specific Source IP address, Destination IP, destination netmask, Service (port number) and Protocol.
`dstsrv <Dest IP> <Service> <Protocol>`	Matches specific Destination IP address, Service (port number) and Protocol.
`subdstsrv <Dest IP> <Netmask> <Port> <Protocol>`	Matches specific Destination IP address, Service (port number) and Protocol. Destination IP address is assigned according to the netmask.
`srcpr <IP> <Protocol>`	Matches the Source IP address and protocol.
`dstpr <IP> <Protocol>`	Matches the Destination IP address and protocol.
`subsrcpr <IP> <Netmask> <Protocol>`	Matches the Source IP address and protocol of connections. Source IP address is assigned according to the netmask.
`subdstpr <IP> <Netmask> <Protocol>`	Matches the Destination IP address and protocol of connections. Destination IP address is assigned according to the netmask.

Parameter	Description
`generic <key=val>+`	Matches the GTP connections based on the specified keys and provided values. Multiple keys are separated by the plus sign (+). Available keys are: ■ `service=gtp` ■ `imsi` ■ `msisdn` ■ `apn` ■ `tunl_dst` ■ `tunl_dport` ■ `tunl_proto`

fw sam_policy

Description

Manages the Suspicious Activity Policy editor that works with these types of rules:

- Suspicious Activity Monitoring (SAM) rules.

  See sk112061: How to create and view Suspicious Activity Monitoring (SAM) Rules.

- Rate Limiting rules.

  See sk112454: How to configure Rate Limiting rules for DoS Mitigation.

Also, see these commands:

- *"fw sam" on page 295*
- *"sam_alert" on page 405*

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax for IPv4

```
fw [-d] sam_policy
      add <options>
      batch
      del <options>
      get <options>
```

```
fw [-d] samp
      add <options>
      batch
      del <options>
      get <options>
```

Syntax for IPv6

```
fw6 [-d] sam_policy
      add <options>
      batch
      del <options>
      get <options>
```

```
fw6 [-d] samp
      add <options>
      batch
      del <options>
      get <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`add <options>`	Adds one Rate Limiting rule one at a time. See *"fw sam_policy add" on page 306*.
`batch`	Adds or deletes many Rate Limiting rules at a time. See *"fw sam_policy batch" on page 319*.
`del <options>`	Deletes one configured Rate Limiting rule one at a time. See *"fw sam_policy del" on page 321*.
`get <options>`	Shows all the configured Rate Limiting rules. See *"fw sam_policy get" on page 324*.

fw sam_policy add

Description

The "*fw sam_policy add*" and "*fw6 sam_policy add*" commands:

- Add one Suspicious Activity Monitoring (SAM) rule at a time.
- Add one Rate Limiting rule at a time.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax to configure a Suspicious Activity Monitoring (SAM) rule for IPv4

```
fw [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] ip <IP Filter Arguments>
```

Syntax to configure a Suspicious Activity Monitoring (SAM) rule for IPv6

```
fw6 [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] ip <IP Filter Arguments>
```

Syntax to configure a Rate Limiting rule for IPv4

```
fw [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] quota <Quota Filter Arguments>
```

Syntax to configure a Rate Limiting rule for IPv6

```
fw6 [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] quota <Quota Filter Arguments
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-u`	Optional. Specifies that the rule category is `User-defined`. Default rule category is `Auto`.
`-a {d | n | b}`	Mandatory. Specifies the rule action if the traffic matches the rule conditions: ■ `d` - Drop the connection. ■ `n` - Notify (generate a log) about the connection and let it through. ■ `b` - Bypass the connection - let it through without checking it against the policy rules. **Note** - Rules with action set to *Bypass* cannot have a log or limit specification. Bypassed packets and connections do not count towards overall number of packets and connection for limit enforcement of type ratio.
`-l {r | a}`	Optional. Specifies which type of log to generate for this rule for all traffic that matches: ■ `-r` - Generate a regular log ■ `-a` - Generate an alert log

Parameter	Description
`-t <Timeout>`	Optional. Specifies the time period (in seconds), during which the rule will be enforced. Default timeout is indefinite.
`-f <Target>`	Optional. Specifies the target Security Gateways, on which to enforce the Rate Limiting rule. *<Target>* can be one of these: ■ `all` - This is the default option. Specifies that the rule should be enforced on all managed Security Gateways. ■ Name of the Security Gateway or Cluster object - Specifies that the rule should be enforced only on this Security Gateway or Cluster object (the object name must be as defined in the SmartConsole). ■ Name of the Group object - Specifies that the rule should be enforced on all Security Gateways that are members of this Group object (the object name must be as defined in the SmartConsole).
`-n "<Rule Name>"`	Optional. Specifies the name (label) for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters. ■ Before each space or a backslash character in this string, you must write a backslash (\) character. Example: `"This\ is\ a\ rule\ name\ with\ a\ backslash\ \\"`
`-c "<Rule Comment>"`	Optional. Specifies the comment for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters. ■ Before each space or a backslash character in this string, you must write a backslash (\) character. Example: `"This\ is\ a\ comment\ with\ a\ backslash\ \\"`

Parameter	Description
`-o "<Rule Originator>"`	Optional. Specifies the name of the originator for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters. ■ Before each space or a backslash character in this string, you must write a backslash (\) character. Example: `"Created\ by\ John\ Doe"`
`-z "<Zone>"`	Optional. Specifies the name of the Security Zone for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters.
`ip <IP Filter Arguments>`	Mandatory (use this `ip` parameter, or the `quota` parameter). Configures the *Suspicious Activity Monitoring (SAM)* rule. Specifies the IP Filter Arguments for the SAM rule (you must use at least one of these options): `[-C] [-s <Source IP>] [-m <Source Mask>] [-d <Destination IP>] [-M <Destination Mask>] [-p <Port>] [-r <Protocol>]` See the explanations below.

Parameter	Description
`quota <Quota Filter Arguments>`	Mandatory (use this `quota` parameter, or the `ip` parameter). Configures the *Rate Limiting* rule. Specifies the Quota Filter Arguments for the Rate Limiting rule (see the explanations below): ■ `[flush true]` ■ `[source-negated {true | false}] source <Source>` ■ `[destination-negated {true | false}] destination <Destination>` ■ `[service-negated {true | false}] service <Protocol and Port numbers>` ■ `[<Limit1 Name> <Limit1 Value>] [<Limit2 Name> <Limit2 Value>] ...[<LimitN Name> <LimitN Value>]` ■ `[track <Track>]` **Important:** ■ The Quota rules are not applied immediately to the Security Gateway. They are only registered in the Suspicious Activity Monitoring (SAM) policy database. To apply all the rules from the SAM policy database immediately, add "`flush true`" in the `fw samp add` command syntax. ■ Explanation: For new connections rate (and for any rate limiting in general), when a rule's limit is violated, the Security Gateway also drops all packets that match the rule. The Security Gateway computes new connection rates on a per-second basis. At the start of the 1-second timer, the Security Gateway allows all packets, including packets for existing connections. If, at some point, during that 1 second period, there are too many new connections, then the Security Gateway blocks all remaining packets for the remainder of that 1-second interval. At the start of the next 1-second interval, the counters are reset, and the process starts over - the Security Gateway allows packets to pass again up to the point, where the rule's limit is violated.

Explanation for the *IP Filter Arguments* syntax for Suspicious Activity Monitoring (SAM) rules

Argument	Description
`-C`	Specifies that open connections should be closed.
`-s <Source IP>`	Specifies the Source IP address.
`-m <Source Mask>`	Specifies the Source subnet mask (in dotted decimal format - x.y.z.w).
`-d <Destination IP>`	Specifies the Destination IP address.
`-M <Destination Mask>`	Specifies the Destination subnet mask (in dotted decimal format - x.y.z.w).
`-p <Port>`	Specifies the port number (see *IANA Service Name and Port Number Registry*).
`-r <Protocol>`	Specifies the protocol number (see *IANA Protocol Numbers*).

Explanation for the *Quota Filter Arguments* syntax for Rate Limiting rules

Argument	Description
`flush true`	Specifies to compile and load the quota rule to the SecureXL immediately.
`[source-negated {true | false}] source <Source>`	Specifies the source type and its value: ■ `any` The rule is applied to packets sent from all sources. ■ `range:<IP Address>` or `range:<IP Address Start>-<IP Address End>` The rule is applied to packets sent from: • Specified IPv4 addresses (x.y.z.w) • Specified IPv6 addresses (xxxx:yyyy:....:zzzz) ■ `cidr:<IP Address>/<Prefix>` The rule is applied to packets sent from: • IPv4 address with Prefix from 0 to 32 • IPv6 address with Prefix from 0 to 128 ■ `cc:<Country Code>` The rule matches the country code to the source IP addresses assigned to this country, based on the Geo IP database. The two-letter codes are defined in ISO 3166-1 alpha-2. ■ `asn:<Autonomous System Number>` The rule matches the AS number of the organization to the source IP addresses that are assigned to this organization, based on the Geo IP database. The valid syntax is *ASnnnn*, where *nnnn* is a number unique to the specific organization. **Notes:** ■ Default is: `source-negated false` ■ The `source-negated true` processes all source types, *except* the specified type.

Argument	Description
`[destination-negated {true | false}] destination <Destination>`	Specifies the destination type and its value: ■ `any` The rule is applied to packets sent to all destinations. ■ `range:<IP Address>` or `range:<IP Address Start>-<IP Address End>` The rule is applied to packets sent to: • Specified IPv4 addresses (x.y.z.w) • Specified IPv6 addresses (xxxx:yyyy:...:zzzz) ■ `cidr:<IP Address>/<Prefix>` The rule is applied to packets sent to: • IPv4 address with Prefix from 0 to 32 • IPv6 address with Prefix from 0 to 128 ■ `cc:<Country Code>` The rule matches the country code to the destination IP addresses assigned to this country, based on the Geo IP database. The two-letter codes are defined in ISO 3166-1 alpha-2. ■ `asn:<Autonomous System Number>` The rule matches the AS number of the organization to the destination IP addresses that are assigned to this organization, based on the Geo IP database. The valid syntax is *ASnnnn*, where *nnnn* is a number unique to the specific organization. **Notes:** ■ Default is: `destination-negated false` ■ The `destination-negated true` will process all destination types except the specified type

Argument	Description
`[service-negated {true | false}] service <Protocol and Port numbers>`	Specifies the Protocol number (see *IANA Protocol Numbers*) and Port number (see *IANA Service Name and Port Number Registry*): ■ `<Protocol>` IP protocol number in the range 1-255 ■ `<Protocol Start>-<Protocol End>` Range of IP protocol numbers ■ `<Protocol>/<Port>` IP protocol number in the range 1-255 and TCP/UDP port number in the range 1-65535 ■ `<Protocol>/<Port Start>-<Port End>` IP protocol number and range of TCP/UDP port numbers from 1 to 65535 **Notes:** ■ Default is: `service-negated false` ■ The `service-negated true` will process all traffic except the traffic with the specified protocols and ports

Argument	Description
`[<Limit 1 Name> <Limit 1 Value>] [<Limit 2 Name> <Limit 2 Value>] ... [<Limit N Name> <Limit N Value>]`	Specifies quota limits and their values. **Note** - Separate multiple quota limits with spaces. ■ `concurrent-conns <Value>` Specifies the maximal number of concurrent active connections that match this rule. ■ `concurrent-conns-ratio <Value>` Specifies the maximal ratio of the *concurrent-conns* value to the total number of active connections through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`). ■ `pkt-rate <Value>` Specifies the maximum number of packets per second that match this rule. ■ `pkt-rate-ratio <Value>` Specifies the maximal ratio of the *pkt-rate* value to the rate of all connections through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`). ■ `byte-rate <Value>` Specifies the maximal total number of bytes per second in packets that match this rule. ■ `byte-rate-ratio <Value>` Specifies the maximal ratio of the *byte-rate* value to the bytes per second rate of all connections through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`). ■ `new-conn-rate <Value>` Specifies the maximal number of connections per second that match the rule. ■ `new-conn-rate-ratio <Value>` Specifies the maximal ratio of the *new-conn-rate* value to the rate of all connections per second through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`).

Argument	Description
`[track <Track>]`	Specifies the tracking option: ■ `source` Counts connections, packets, and bytes for specific source IP address, and not cumulatively for this rule. ■ `source-service` Counts connections, packets, and bytes for specific source IP address, and for specific IP protocol and destination port, and not cumulatively for this rule.

Examples

Example 1 - Rate Limiting rule with a range

```
fw sam_policy add -a d -l r -t 3600 quota service any source range:172.16.7.11-172.16.7.13 new-conn-rate 5 flush true
```

Explanations:

- This rule drops packets for all connections (`-a d`) that exceed the quota set by this rule, including packets for existing connections.
- This rule logs packets (`-l r`) that exceed the quota set by this rule.
- This rule will expire in 3600 seconds (`-t 3600`).
- This rule limits the rate of creation of new connections to 5 connections per second (`new-conn-rate 5`) for any traffic (`service any`) from the source IP addresses in the range 172.16.7.11 - 172.16.7.13 (`source range:172.16.7.11-172.16.7.13`).

  Note - The limit of the total number of log entries per second is configured with the *fwaccel dos config set -n <rate>* command.
- This rule will be compiled and loaded on the SecureXL, together with other rules in the Suspicious Activity Monitoring (SAM) policy database immediately, because this rule includes the "`flush true`" parameter.

Example 2 - Rate Limiting rule with a service specification

```
fw sam_policy add -a n -l r quota service 1,50-51,6/443,17/53 service-negated true source cc:QQ byte-rate 0
```

Explanations:

- This rule logs and lets through all packets (`-a n`) that exceed the quota set by this rule.
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to all packets except (`service-negated true`) the packets with IP protocol number 1, 50-51, 6 port 443 and 17 port 53 (`service 1,50-51,6/443,17/53`).
- This rule applies to all packets from source IP addresses that are assigned to the country with specified country code (`cc:QQ`).
- This rule does not let any traffic through (`byte-rate 0`) except the packets with IP protocol number 1, 50-51, 6 port 443 and 17 port 53.
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

Example 3 - Rate Limiting rule with ASN

```
fw sam_policy -a d quota source asn:AS64500,cidr:[::FFFF:C0A8:1100]/120 service any pkt-rate 0
```

Explanations:

- This rule drops (`-a d`) all packets that match this rule.
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to packets from the Autonomous System number 64500 (`asn:AS64500`).
- This rule applies to packets from source IPv6 addresses FFFF:C0A8:1100/120 (`cidr:[::FFFF:C0A8:1100]/120`).
- This rule applies to all traffic (`service any`).
- This rule does not let any traffic through (`pkt-rate 0`).
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

Example 4 - Rate Limiting rule with an Allow List

```
fw sam_policy add -a b quota source range:172.16.8.17-172.16.9.121 service 6/80
```

Explanations:

- This rule bypasses (`-a b`) all packets that match this rule.

  Note - The Access Control Policy and other types of security policy rules still apply.
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to packets from the source IP addresses in the range 172.16.8.17 - 172.16.9.121 (`range:172.16.8.17-172.16.9.121`).
- This rule applies to packets sent to TCP port 80 (`service 6/80`).
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

Example 5 - Rate Limiting rule with tracking

```
fw sam_policy add -a d quota service any source-negated true source cc:QQ concurrent-conns-ratio 655 track source
```

Explanations:

- This rule drops (`-a d`) all packets that match this rule.
- This rule does not log any packets (the `-l r` parameter is not specified).
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to all traffic (`service any`).
- This rule applies to all sources except (`source-negated true`) the source IP addresses that are assigned to the country with specified country code (`cc:QQ`).
- This rule limits the maximal number of concurrent active connections to 655/65536=~1% (`concurrent-conns-ratio 655`) for any traffic (`service any`) except (`service-negated true`) the connections from the source IP addresses that are assigned to the country with specified country code (`cc:QQ`).
- This rule counts connections, packets, and bytes for traffic only from sources that match this rule, and not cumulatively for this rule.
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

fw sam_policy batch

Description

The "*fw sam_policy batch*" and "*fw6 sam_policy batch*" commands:

- Add and delete many Suspicious Activity Monitoring (SAM) rules at a time.
- Add and delete many Rate Limiting rules at a time.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Procedure

1. **Start the batch mode**

   - For IPv4, run:

     ```
     fw sam_policy batch << EOF
     ```

   - For IPv6, run:

     ```
     fw6 sam_policy batch << EOF
     ```

2. **Enter the applicable commands**

   - Enter one "`add`" or "`del`" command on each line, on as many lines as necessary.

     Start each line with only "`add`" or "`del`" parameter (not with "`fw samp`").
   - Use the same set of parameters and values as described in these commands:
     - `fw sam_policy add`
     - `fw sam_policy del`
   - Terminate each line with a Return (ASCII 10 - Line Feed) character (press Enter).

3. **End the batch mode**

   Type `EOF` and press Enter.

Example of a Rate Limiting rule for IPv4

```
[Expert@HostName]# fw samp batch <<EOF

add -a d -l r -t 3600 -c "Limit\ conn\ rate\ to\ 5\ conn/sec from\ these\ sources" quota service
any source range:172.16.7.13-172.16.7.13 new-conn-rate 5

del <501f6ef0,00000000,cb38a8c0,0a0afffe>

add -a b quota source range:172.16.8.17-172.16.9.121 service 6/80

EOF
[Expert@HostName]#
```

fw sam_policy del

Description

The "*fw sam_policy del*" and "*fw6 sam_policy del*" commands:

- Delete one configured Suspicious Activity Monitoring (SAM) rule at a time.
- Delete one configured Rate Limiting rule at a time.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax for IPv4

```
fw [-d] sam_policy del '<Rule UID>'
```

Syntax for IPv6

```
fw6 [-d] sam_policy del '<Rule UID>'
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`'<Rule UID>'`	Specifies the UID of the rule you wish to delete. **Important:** ■ The quote marks and angle brackets (`'<...>'`) are mandatory. ■ To see the Rule UID, run the "`fw sam_policy get`" command.

Procedure

1. **List all the existing rules in the Suspicious Activity Monitoring policy database**

   List all the existing rules in the Suspicious Activity Monitoring policy database.

   - For IPv4, run:

     ```
     fw sam_policy get
     ```

   - For IPv6, run:

     ```
     fw6 sam_policy get
     ```

   The rules show in this format:

   ```
   operation=add uid=<Value1,Value2,Value3,Value4> target=...
   timeout=... action=... log= ... name= ... comment=...
   originator= ... src_ip_addr=... req_tpe=...
   ```

   Example for IPv4:

   ```
   operation=add uid=<5ac3965f,00000000,3403a8c0,0000264a>
   target=all timeout=300 action=notify log=log name=Test\ Rule
   comment=Notify\ about\ traffic\ from\ 1.1.1.1
   originator=John\ Doe src_ip_addr=1.1.1.1 req_tpe=ip
   ```

2. **Delete a rule from the list by its UID**

   - For IPv4, run:

     ```
     fw [-d] sam_policy del '<Rule UID>'
     ```

   - For IPv6, run:

     ```
     fw6 [-d] sam_policy del '<Rule UID>'
     ```

   Example for IPv4:

   ```
   fw samp del '<5ac3965f,00000000,3403a8c0,0000264a>'
   ```

3. **Add the flush-only rule**

   - For IPv4, run:

     ```
     fw samp add -t 2 quota flush true
     ```

   - For IPv6, run:

     ```
     fw6 samp add -t 2 quota flush true
     ```

   Explanation:

   The "`fw samp del`" and "`fw6 samp del`" commands only remove a rule from the persistent database. The Security Gateway continues to enforce the deleted rule until the next time you compiled and load a policy. To force the rule deletion immediately, you must enter a flush-only rule right after the "`fw samp del`" and "`fw6 samp del`" command. This flush-only rule immediately deletes the rule you specified in the previous step, and times out in 2 seconds.

   Best Practice - Specify a short timeout period for the flush-only rules. This prevents accumulation of rules that are obsolete in the database.

fw sam_policy get

Description

The "*fw sam_policy get*" and "*fw6 sam_policy get*" commands:

- Show all the configured Suspicious Activity Monitoring (SAM) rules.
- Show all the configured Rate Limiting rules.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax for IPv4

```
fw [-d] sam_policy get [-l] [-u '<Rule UID>'] [-k '<Key>' -t
<Type> [+{-v '<Value>'}] [-n]]
```

Syntax for IPv6

```
fw6 [-d] sam_policy get [-l] [-u '<Rule UID>'] [-k '<Key>' -t
<Type> [+{-v '<Value>'}] [-n]]
```

Parameters

Note - All these parameters are optional.

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-l`	Controls how to print the rules: ■ In the default format (without "`-l`"), the output shows each rule on a separate line. ■ In the list format (with "`-l`"), the output shows each parameter of a rule on a separate line. ■ See the "`fw sam_policy add`" command.
`-u '<`*`Rule UID`*`>'`	Prints the rule specified by its Rule UID or its zero-based rule index. The quote marks and angle brackets ('<...>') are mandatory.
`-k '<`*`Key`*`>'`	Prints the rules with the specified predicate key. The quote marks are mandatory.
`-t <`*`Type`*`>`	Prints the rules with the specified predicate type. For Rate Limiting rules, you must always use "`-t in`".
`+{-v '<`*`Value`*`>'}`	Prints the rules with the specified predicate values. The quote marks are mandatory.
`-n`	Negates the condition specified by these predicate parameters: ■ `-k` ■ `-t` ■ `+-v`

Examples

Example 1 - Output in the default format

```
[Expert@HostName:0]# fw samp get

operation=add uid=<5ac3965f,00000000,3403a8c0,0000264a> target=all timeout=300 action=notify
log=log name=Test\ Rule comment=Notify\ about\ traffic\ from\ 1.1.1.1 originator=John\ Doe
src_ip_addr=1.1.1.1 req_tpe=ip
```

Example 2 - Output in the list format

```
[Expert@HostName:0]# fw samp get -l

uid
<5ac3965f,00000000,3403a8c0,0000264a>
target
all
timeout
2147483647
action
notify
log
log
name
Test\ Rule
comment
Notify\ about\ traffic\ from\ 1.1.1.1
originator
John\ Doe
src_ip_addr
1.1.1.1
req_type
ip
```

Example 3 - Printing a rule by its Rule UID

```
[Expert@HostName:0]# fw samp get -u '<5ac3965f,00000000,3403a8c0,0000264a>'
0
operation=add uid=<5ac3965f,00000000,3403a8c0,0000264a> target=all timeout=300 action=notify
log=log name=Test\ Rule comment=Notify\ about\ traffic\ from\ 1.1.1.1 originator=John\ Doe
src_ip_addr=1.1.1.1 req_tpe=ip
```

Example 4 - Printing rules that match the specified filters

```
[Expert@HostName:0]# fw samp get
no corresponding SAM policy requests
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a d -l r -t 3600 quota service any source
range:172.16.7.11-172.16.7.13 new-conn-rate 5 flush true
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a n -l r quota service 1,50-51,6/443,17/53 service-negated
true source cc:QQ byte-rate 0
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a b quota source range:172.16.8.17-172.16.9.121 service
6/80
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a d quota service any source-negated true source cc:QQ
concurrent-conns-ratio 655 track source
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get
operation=add uid=<5bab3acf,00000000,3503a8c0,00003ddc> target=all timeout=indefinite
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
operation=add uid=<5bab3ac6,00000000,3503a8c0,00003dbf> target=all timeout=3586 action=drop
log=log service=any source=range:172.16.7.11-172.16.7.13 new-conn-rate=5 flush=true req_
type=quota
operation=add uid=<5bab3acc,00000000,3503a8c0,00003dd7> target=all timeout=indefinite
action=bypass source=range:172.16.8.17-172.16.9.121 service=6/80 req_type=quota
operation=add uid=<5bab3ac9,00000000,3503a8c0,00003dd5> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'service' -t in -v '6/80'
operation=add uid=<5bab3acc,00000000,3503a8c0,00003dd7> target=all timeout=indefinite
action=bypass source=range:172.16.8.17-172.16.9.121 service=6/80 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'service-negated' -t in -v 'true'
operation=add uid=<5bab3ac9,00000000,3503a8c0,00003dd5> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'source' -t in -v 'cc:QQ'
operation=add uid=<5bab3acf,00000000,3503a8c0,00003ddc> target=all timeout=indefinite
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
operation=add uid=<5bab3ac9,00000000,3503a8c0,00003dd5> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k source -t in -v 'cc:QQ' -n
operation=add uid=<5bab3ac6,00000000,3503a8c0,00003dbf> target=all timeout=3291 action=drop
log=log service=any source=range:172.16.7.11-172.16.7.13 new-conn-rate=5 flush=true req_
type=quota
operation=add uid=<5bab3acc,00000000,3503a8c0,00003dd7> target=all timeout=indefinite
action=bypass source=range:172.16.8.17-172.16.9.121 service=6/80 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'source-negated' -t in -v 'true'
operation=add uid=<5baa94e0,00000000,860318ac,00003016> target=all timeout=indefinite
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'byte-rate' -t in -v '0'
operation=add uid=<5baa9431,00000000,860318ac,00002efd> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'flush' -t in -v 'true'
operation=add uid=<5baa9422,00000000,860318ac,00002eea> target=all timeout=2841 action=drop
log=log service=any source=range:172.16.7.11-172.16.7.13 new-conn-rate=5 flush=true req_
type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'concurrent-conns-ratio' -t in -v '655'
operation=add uid=<5baa94e0,00000000,860318ac,00003016> target=all timeout=indefinite
```

```
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
[Expert@HostName:0]#
```

fw sdwan

Description

- Shows the current installed SD-WAN Policy on the Security Gateway.
- Fetches the SD-WAN Policy from a local directory on the Security Gateway.

For more information about SD-WAN, see sk180605.

Important - You can run this command in the Expert mode or in Gaia Clish.

Syntax

- To show the built-in help:

```
fw sdwan
```

- To show the current installed SD-WAN policy on the Security Gateway:

```
fw [-d] sdwan stat
```

- To fetch the SD-WAN policy stored locally on the Security Gateway in the default directory `$FWDIR/state/`:

```
fw [-d] sdwan fetch local
```

- To fetch the SD-WAN policy stored locally on the Security Gateway in the specified directory:

```
fw [-d] sdwan fetchlocal -d <Full Path to Directory>
```

Warning - It is **not** supported to run these commands manually (they can only be executed by internal tasks on the Security Gateway):

- `fw sdwan uninstall`
- `fw sdwan unload`

Parameters

Parameter	Description
`fw -d ...`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-d <Full Path to Directory>`	Specifies the local directory on the Security Gateway, from which to fetch the policy files.

Example

```
[Expert@MyGW:0]# fw sdwan stat
POLICY                DATE
SD-WAN Policy         Thu Dec 15 15:34:03 2023
[Expert@MyGW:0]#
```

fw showuptables

Description

Shows the formatted contents of the Unified Policy kernel tables.

Syntax

```
fw [-d] showuptables
       [-h]
       [-i]
```

Parameters

Parameter	Description
-d	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the script command to save the entire CLI session.
-h	Shows the built-in usage.
-i	Shows the implied rules layers.

fw stat

Description

Shows the following information about the policy on the Security Gateway:

- Name of the installed policy.
- Date of the last policy installation.
- Names of the interfaces protected by the installed policy, and in which direction the policy protects them.

Important - This command is outdated and exists only for backward compatibility with very old versions. Use the "`cpstat -f policy fw`" command instead (see *"cpstat" on page 1019*).

Syntax

```
fw [-d] stat [-l | -s] [<Name of Object>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
No Parameters	Shows default output - all information is on one line.

Parameter	Description
`-l`	Shows long output. Shows each interface and its protected traffic direction is on a separate line. In addition, shows this information: ■ `Total` - Number of packets the Security Gateway received on this interface ■ `Reject` - Number of packets the Security Gateway rejected on this interface ■ `Drop` - Number of packets the Security Gateway dropped on this interface ■ `Accept` - Number of packets the Security Gateway accepted on this interface ■ `Log` - Whether Security Gateway sends its logs from this interface (0 - no, 1 - yes)
`-s`	Shows short output. Shows each interface and its protected traffic direction is on a separate line.
<Name of Object>	Specifies the name of the Security Gateway or Cluster Member object (as defined in SmartConsole), from which to show the information. Use this parameter only on the Management Server. This requires the established SIC with that Check Point server.

Example 1 - Default output

```
[Expert@MyGW:0]# fw stat
HOST POLICY DATE
localhost MyGW_Policy 10Sep2018 14:01:25 : [>eth0] [<eth0] [>eth1]
[Expert@MyGW:0]#
```

Example 2 - Short output

```
[Expert@MyGW:0]# fw stat -s
HOST IF POLICY DATE
localhost >eth0 MyGW_Policy 10Sep2018 14:01:25 :
localhost <eth0 MyGW_Policy 10Sep2018 14:01:25 :
localhost >eth1 MyGW_Policy 10Sep2018 14:01:25 :
[Expert@MyGW:0]#
```

Example 3 - Long output

```
[Expert@MyGW:0]# fw stat -l
HOST IF POLICY DATE TOTAL REJECT DROP ACCEPT LOG
localhost >eth0 MyGW_Policy 10Sep2018 14:01:25 : 14377 0 316 14061 1
localhost <eth0 MyGW_Policy 10Sep2018 14:01:25 : 60996 0 0 60996 0
localhost >eth1 MyGW_Policy 10Sep2018 14:01:25 : 304 0 304 0 0
[Expert@MyGW:0]#
```

Example 4 - Long output from the Management Server

```
[Expert@MGMY:0]# fw stat -l MyGW
HOST IF POLICY DATE TOTAL REJECT DROP ACCEPT LOG
MyGW >eth0 MyGW_Policy 12Sep2018 16:34:56 : 120113 0 0 120113 0
MyGW <eth0 MyGW_Policy 12Sep2018 16:34:56 : 10807 0 0 10807 0
MyGW >eth2 MyGW_Policy 12Sep2018 16:34:56 : 3 0 0 3 0
MyGW <eth2 MyGW_Policy 12Sep2018 16:34:56 : 3 0 0 3 0
[Expert@MGMT:0]#
```

fw tab

Description

Shows data from the specified Security Gateway kernel tables.

This command also changes the content of dynamic kernel tables. You cannot change the content of static kernel tables.

Kernel tables (also known as State tables) store data that the Firewall and other Software Blades use to inspect packets. These kernel tables are a critical component of Stateful Inspection.

Best Practices:

- Use the "`fw tab -t connections -f`" command to see the detailed (and more technical) information about the current connections in the **Connections** kernel table (ID 8158).
- Use the *"fw ctl conntab" on page 1088* command to see the simplified information about the current connections in the **Connections** kernel table (ID 8158).

Syntax

```
fw tab {-h | -help}
```

```
fw [-d] tab
      -v
      -t <Table>
      {-c | -s}
      -f [-r]
      -o <Output File>
      {-u | -m <Limit>}
      -a -e "<Entry>"
      -A -e "<Entry>"
      -x [-e "<Entry>"]
      -y
      {-z [-l] | -M}
      <Name of Object>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-h` `-help`	Shows the built-in usage.

`-t <Table>`	Specifies the kernel table by its name of unique ID.
	To see the names and IDs of the available kernel tables, run:
	`fw tab -s`
	Because the output of this command is very long, we recommend to redirect it to a file. For example:
	`fw tab -s > /tmp/output.txt`
	Notes:
	■ If you do not specify kernel tables, then the command shows the summary data for all kernel tables.
	■ You can specify several different kernel tables in the same command.

`-a -e "<Entry>"`	Adds the specified entry to the specified kernel table. If a kernel table has the "`expire`" attribute, when you add an entry with the "`-a -e <Entry>`" parameter, the new entry gets the default table timeout. You can use this parameter only locally on a Security Gateway / Cluster Member. **Important** - Each kernel table has its own internal format. **Warning** - If you add a wrong entry, you can make your Security Gateway / Cluster Memberunresponsive.

Parameter	Description
`-A -e "<Entry>"`	Adds the specified entry to the specified kernel table - in all CoreXL Firewall instances. If a kernel table has the "`expire`" attribute, when you add an entry with the "`-A -e <Entry>`" parameter, the new entry gets the default table timeout. You can use this parameter only locally on a Security Gateway / Cluster Member. **Important** - Each kernel table has its own internal format. **Warning** - If you add a wrong entry, you can make your Security Gateway / Cluster Member unresponsive.
`-c`	Shows formatted kernel table data in the common format. This is the default. The parameters "`-c`" and "`-s`" are mutually exclusive.
`-e "<Entry>"`	Specifies the entry in the kernel table. **Important** - Each kernel table has its own internal format. For the "`Connections`" (ID 8158) table, see sk65133.
`-f`	Shows formatted kernel table data. For example, shows: ▪ All IP addresses and port numbers in the decimal format. ▪ All dates and times in human readable format. The parameter "`-r`" resolves IP addresses into hostnames. **Note** - Each table can use a different style. **Important** - If the specified kernel table is large, this consumes a large amount of RAM. This can make your Security Gateway unresponsive.
`-o <Output File>`	Saves the output in the specified file in the CL format as a Check Point Firewall log. You can later open this file with the *"fw log" on page 1131* command. If you do not specify the full path explicitly, this command saves the output file in the current working directory.
`-m <Limit>`	Specifies the maximum number of kernel table entries to show. This command counts the entries from the beginning of the kernel table. The parameters "`-m`" and "`-u`" are mutually exclusive.
`-s`	Shows a short summary of the kernel table data. The parameters "`-s`" and "`-c`" are mutually exclusive.

Parameter	Description
`-u`	Specifies to show an unlimited number of kernel table entries. The parameters "`-u`" and "`-m`" are mutually exclusive. **Important** - If the specified kernel table is large, this consumes a large amount of RAM. This can make your Security Gateway unresponsive.
`-v`	Shows the CoreXL Firewall instance number as a prefix for each line.
`-x [-e <Entry>]`	Deletes all entries or the specified entry from the specified kernel table. You can use this parameter only locally on a Security Gateway / Cluster Member. **Warning** - We do not recommend this command for any production use, only for debugging and experimenting. If you delete a wrong entry, you can break the current connections through your Security Gateway / Cluster Member. This includes the remote SSH connection. For more information, see sk103876.
`-y`	Specifies not to show a prompt before Security Gateway executes a command. Applies to these parameters: "`-a`", "`-A`", and "`-x`".
`-z [-l]`	In the "Connections" table (ID 8158) shows only connections in Slow Path (F2F) and the reason why acceleration is not possible for each connection. These are connections that SecureXL cannot accelerate and forwards to the Firewall. The parameter "`-l`" shows statistics for connections. The parameter "`-z`" implicitly runs the parameter "`-u`". The parameters "`-z`" and "`-M`" are mutually exclusive. See the corresponding example (with the legend) below.
`-M`	In the "Connections" table (ID 8158) shows Used Memory and Peak Memory for each connection. The parameter "`-M`"implicitly runs the parameter "`-u`". The parameters "`-M`" and "`-z`" are mutually exclusive. See the corresponding example (with the legend) below.
<Name of Object>	Appplies only when you run this command on the Management Server. Specifies the name of the Security Gateway or Cluster Member object (as defined in SmartConsole), from which to show the information. This requires the established SIC with the Security Gateway / Cluster Member. If you do not use this parameter, the default is `localhost`.

Examples

Example 1 - Show the summary of all kernel tables

```
[Expert@MyGW:0]# fw tab -s
HOST                 NAME                               ID #VALS #PEAK #SLINKS
localhost            vsx_firewalled                      0     1     1       0
localhost            firewalled_list                     1     2     2       0
localhost            external_firewalled_list            2     0     0       0
localhost            management_list                     3     2     2       0
localhost            external_management_list            4     0     0       0
localhost            log_server_list                     5     0     0       0
localhost            ips1_sensors_list                   6     0     0       0
localhost            all_tcp_services                    7   141   141       0
localhost            tcp_services                        8     1     1       0
... ...
localhost            connections                      8158     2    56       2
... ...
localhost            up_251_rule_to_clob_uuid        14083     0     0       0
... ...
localhost            urlf_cache_tbl                     29     0     0       0
localhost            proxy_outbound_conn_tbl            30     0     0       0
localhost            dns_cache_tbl                      31     0     0       0
localhost            appi_referrer_table                32     0     0       0
localhost            uc_hits_htab                       33     0     0       0
localhost            uc_cache_htab                      34     0     0       0
localhost            uc_incident_to_instance_htab       35     0     0       0
localhost            fwx_cntl_dyn_ghtab                 36     0     0       0
localhost            frag_table                         37     0     0       0
localhost            dos_blacklist_notifs               38     0     0       0
[Expert@MyGW:0]#
```

Example 2 - Show the raw data in the "Connections" table

```
[Expert@MyGW:0]# fw tab -t connections
localhost:
-------- connections --------
dynamic, id 8158, num ents 0, load factor 0.0, attributes: keep, sync, aggressive aging,
kbufs 21 22 23 24 25 26 27 28 29 30 31 32 33 34, expires 25, refresh, , hashsize 2097152,
unlimited
<00000000, c0a8cc01, 0000d28d, c0a8cc28, 00000016, 00000006; 0001c001, 00044000, 00000002,
000001e1, 00000000, 5b9687cd, 00000000, 28cca8c0, c0000001, 00000001, 00000001, ffffffff,
ffffffff, 02007800, 000f9000, 00000080, 00000000, 00000000, 38edac90, ffffc200, 00000000,
00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000,
00000000, 00000000, 00000000, 00000000; 1996/3600>
<00000001, c0a8cc28, 00000016, c0a8cc01, 0000d28d, 00000006> -> <00000000, c0a8cc01,
0000d28d, c0a8cc28, 00000016, 00000006> (00000805)
<00000000, c0a8cc01, 0000c9f6, c0a8cc28, 00000016, 00000006; 0001c001, 00044000, 00000002,
000001e1, 00000000, 5b9679de, 00000000, 28cca8c0, c0000001, 00000001, 00000001, ffffffff,
ffffffff, 02007800, 000f9000, 00000080, 00000000, 00000000, 38edaa98, ffffc200, 00000000,
00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000,
00000000, 00000000, 00000000, 00000000; 3597/3600>
<00000001, c0a8cc28, 00000016, c0a8cc01, 0000c9f6, 00000006> -> <00000000, c0a8cc01,
0000c9f6, c0a8cc28, 00000016, 00000006> (00000805)
[Expert@MyGW:0]#
```

Example 3 - Show the formatted data in the "Connections" table

```
[Expert@MyGW:0]# fw tab -t connections -f
 Using cptfmt
Formatting table's data - this might take a while...

localhost:
 Date: Sep 10, 2018
 20:30:48 5 N/A  N/A    192.168.204.40 > N/A  LogId: <max_null>; ContextNum: <max_null>;
OriginSicName: cn=cp_mgmt,o=MyGW..44jkyv;  : (+)==================================(+);
Table_Name: connections; : (+); Attributes: dynamic, id 8158, attributes: keep, sync,
aggressive aging, kbufs 21 22 23 24 25 26 27 28 29 30 31 32 33 34, expires 25, refresh, ,
hashsize 2097152, unlimited; LastUpdateTime: 10Sep2018 20:30:48; ProductName: VPN-1 &
FireWall-1; ProductFamily: Network;

 20:30:48 5 N/A  N/A    192.168.204.40 > N/A  LogId: <max_null>; ContextNum: <max_null>;
OriginSicName: cn=cp_mgmt,o=MyGW..44jkyv; : ----------------------------------(+);
Direction: 1; Source: 192.168.204.40; SPort: 55411; Dest: 192.168.204.1; DPort: 53; Protocol:
udp; CPTFMT_sep: ;; Type: 131073; Rule: 0; Timeout: 335; Handler: 0; Ifncin: -1; Ifncout: -1;
Ifnsin: 1; Ifnsout: 1; Bits: 0000780000000000; Expires: 2/40; LastUpdateTime: 10Sep2018
20:30:48; ProductName: VPN-1 & FireWall-1; ProductFamily: Network;

 20:30:48 5 N/A  N/A    192.168.204.40 > N/A  LogId: <max_null>; ContextNum: <max_null>;
OriginSicName: cn=cp_mgmt,o=MyGW..44jkyv; : ----------------------------------(+);
Direction: 0; Source: 192.168.204.1; SPort: 53901; Dest: 192.168.204.40; DPort: 22; Protocol:
tcp; CPTFMT_sep: ;; Type: 114689; Rule: 2; Timeout: 481; Handler: 0; Ifncin: 1; Ifncout: 1;
Ifnsin: -1; Ifnsout: -1; Bits: 02007800000f9000; Expires: 2002/3600; LastUpdateTime:
10Sep2018 20:30:48; ProductName: VPN-1 & FireWall-1; ProductFamily: Network;

 20:30:48 5 N/A  N/A    192.168.204.40 > N/A  LogId: <max_null>; ContextNum: <max_null>;
OriginSicName: cn=cp_mgmt,o=MyGW..44jkyv; : ----------------------------------(+);
Direction: 1; Source: 192.168.204.40; SPort: 22; Dest: 192.168.204.1; DPort: 53901; Protocol:
tcp; CPTFMT_sep_1: ->; Direction_1: 0; Source_1: 192.168.204.1; SPort_1: 53901; Dest_1:
192.168.204.40; DPort_1: 22; Protocol_1: tcp; FW_symval: 2053; LastUpdateTime: 10Sep2018
20:30:48; ProductName: VPN-1 & FireWall-1; ProductFamily: Network;

 20:30:48 5 N/A  N/A    192.168.204.40 > N/A  LogId: <max_null>; ContextNum: <max_null>;
OriginSicName: cn=cp_mgmt,o=MyGW..44jkyv; : ----------------------------------(+);
Direction: 0; Source: 192.168.204.1; SPort: 51702; Dest: 192.168.204.40; DPort: 22; Protocol:
tcp; CPTFMT_sep: ;; Type: 114689; Rule: 2; Timeout: 481; Handler: 0; Ifncin: 1; Ifncout: 1;
Ifnsin: -1; Ifnsout: -1; Bits: 02007800000f9000; Expires: 3600/3600; LastUpdateTime:
10Sep2018 20:30:48; ProductName: VPN-1 & FireWall-1; ProductFamily: Network;

 20:30:48 5 N/A  N/A    192.168.204.40 > N/A  LogId: <max_null>; ContextNum: <max_null>;
OriginSicName: cn=cp_mgmt,o=MyGW..44jkyv; : ----------------------------------(+);
Direction: 1; Source: 192.168.204.40; SPort: 22; Dest: 192.168.204.1; DPort: 51702; Protocol:
tcp; CPTFMT_sep_1: ->; Direction_1: 0; Source_1: 192.168.204.1; SPort_1: 51702; Dest_1:
192.168.204.40; DPort_1: 22; Protocol_1: tcp; FW_symval: 2053; LastUpdateTime: 10Sep2018
20:30:48; ProductName: VPN-1 & FireWall-1; ProductFamily: Network;

 20:30:48 5 N/A  N/A    192.168.204.40 > N/A  LogId: <max_null>; ContextNum: <max_null>;
OriginSicName: cn=cp_mgmt,o=MyGW..44jkyv; : ----------------------------------(+);
Direction: 0; Source: 192.168.204.1; SPort: 53; Dest: 192.168.204.40; DPort: 55411; Protocol:
udp; CPTFMT_sep_1: ->; Direction_2: 1; Source_2: 192.168.204.40; SPort_2: 55411; Dest_2:
192.168.204.1; DPort_2: 53; Protocol_2: udp; FW_symval: 2054; LastUpdateTime: 10Sep2018
20:30:48; ProductName: VPN-1 & FireWall-1; ProductFamily: Network;
[Expert@MyGW:0]#
```

Example 4 - Show only two entries in the "Connections" table

```
[Expert@MyGW:0]# fw tab -t connections -m 2
localhost:
-------- connections --------
dynamic, id 8158, num ents 0, load factor 0.0, attributes: keep, sync, aggressive aging,
kbufs 21 22 23 24 25 26 27 28 29 30 31 32 33 34, expires 25, refresh, , hashsize 2097152,
unlimited
<00000000, c0a8cc01, 0000d28d, c0a8cc28, 00000016, 00000006; 0001c001, 00044000, 00000002,
000001e1, 00000000, 5b9687cd, 00000000, 28cca8c0, c0000001, 00000001, 00000001, ffffffff,
ffffffff, 02007800, 000f9000, 00000080, 00000000, 00000000, 38edac90, ffffc200, 00000000,
00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000,
00000000, 00000000, 00000000, 00000000; 1961/3600>
<00000001, c0a8cc28, 00000016, c0a8cc01, 0000d28d, 00000006> -> <00000000, c0a8cc01,
0000d28d, c0a8cc28, 00000016, 00000006> (00000805)
...(4 More)
[Expert@MyGW:0]#
```

Example 5 - Show the raw data in the "Connections" table and show the IDs of CoreXL Firewall instances for each entry

```
[Expert@MyGW:0]# fw tab -t 8158 -v
localhost:
-------- connections --------
dynamic, id 8158, num ents 6, load factor 0.0, attributes: keep, sync, aggressive aging,
kbufs 21 22 23 24 25 26 27 28 29 30 31 32 33 34, expires 25, refresh, , hashsize 2097152,
unlimited
[fw_0] <00000001, c0a80335, 00004710, c0a803f0, 00008652, 00000006> -> <00000000, c0a803f0,
00008652, c0a80335, 00004710, 00000006> (00000805)
[fw_0] <00000001, c0a80335, 00008adf, c0a803f0, 0000470f, 00000006; 0002d001, 00046000,
10000000, 0000000e, 00000000, 5b9a4129, 00030000, 3503a8c0, c0000000, ffffffff, ffffffff,
00000001, 00000001, 00000800, 00000000, 80008080, 00000000, 00000000, 338ea330, ffffc200,
00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000,
00000000, 00000000, 00000000, 00000000, 00000000; 3162/3600>
[fw_0] <00000000, c0a803f0, 00008652, c0a80335, 00004710, 00000006; 0001c001, 00044000,
12000000, 0000000f, 00000000, 5b8fed6a, 00030001, 3503a8c0, c0000000, 00000001, 00000001,
ffffffff, ffffffff, 00000800, 08000000, 00000080, 00000000, 00000000, 337b0978, ffffc200,
00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000,
00000000, 00000000, 00000000, 00000000, 00000000; 3599/3600>
[fw_0] <00000000, c0a803f0, 0000470f, c0a80335, 00008adf, 00000006> -> <00000001, c0a80335,
00008adf, c0a803f0, 0000470f, 00000006> (00000806)
[fw_0] <00000001, c0a80334, 00004710, c0a803f0, 0000a659, 00000006> -> <00000000, c0a803f0,
0000a659, c0a80334, 00004710, 00000006> (00000805)
[fw_0] <00000000, c0a803f0, 0000a659, c0a80334, 00004710, 00000006; 0001c001, 00044100,
12000000, 0000000f, 00000000, 5b8feabb, 0000007a, 3403a8c0, c0000000, ffffffff, ffffffff,
ffffffff, ffffffff, 00000000, 10000000, 04000080, 00000000, 00000000, 3364aed0, ffffc200,
00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000,
00000000, 00000000, 00000000, 00000000, 00000000; 3484/3600>
[fw_1] <00000001, c0a80334, 00004710, c0a803f0, 0000bc74, 00000006> -> <00000000, c0a803f0,
0000bc74, c0a80334, 00004710, 00000006> (00000805)
[fw_1] <00000001, c0a80335, 00000016, ac14a810, 0000e056, 00000006> -> <00000000, ac14a810,
0000e056, c0a80335, 00000016, 00000006> (00000805)
[fw_1] <00000000, ac14a810, 0000e056, c0a80335, 00000016, 00000006; 0001c001, 00044000,
00000003, 000001df, 00000000, 5b9a3832, 00030000, 3503a8c0, c0000001, 00000001, 00000001,
ffffffff, ffffffff, 00000800, 08000000, 00000080, 00000000, 00000000, 33410370, ffffc200,
00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000,
00000000, 00000000, 00000000, 00000000, 00000000; 3600/3600>
[fw_1] <00000000, c0a803f0, 0000bc74, c0a80334, 00004710, 00000006; 0001c001, 00044100,
12000000, 0000000f, 00000000, 5b8fe89b, 00000001, 3403a8c0, c0000001, ffffffff, ffffffff,
ffffffff, ffffffff, 00000000, 10000000, 04000080, 00000000, 00000000, 335841e0, ffffc200,
00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000,
00000000, 00000000, 00000000, 00000000, 00000000; 3600/3600>
[fw_2] <00000000, c0a803f0, 0000ab74, c0a80335, 00004710, 00000006; 0001c001, 00044000,
12000000, 0000000f, 00000000, 5b8fed7e, 00030000, 3503a8c0, c0000002, 00000001, 00000001,
ffffffff, ffffffff, 00000800, 08000000, 00000080, 00000000, 00000000, 33337660, ffffc200,
00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000,
00000000, 00000000, 00000000, 00000000, 00000000; 3556/3600>
[fw_2] <00000001, c0a80335, 00004710, c0a803f0, 0000ab74, 00000006> -> <00000000, c0a803f0,
0000ab74, c0a80335, 00004710, 00000006> (00000805)
[fw_2] <00000001, c0a80335, 00001fb4, 00000000, 00001fb4, 00000011> -> <00000000, 00000000,
00001fb4, c0a80335, 00001fb4, 00000011> (00000805)
[fw_2] <00000000, 00000000, 00001fb4, c0a80335, 00001fb4, 00000011; 00010001, 00004000,
00000003, 00000028, 00000000, 5b8fed76, 00030000, 3503a8c0, c0000002, 00000001, ffffffff,
ffffffff, ffffffff, 00000800, 08000000, 00000084, 00000000, 00000000, 336d4e30, ffffc200,
00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000,
00000000, 00000000, 00000000, 00000000, 00000000; 38/40>
[fw_2] <00000000, 00000000, 00001fb4, c0a80334, 00001fb4, 00000011; 00010001, 00004100,
00000003, 00000028, 00000000, 5b8fed72, 0000025f, 3403a8c0, c0000002, ffffffff, ffffffff,
ffffffff, ffffffff, 00000000, 10000000, 04000084, 00000000, 00000000, 00000000, 00000000,
00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000, 00000000,
00000000, 00000000, 00000000, 00000000, 00000000; 39/40>
[fw_2] <00000001, c0a80334, 00001fb4, 00000000, 00001fb4, 00000011> -> <00000000, 00000000,
00001fb4, c0a80334, 00001fb4, 00000011> (00000805)
Table fetched in 3 chunks
[Expert@MyGW:0]#
```

Example 6 - Show only Slow Path (F2F) entries in the "Connections" table

```
[Expert@MyGW:0]# fw tab -t connections -z
Dir  Source IP        SPort  Destination IP   DPort  PR  FW State          Expires        SXL
ID  Reason                          Total Pkts  Total Bytes  Duration    Last Seen
---  ---------------  -----  ---------------  -----  --  ---------------  -------------  ----
--  --------------------------------  ----------  -----------  ----------  -----------
1    172.23.7.34      60660  172.23.39.5      53     17  UDP              3/40           N/A
   Local connection                2           601B         37s         37s
1    172.23.7.34      22     172.20.38.105    65509  6   Link
0    172.20.38.105    64285  172.23.7.34      22     6   TCP Estab.       3600/3600      N/A
   Local incoming connection         192         20.16KB      38s         0s
0    172.23.7.86      67     255.255.255.255  68     17  UDP              30/40          N/A
   Local incoming connection         556         178.09KB     107h58m33s  9s
0    172.20.38.105    65509  172.23.7.34      22     6   TCP Estab.       1990/3600      N/A
   Local incoming connection         122         27.15KB      107h58m27s  107h53m54s
0    0.0.0.0          0      224.0.0.1        0      2   IGMP             21/60          N/A
   Local incoming connection         1           36B          107h27m43s  107h27m43s
1    172.23.7.34      22     172.20.38.105    64285  6   Link
0    172.23.39.5      53     172.23.7.34      60660  17  Link
0    172.23.39.5      53     172.23.7.34      60048  17  Link
1    172.23.7.34      18192  172.23.7.32      47062  6   Link
0    172.20.38.105    64286  172.23.7.34      22     6   TCP Estab.       3567/3600      N/A
   Local incoming connection         44          10.58KB      33s         33s
0    172.23.7.32      47062  172.23.7.34      18192  6   TCP Estab.       3591/3600      N/A
   Local incoming connection         40          12.57KB      9s          9s
1    172.23.7.34      60048  172.23.39.5      53     17  UDP              2/40           N/A
   Local connection                2           602B         38s         38s
1    172.23.7.34      22     172.20.38.105    64286  6   Link
1    172.23.7.34      52786  172.23.39.5      53     17  UDP              2/40           N/A
   Local connection                2           553B         38s         38s
15 slow-path connections out of 100 connections
[Expert@MyGW:0]#
```

Legend:

Column	Description
`Dir`	The direction of the connection: ■ 0 - Client to Server (request). ■ 1 - Server to Client (response).
`Source IP`	Source IP address of the connection.
`SPort`	Source Port of the connection. See *IANA Service Name and Port Number Registry*.
`Destination IP`	Destination IP address of the connection.
`DPort`	Destination Port of the connection. See *IANA Service Name and Port Number Registry*.
`PR`	Protocol number of the connection: ■ 6 - TCP ■ 17 - UDP See *IANA Protocol Numbers*
`FW State`	Connection state in the Firewall.
`Expires`	How many seconds remain before the connection expires (based on the maximum expiration time). Also, refer to the "`Duration`" column. For example, 1990/3600 means: ■ The maximum expiration time is 3600 seconds. ■ If the connection remains idle for the next 1990 seconds, it expires in the "Connections" table.
`SXL ID`	SecureXL Instance ID. Currently not used.
`Reason`	Reason for why SecureXL cannot accelerate this connection.
`Total Pkts`	The number of packets transferred in this connection.
`Total Bytes`	The number of bytes transferred in this connection.
`Duration`	How many seconds this connection is open. Also, refer to the "`Expires`" column.

Column	Description
`Last Seen`	How many seconds passed since the last packet transferred in this connection.

Example 7 - Show memory utilization for entries in the "Connections" table

```
[Expert@MyGW:0]# fw tab -t connections -M

Dir  Source IP        SPort  Destination IP   DPort  PR  FW State         Expires        Used
Memory  Peak Memory  Duration
---  ---------------  -----  ---------------  -----  --  ---------------  -------------  ----
-------  -----------  ----------
0    3.3.3.3          80     192.168.3.57     47437  17  Link
1    192.168.3.57     47437  3.3.3.3          80     17  UDP              15/40          0B
        0B           25s
0    17.23.5.3        18192  192.168.3.57     24764  6   Link
1    192.168.3.57     54533  17.23.5.3        18192  6   TCP None         2/25           0B
        0B           23s
0    172.20.219.13    64684  192.168.3.57     22     6   TCP Estab.       3598/3600      0B
        0B           2m39s
1    192.168.3.57     41565  17.23.5.2        18192  6   TCP None         12/25          0B
        0B           13s
0    17.23.5.2        18192  192.168.3.57     37193  6   Link
1    192.168.3.57     22     172.20.219.13    64684  6   Link
1    192.168.3.57     61561  17.23.5.3        18192  6   TCP None         22/25          0B
        0B           3s
0    17.23.5.3        18192  192.168.3.57     49757  6   Link
[Expert@MyGW:0]#
```

Legend:

Column	Description
`Dir`	The direction of the connection: ■ 0 - Client to Server (request) ■ 1 - Server to Client (response)
`Source IP`	Source IP address of the connection.
`SPort`	Source Port of the connection. See *IANA Service Name and Port Number Registry*.
`Destination IP`	Destination IP address of the connection.
`DPort`	Destination Port of the connection. See *IANA Service Name and Port Number Registry*.
`PR`	Protocol number of the connection: ■ 6 - TCP ■ 17 - UDP See *IANA Protocol Numbers*
`FW State`	Connection state in the Firewall.

Column	Description
`Expires`	How many seconds remain before the connection expires (based on the maximum expiration time). Also, refer to the "`Duration`" column. For example, 1990/3600 means: ■ The maximum expiration time is 3600 seconds. ■ If the connection remains idle for the next 1990 seconds, it expires from the Firewall "Connections" table.
`Used Memory`	Currently used memory for this connection.
`Peak Memory`	Maximum used memory for this connection (since it was recorded).
`Duration`	How many seconds this connection is open. Also, refer to the "`Expires`" column.

fw unloadlocal

Description

Uninstalls all policies from the Security Gateway or Cluster Member.

Warning:

1. The "`fw unloadlocal`" command prevents all traffic from passing through the Security Gateway (Cluster Member), because it disables the IP Forwarding in the Linux kernel on the Security Gateway (Cluster Member).
2. The "`fw unloadlocal`" command removes all policies from the Security Gateway (Cluster Member). This means that the Security Gateway (Cluster Member) accepts all incoming connections destined to all active interfaces without any filtering or protection enabled.

Notes

- If it is necessary to remove the current policy, but keep the Security Gateway (Cluster Member) protected, then run the *"comp_init_policy" on page 965* command on the Security Gateway (Cluster Member).
- To load the policies on the Security Gateway (Cluster Member), run one of these commands on the Security Gateway (Cluster Member), or reboot:
  - *"fw fetch" on page 1119*
  - *"cpstart" on page 1018*
- See the related command *"fwm unload" on page 360*.

Syntax

```
fw [-d] unloadlocal
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.

Example

```
[Expert@MyGW:0]# cpstat -f policy fw

Product name: Firewall
Policy name: My_Policy
Policy install time: Tue Oct 23 18:23:14 2018
... ... ...
[Expert@MyGW:0]#

[Expert@MyGW:0]# sysctl -a | grep forwarding | grep -v bridge
net.ipv6.conf.bond0.forwarding = 1
net.ipv6.conf.eth1.forwarding = 1
net.ipv6.conf.eth3.forwarding = 1
net.ipv6.conf.eth2.forwarding = 1
net.ipv6.conf.eth4.forwarding = 1
net.ipv6.conf.eth5.forwarding = 1
net.ipv6.conf.eth0.forwarding = 1
net.ipv6.conf.eth6.forwarding = 1
net.ipv6.conf.default.forwarding = 1
net.ipv6.conf.all.forwarding = 1
net.ipv6.conf.lo.forwarding = 1
net.ipv4.conf.bond0.mc_forwarding = 0
net.ipv4.conf.bond0.forwarding = 1
net.ipv4.conf.eth1.mc_forwarding = 0
net.ipv4.conf.eth1.forwarding = 1
net.ipv4.conf.eth2.mc_forwarding = 0
net.ipv4.conf.eth2.forwarding = 1
net.ipv4.conf.eth0.mc_forwarding = 0
net.ipv4.conf.eth0.forwarding = 1
net.ipv4.conf.lo.mc_forwarding = 0
net.ipv4.conf.lo.forwarding = 1
net.ipv4.conf.default.mc_forwarding = 0
net.ipv4.conf.default.forwarding = 1
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.all.forwarding = 1
[Expert@MyGW:0]#

[Expert@MyGW:0]# fw unloadlocal

Uninstalling Security Policy from all.all@MyGW
Done.
[Expert@MyGW:0]#

[Expert@MyGW:0]# cpstat -f policy fw

Product name: Firewall
Policy name:
Policy install time:
... ... ...
[Expert@MyGW:0]#

[Expert@MyGW:0]# sysctl -a | grep forwarding | grep -v bridge
net.ipv6.conf.bond0.forwarding = 0
net.ipv6.conf.eth1.forwarding = 0
net.ipv6.conf.eth3.forwarding = 0
net.ipv6.conf.eth2.forwarding = 0
net.ipv6.conf.eth4.forwarding = 0
net.ipv6.conf.eth5.forwarding = 0
net.ipv6.conf.eth0.forwarding = 0
net.ipv6.conf.eth6.forwarding = 0
net.ipv6.conf.default.forwarding = 0
net.ipv6.conf.all.forwarding = 0
net.ipv6.conf.lo.forwarding = 0
net.ipv4.conf.bond0.mc_forwarding = 0
net.ipv4.conf.bond0.forwarding = 0
net.ipv4.conf.eth1.mc_forwarding = 0
net.ipv4.conf.eth1.forwarding = 0
net.ipv4.conf.eth2.mc_forwarding = 0
net.ipv4.conf.eth2.forwarding = 0
net.ipv4.conf.eth0.mc_forwarding = 0
net.ipv4.conf.eth0.forwarding = 0
net.ipv4.conf.lo.mc_forwarding = 0
net.ipv4.conf.lo.forwarding = 0
```

```
net.ipv4.conf.default.mc_forwarding = 0
net.ipv4.conf.default.forwarding = 0
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.all.forwarding = 0
[Expert@MyGW:0]#

[Expert@MyGW:0]# fw fetch localhost
Installing Security Policy My_Policy on all.all@MyGW
Fetching Security Policy from localhost succeeded
[Expert@MyGW:0]#
```

fw up_execute

Description

Executes the offline Unified Policy.

This command only supports:

- Source IP address, Destination IP address, and objects that contain an IP address
- Simple services objects (based on destination port, source port, and protocol)
- Protocol detection
- Application detection

These are not supported:

- Implied rules
- All other objects are not supported (Security Zone, Access Roles, Domain Objects, Updatable Objects, Dynamic Objects, Other/DCERPC service, Content awareness, VPN, Resource, Mobile Access application, Time Objects, and so on)

Syntax

```
fw [-d] up_execute ipp=<IANA Protocol Number> [src=<Source IP>]
[dst=<Destination IP>] [sport=<Source Port>] [dport=<Destination
Port>] [protocol=<Protocol Detection Name>]
[application=<Application/Category Name 1>
[application=<Application/Category Name 2> ...]]
```

Parameters

Parameter	Description
No Parameters	Shows the built-in usage.
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.

Parameter	Description
`ipp=<IANA Protocol Number>`	IANA Protocol Number in the Hexadecimal format. **Important** - This parameter is always mandatory. For example: ■ TCP = 6 ■ UDP = 17 ■ ICMP = 1 See *IANA Protocol Numbers*.
`src=<Source IP>`	Source IP address.
`dst=<Destination IP>`	Destination IP address.
`sport=<Source Port>`	Source Port number in the Decimal format. See *IANA Service Name and Port Number Registry*.
`dport=<Destination Port>`	Destination Port number in the Decimal format. **Important** - This parameter is mandatory for the TCP (6) and UDP (17) protocols. See *IANA Service Name and Port Number Registry*.
`protocol=<Protocol Detection Name>`	Protocol detection name (HTTP, HTTPS, and so on).
`application=<Application/Category Name>`	Name of the Application/Category as defined in SmartConsole. You can specify multiple applications.

Example 1

```
[Expert@MyGW:0]# fw up_execute src=126.200.49.240 dst=10.1.1.1 ipp=1

Rulebase execution ended successfully.
Overall status:
----------------
Active clob mask: 0
Required clob mask: 0
Match status: MATCH
Match action: Accept

Per Layer:
------------
Layer name: Network
Layer id: 0
Match status: MATCH
Match action: Accept
Matched rule: 2
Possible rules: 2 16777215

[Expert@MyGW:0]#
```

Example 2

```
[Expert@MyGW:0]# fw up_execute src=10.1.1.1 ipp=6 dport=8080 protocol=HTTP application=Facebook
application=Opera

Rulebase execution ended successfully.
Overall status:
----------------
Active clob mask: 0
Required clob mask: 0
Match status: MATCH
Match action: Accept

Per Layer:
------------
Layer name: Network
Layer id: 0
Match status: MATCH
Match action: Accept
Matched rule: 2
Possible rules: 2 16777215

[Expert@MyGW:0]#
```

fw ver

Description

Shows this information about the Security Gateway software:

- Major version
- Minor version
- Build number
- Kernel build number

Syntax

```
fw [-d] ver [-k] [-f <Output File>]
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`ver`	Shows: ■ Major version ■ Minor version ■ Build number
`-k`	■ Shows: ■ Major version ■ Minor version ■ Build number ■ Kernel build number
`-f <Output File>`	Saves the output to the specified file. If you do not specify the full path explicitly, this command saves the output file in the current working directory.

Example 1

```
[Expert@MyGW:0]# fw ver
This is Check Point's software version R81.20 - Build 123
[Expert@MyGW:0]#
```

Example 2

```
[Expert@MyGW:0]# fw ver -k
This is Check Point's software version R81.20 - Build 123
kernel: R81.20 - Build 456
[Expert@MyGW:0]#
```

fwboot

Description

Configures Check Point boot options.

Important - Most of these commands are for Check Point use only.

Syntax

```
[Expert@HostName:0]# $FWDIR/boot/fwboot
      bootconf <options>
      corexl <options>
      cpuid <options>
      default <options>
      fwboot_ipv6 <options>
      fwdefault <options>
      ha_conf <options>
      ht <options>
      multik_reg <options>
      post_drv <options>
```

Parameters

Parameter	Description
`bootconf <options>`	Shows and configures the security boot options. See *"fwboot bootconf" on page 1253*.
`corexl <options>`	Configures and monitors the CoreXL. See *"fwboot corexl" on page 1257*.
`cpuid <options>`	Shows the number of available CPUs and CPU cores on this Security Gateway. See *"fwboot cpuid" on page 1264*.
`default <options>`	Loads the specified Default Filter policy on this Security Gateway. See *"fwboot default" on page 1266*.
`fwboot_ipv6 <options>`	Shows the internal memory address of the hook function for the specified CoreXL Firewall instance. See *"fwboot fwboot_ipv6" on page 1267*.

Parameter	Description
`fwdefault <options>`	Loads the specified Default Filter policy on this Security Gateway. See *"fwboot fwdefault" on page 1268*.
`ha_conf <options>`	Configures the cluster mechanism during boot. See *"fwboot ha_conf" on page 1269*.
`ht <options>`	This command is obsolete and not supported. See *"fwboot ht" on page 1270*.
`multik_reg <options>`	Shows the internal memory address of the registration function for the specified CoreXL Firewall instance. See *"fwboot multik_reg" on page 1271*.
`post_drv <options>`	Loads the Firewall driver for CoreXL during boot. See *"fwboot post_drv" on page 1273*.

fwboot bootconf

Description

Configures boot security options.

Notes:

- You must run this command from the Expert mode.
- The settings are saved in the `$FWDIR/boot/boot.conf` file.

  Warning - To avoid issues, do not edit the `$FWDIR/boot/boot.conf` file manually. Edit the file only with this command.
- Refer to these related commands:
  - *"fwboot corexl" on page 1257*
  - *"control_bootsec" on page 973*

Syntax to show the current boot security options

```
[Expert@HostName:0]# $FWDIR/boot/fwboot bootconf
      get_corexl
      get_core_override
      get_def
      get_ipf
      get_ipv6
      get_kernnum
      get_kern6num
```

Syntax to configure the boot security options

```
[Expert@HostName:0]# $FWDIR/boot/fwboot bootconf
      set_corexl {0 | 1}
      set_core_override <number>
      set_def [</path/filename>]
      set_ipf {0 | 1}
      set_ipv6 {0 | 1}
      set_kernnum <number>
      set_kern6num <number>
```

Parameters

Parameter	Description
No Parameters	Shows the built-in help with available parameters.
`get_corexl`	Shows if the CoreXL is enabled or disabled: ■ 0 - disabled ■ 1 - enabled **Note** - In the `$FWDIR/boot/boot.conf` file, refer to the value of the `COREXL_INSTALLED`.
`get_core_override`	Shows the number of overriding CPU cores. The SMT (HyperThreading) feature (sk93000) uses this configuration to set the number of CPU cores after reboot. **Note** - In the `$FWDIR/boot/boot.conf` file, refer to the value of the `CORE_OVERRIDE`.
`get_def`	Shows the configured path and the name of the Default Filter policy file (default is `$FWDIR/boot/default.bin`). **Note** - In the `$FWDIR/boot/boot.conf` file, refer to the value of the `DEFAULT_FILTER_PATH`.
`get_ipf`	Shows if the IP Forwarding during boot is enabled or disabled: ■ 0 - disabled (Security Gateway does not forward traffic between its interfaces during boot) ■ 1 - enabled **Note** - In the `$FWDIR/boot/boot.conf` file, refer to the value of the `CTL_IPFORWARDING`.
`get_ipv6`	Shows if the IPv6 support is enabled or disabled: ■ 0 - disabled ■ 1 - enabled **Note** - In the `$FWDIR/boot/boot.conf` file, refer to the value of the `IPV6_INSTALLED`.
`get_kernnum`	Shows the configured number of IPv4 CoreXL Firewall instances. **Note** - In the `$FWDIR/boot/boot.conf` file, refer to the value of the `KERN_INSTANCE_NUM`.

Parameter	Description
`get_kern6num`	Shows the configured number of IPv6 CoreXL Firewall instances. **Note** - In the `$FWDIR/boot/boot.conf` file, refer to the value of the `KERN6_INSTANCE_NUM`.
`set_corexl {0 | 1}`	Enables or disables CoreXL: ■ 0 - disables ■ 1 - enables **Notes:** ■ In the `$FWDIR/boot/boot.conf` file, refer to the value of the `COREXL_INSTALLED`. ■ To configure CoreXL, use the *"cpconfig" on page 996* menu.
`set_core_override <number>`	Configures the number of overriding CPU cores. The SMT (HyperThreading) feature (sk93000) uses this configuration to set the number of CPU cores after reboot. **Note** - In the `$FWDIR/boot/boot.conf` file, refer to the value of the `CORE_OVERRIDE`.
`set_def [< /path/filename >]`	Configures the path and the name of the Default Filter policy file (default is `$FWDIR/boot/default.bin`). **Notes:** ■ In the `$FWDIR/boot/boot.conf` file, refer to the value of the `DEFAULT_FILTER_PATH`. ■ If you do not specify the path and the name explicitly, then the value of the `DEFAULT_FILTER_PATH` is set to 0. As a result, Security Gateway does not load a Default Filter during boot. **Best Practice** - The best location for this file is the `$FWDIR/boot/` directory.
`set_ipf {0 | 1}`	Configures the IP forwarding during boot: ■ 0 - disables (forbids the Security Gateway to forward traffic between its interfaces during boot) ■ 1 - enables **Note** - In the `$FWDIR/boot/boot.conf` file, refer to the value of the `CTL_IPFORWARDING`.

Parameter	Description
`set_ipv6 {0 | 1}`	Enables or disables the IPv6 Support: ■ 0 - disables ■ 1 - enables **Notes:** ■ In the `$FWDIR/boot/boot.conf` file, refer to the value of the `IPV6_INSTALLED`. ■ Configure the IPv6 Support in Gaia Portal, or Gaia Clish. See the *R81.20 Gaia Administration Guide*.
`set_kernnum <number>`	Configures the number of IPv4 CoreXL Firewall instances. **Notes:** ■ In the `$FWDIR/boot/boot.conf` file, refer to the value of the `KERN_INSTANCE_NUM`. ■ To configure CoreXL, use the *"cpconfig" on page 996* menu.
`set_kern6num <number>`	Configures the number of IPv6 CoreXL Firewall instances. **Notes:** ■ In the `$FWDIR/boot/boot.conf` file, refer to the value of the `KERN6_INSTANCE_NUM`. ■ To configure CoreXL, use the *"cpconfig" on page 996* menu.

fwboot corexl

Description

Configures and monitors the CoreXL.

Note - The settings are saved in the `$FWDIR/boot/boot.conf` file.

Warning - To avoid issues, do not edit the `$FWDIR/boot/boot.conf` file manually. Edit the file only with this command.

Syntax to show CoreXL configuration

```
[Expert@HostName:0]# $FWDIR/boot/fwboot corexl
      core_count
      curr_instance4_count
      curr_instance6_count
      def_instance4_count
      def_instance6_count
      eligible
      installed
      max_instance4_count
      max_instances4_32bit
      max_instances4_64bit
      max_instance6_count
      max_instances_count
      max_instances_32bit
      max_instances_64bit
      min_instance_count
      unsupported_features
```

Syntax to configure CoreXL

Important:

- The configuration commands are for Check Point use only. To configure CoreXL, use the **Check Point CoreXL** option in the *"cpconfig" on page 996* menu.
- After all changes in CoreXL configuration on the Security Gateway, you must reboot it.
- In a Cluster, you must configure all the Cluster Members in the same way.

```
[Expert@HostName:0]# $FWDIR/boot/fwboot corexl
      def_by_allowed [n]
      default
      [-v] disable
      [-v] enable [n] [-6 k]
      vmalloc_recalculate
```

Parameters

Parameter	Description
No Parameters	Shows the built-in help with available parameters.

`core_count`	Returns the number of CPU cores on this server.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl core_count`
	`[Expert@MyGW:0]# echo $?`
	`4`
	`[Expert@MyGW:0]#`
	`[Expert@MyGW:0]# cat /proc/cpuinfo | grep processor`
	`processor : 0`
	`processor : 1`
	`processor : 2`
	`processor : 3`
	`[Expert@MyGW:0]#`

Parameter	Description

`curr_ instance4_ count`	Returns the current configured number of IPv4 CoreXL Firewall instances.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl curr_ instance4_count`
	`[Expert@MyGW:0]# echo $?`
	`3`
	`[Expert@MyGW:0]#`
	`[Expert@MyGW:0]# fw ctl multik stat`
	`ID | Active | CPU | Connections | Peak`
	`----------`
	` 0 | Yes | 3 | 11 | 18`
	` 1 | Yes | 2 | 12 | 18`
	` 2 | Yes | 1 | 13 | 18`
	`[Expert@MyGW:0]#`

`curr_ instance6_ count`	Returns the current configured number of IPv6 CoreXL Firewall instances.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl curr_ instance6_count`
	`[Expert@MyGW:0]# echo $?`
	`2`
	`[Expert@MyGW:0]#`
	`[Expert@MyGW:0]# fw6 ctl multik stat`
	`ID | Active | CPU | Connections | Peak`
	`----------`
	` 0 | Yes | 3 | 11 | 18`
	` 1 | Yes | 2 | 12 | 18`
	`[Expert@MyGW:0]#`

`def_by_ allowed [n]`	Sets the default configuration for CoreXL according to the specified allowed number of CPU cores.
`default`	Sets the default configuration for CoreXL.

Parameter	Description

`def_ instance4_ count`	Returns the default number of IPv4 CoreXL Firewall instances for this Security Gateway.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl def_ instance4_count`
	`[Expert@MyGW:0]# echo $?`
	`3`
	`[Expert@MyGW:0]#`

`def_ instance6_ count`	Returns the default number of IPv6 CoreXL Firewall instances for this Security Gateway.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl def_ instance6_count`
	`[Expert@MyGW:0]# echo $?`
	`2`
	`[Expert@MyGW:0]#`

`[-v] disable`	Disables CoreXL. ■ `-v` - Leaves the high memory (`vmalloc`) unchanged. See the *"cp_conf corexl" on page 983* command.

`eligible`	Returns whether CoreXL can be enabled on this Security Gateway.
	■ 0 - CoreXL cannot be enabled
	■ 1 - CoreXL can be enabled
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl eligible`
	`[Expert@MyGW:0]# echo $?`
	`1`
	`[Expert@MyGW:0]#`

Parameter	Description
`[-v] enable [n] [-6 k]`	Enables CoreXL with '`n`' IPv4 Firewall instances and optionally '`k`' IPv6 Firewall instances. ■ `-v` - Leaves the high memory (`vmalloc`) unchanged. ■ `n` - Denotes the number of IPv4 CoreXL Firewall instances. ■ `k` - Denotes the number of IPv6 CoreXL Firewall instances. See the *"cp_conf corexl" on page 983* command.

`installed`	Returns whether CoreXL is installed (enabled) on this Security Gateway.
	■ 0 - CoreXL is not enabled
	■ 1 - CoreXL is enabled
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl installed`
	`[Expert@MyGW:0]# echo $?`
	`1`
	`[Expert@MyGW:0]#`

`max_ instance4_ count`	Returns the maximal allowed number of IPv4 CoreXL Firewall instances for this Security Gateway.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl max_ instance4_count`
	`[Expert@MyGW:0]# echo $?`
	`4`
	`[Expert@MyGW:0]#`

`max_ instances 4_32bit`	Returns the maximal allowed number of IPv4 CoreXL Firewall instances for a Security Gateway that runs Gaia with 32-bit kernel.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl max_ instances4_32bit`
	`[Expert@MyGW:0]# echo $?`
	`14`
	`[Expert@MyGW:0]#`

Parameter	Description

`max_ instances 4_64bit`	Returns the maximal allowed number of IPv4 CoreXL Firewall instances for a Security Gateway that runs Gaia with 64-bit kernel.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl max_ instances4_64bit`
	`[Expert@MyGW:0]# echo $?`
	`38`
	`[Expert@MyGW:0]#`

`max_ instance6_ count`	Returns the maximal allowed number of IPv6 CoreXL Firewall instances for this Security Gateway.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl max_ instance6_count`
	`[Expert@MyGW:0]# echo $?`
	`3`
	`[Expert@MyGW:0]#`

`max_ instances_ count`	Returns the total maximal allowed number of CoreXL Firewall instances (IPv4 and IPv6) for this Security Gateway.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl max_ instances_count`
	`[Expert@MyGW:0]# echo $?`
	`40`
	`[Expert@MyGW:0]#`

`max_ instances_ 32bit`	Returns the total maximal allowed number of CoreXL Firewall instances for a Security Gateway that runs Gaia with 32-bit kernel.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl max_ instances_32bit`
	`[Expert@MyGW:0]# echo $?`
	`16`
	`[Expert@MyGW:0]#`

Parameter	Description

`max_instances_64bit`	Returns the total maximal allowed number of CoreXL Firewall instances for a Security Gateway that runs Gaia with 64-bit kernel.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl max_instances_64bit`
	`[Expert@MyGW:0]# echo $?`
	`40`
	`[Expert@MyGW:0]#`

`min_instance_count`	Returns the minimal allowed number of IPv4 CoreXL Firewall instances.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl min_instance_count`
	`[Expert@MyGW:0]# echo $?`
	`2`
	`[Expert@MyGW:0]#`

`vmalloc_recalculate`	Updates the value of the `vmalloc` parameter in the `/boot/grub/grub.conf` file.

`unsupported_features`	Returns 1 if at least one feature is configured, which CoreXL does not support.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl unsupported_features`
	`corexl unsupported feature: QoS is configured.`
	`[Expert@MyGW:0]# echo $?`
	`1`
	`[Expert@MyGW:0]#`

fwboot cpuid

Description

Shows the number of available CPUs and CPU cores on this Security Gateway.

Syntax

```
[Expert@HostName:0]# $FWDIR/boot/fwboot cpuid
      {-h | -help | --help}
      -c
      --full
      ht_aware
      -n
      --possible
```

Parameters

Parameter	Description

No Parameters	Shows the IDs of the available CPU cores on this Security Gateway.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot cpuid`
	`3 2 1 0`
	`[Expert@MyGW:0]#`

`-c`	Counts the number of available CPU cores on this Security Gateway.
	The command stores the returned number as its exit code.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot cpuid -c`
	`[Expert@MyGW:0]# echo $?`
	`4`
	`[Expert@MyGW:0]#`

Parameter	Description

`--full`	Shows a full map of the available CPUs and CPU cores on this Security Gateway.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot cpuid --full`
	`cpuid phys_id core_id thread_id`
	` 0 0 0 0`
	` 1 2 0 0`
	` 2 4 0 0`
	` 3 6 0 0`
	`[Expert@MyGW:0]#`

`ht_aware`	Shows the CPU cores in the order of their awareness of Hyper-Threading.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot cpuid ht_aware`
	`3 2 1 0`
	`[Expert@MyGW:0]#`

`-n`	Counts the number of available CPUs on this Security Gateway.
	The command stores the returned number as its exit code.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot cpuid -n`
	`[Expert@MyGW:0]# echo $?`
	`4`
	`[Expert@MyGW:0]#`

`--possible`	Counts the number of possible CPU cores.
	The command stores the returned number as its exit code.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot cpuid --possible`
	`[Expert@MyGW:0]# echo $?`
	`4`
	`[Expert@MyGW:0]#`

fwboot default

Description

Loads the specified Default Filter policy on this Security Gateway.

Notes:

- You must run this command from the Expert mode.
- This command is the same as the *"fwboot fwdefault" on page 1268* command.
- Refer to these related commands:
  - *"fw defaultgen" on page 1117*
  - *"fwboot bootconf" on page 1253*
  - *"control_bootsec" on page 973*
  - *"comp_init_policy" on page 965*

Syntax

```
[Expert@HostName:0]# $FWDIR/boot/fwboot default <Default Filter Policy File>
```

Parameters

Parameter	Description
No Parameters	Shows the built-in help with available parameters.
<Default Filter Policy File>	Specifies the full path and name of the Default Filter policy file. The default is `$FWDIR/boot/default.bin`

Example

```
[Expert@MyGW:0]# $FWDIR/boot/fwboot default $FWDIR/boot/default.bin
FW-1: Default filter installed successfully
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw stat
HOST POLICY DATE
localhost defaultfilter 13Sep2018 14:27:23 : [>eth0] [<eth0]
[Expert@MyGW:0]
```

fwboot fwboot_ipv6

Description

Shows the internal memory address of the hook function for the specified CoreXL Firewall instance.

Important - This command is for Check Point use only.

Syntax

```
[Expert@HostName:0]# $FWDIR/boot/fwboot fwboot_ipv6 <Number of CoreXL Firewall instance> hook [-d]
```

Parameters

Parameter	Description
No Parameters	Shows the built-in help with available parameters.
<Number of CoreXL Firewall instance>	Specifies the ID number of the CoreXL Firewall instance.
`-d`	Shows the decimal 64-bit address of the hook function.

Example

```
[Expert@MyGW:0]# fw ctl multik stat
ID | Active  | CPU    | Connections | Peak
----------------------------------------------
 0 | Yes     | 3      |          11 |       18
 1 | Yes     | 2      |          12 |       18
 2 | Yes     | 1      |          13 |       18
[Expert@MyGW:0]#

[Expert@MyGW:0]# $FWDIR/boot/fwboot fwboot_ipv6 0 hook
0xffffffff89f8fc00
[Expert@MyGW:0]#

[Expert@MyGW:0]# $FWDIR/boot/fwboot fwboot_ipv6 1 hook
0xffffffff8cd71c00
[Expert@MyGW:0]#

[Expert@MyGW:0]# $FWDIR/boot/fwboot fwboot_ipv6 2 hook
0xffffffff8fb53c00
[Expert@MyGW:0]#
```

fwboot fwdefault

Description

Loads the specified Default Filter policy on this Security Gateway.

Notes:

- You must run this command from the Expert mode.
- This command is the same as the *"fwboot default" on page 1266*command.
- Refer to these related commands:
  - *"fw defaultgen" on page 1117*
  - *"fwboot bootconf" on page 1253*
  - *"control_bootsec" on page 973*
  - *"comp_init_policy" on page 965*

Syntax

```
[Expert@HostName:0]# $FWDIR/boot/fwboot fwdefault <Default Filter Policy File>
```

Parameters

Parameter	Description
No Parameters	Shows the built-in help with available parameters.
<Default Filter Policy File>	Specifies the full path and name of the Default Filter policy file. The default file is `$FWDIR/boot/default.bin`

Example

```
[Expert@MyGW:0]# $FWDIR/boot/fwboot fwdefault $FWDIR/boot/default.bin
FW-1: Default filter installed successfully
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw stat
HOST POLICY DATE
localhost defaultfilter 13Sep2018 14:27:23 : [>eth0] [<eth0]
[Expert@MyGW:0]
```

fwboot ha_conf

Description

Configures the cluster mechanism during boot.

Important - This command is for Check Point use only.

Notes:

- You must run this command from the Expert mode.
- Refer to these related commands:
  - *"fw defaultgen" on page 1117*
  - *"fwboot bootconf" on page 1253*
  - *"control_bootsec" on page 973*
  - *"comp_init_policy" on page 965*
- To install a cluster, see the *R81.20 Installation and Upgrade Guide*.
- To configure a cluster , see the *R81.20 Installation and Upgrade Guide* and *R81.20 ClusterXL Administration Guide*.

Syntax

```
[Expert@HostName:0]# $FWDIR/boot/fwboot ha_conf
```

fwboot ht

Important - This command is obsolete and is not supported. To configure SMT (HyperThreading) feature, follow sk93000.

fwboot multik_reg

Description

Shows the internal memory address of the registration function for the specified CoreXL Firewall instance.

Important - This command is for Check Point use only.

Note - You must run this command from the Expert mode.

Syntax

```
[Expert@HostName:0]# $FWDIR/boot/fwboot multik_reg <Number of CoreXL Firewall instance> {ipv4 | ipv6} [-d]
```

Parameters

Parameter	Description
No Parameters	Shows the built-in help with available parameters.
<Number of CoreXL Firewall instance>	Specifies the ID number of the CoreXL Firewall instance.
`ipv4`	Specifies to work with IPv4 CoreXL Firewall instances.
`ipv6`	Specifies to work with IPv6 CoreXL Firewall instances.
`-d`	Shows the decimal 64-bit address of the hook function.

Example

```
[Expert@MyGW:0]# fw ctl multik stat
ID | Active  | CPU    | Connections | Peak
----------------------------------------------
 0 | Yes     | 3      |          11 |       18
 1 | Yes     | 2      |          12 |       18
 2 | Yes     | 1      |          13 |       18
[Expert@MyGW:0]#


[Expert@MyGW:0]# $FWDIR/boot/fwboot multik_reg 0 ipv4
0
[Expert@MyGW:0]#

[Expert@MyGW:0]# $FWDIR/boot/fwboot multik_reg 1 ipv4
0xffffffff8a2a5690
[Expert@MyGW:0]#

[Expert@MyGW:0]# $FWDIR/boot/fwboot multik_reg 2 ipv4
0xffffffff8a2a5690
[Expert@MyGW:0]#
```

fwboot post_drv

Description

Loads the Firewall driver for CoreXL during boot.

Important:

- This command is for Check Point use only.
- If you run this command, Security Gateway can block all traffic. In such case, you must connect to the Security Gateway over a console and restart Check Point services with the *"cpstop" on page 1029* and *"cpstart" on page 1018* commands. Alternatively, you can reboot the Security Gateway.

Note - You must run this command from the Expert mode.

Syntax

```
[Expert@HostName:0]# $FWDIR/boot/fwboot post_drv {ipv4 | ipv6}
```

Parameters

Parameter	Description
No Parameters	Shows the built-in help with available parameters.
`ipv4`	Loads the IPv4 Firewall driver for CoreXL.
`ipv6`	Loads the IPv6 Firewall driver for CoreXL.

sam_alert

Description

For SAM v1, this utility executes Suspicious Activity Monitoring (SAM) actions according to the information received from the standard input.

For SAM v2, this utility executes Suspicious Activity Monitoring (SAM) actions with User Defined Alerts mechanism.

Important:

- You must run this command on the Management Server.
- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Notes:

- VSX Gateways and VSX Cluster Members do **not** support Suspicious Activity Monitoring (SAM) Rules. See sk79700.
- See the *"fw sam" on page 295* and *"fw sam_policy" on page 303* commands.

SAM v1 syntax

```
sam_alert [-v] [-o] [-s <SAM Server>] [-t <Time>] [-f <Security
Gateway>] [-C] {-n|-i|-I} {-src|-dst|-any|-srv}
```

Parameters for SAM v1

Parameter	Description
`-v`	Enables the verbose mode for the "`fw sam`" command.
`-o`	Specifies to print the input of this tool to the standard output (to use with pipes in a CLI syntax).
`-s <SAM Server>`	Specifies the SAM Server to be contacted. Default is "localhost".
`-t <Time>`	Specifies the time (in seconds), during which to enforce the action. The default is forever.

Parameter	Description
`-f <Security Gateway>`	Specifies the Security Gateway / Cluster object, on which to run the operation. **Important** - If you do not specify the target Security Gateway / Cluster object explicitly, this command applies to all managed Security Gateways and Clusters.
`-C`	Cancels the specified operation.
`-n`	Specifies to notify every time a connection, which matches the specified criteria, passes through the Security Gateway / ClusterXL / Security Group.
`-i`	Inhibits (drops or rejects) connections that match the specified criteria.
`-I`	Inhibits (drops or rejects) connections that match the specified criteria and closes all existing connections that match the specified criteria.
`-src`	Matches the source address of connections.
`-dst`	Matches the destination address of connections.
`-any`	Matches either the source or destination address of connections.
`-srv`	Matches specific source, destination, protocol and port.

SAM v2 syntax

```
sam_alert -v2 [-v] [-O] [-S <SAM Server>] [-t <Time>] [-f
<Security Gateway>] [-n <Name>] [-c "<Comment">] [-o
<Originator>] [-l {r | a}] -a {d | r| n | b | q | i} [-C] {-ip
|-eth} {-src|-dst|-any|-srv}
```

Parameters for SAM v2

Parameter	Description
`-v2`	Specifies to use SAM v2.
`-v`	Enables the verbose mode for the "`fw sam`" command.
`-O`	Specifies to print the input of this tool to the standard output (to use with pipes in a CLI syntax).
`-S <SAM Server>`	Specifies the SAM server to be contacted. Default is "localhost".
`-t <Time>`	Specifies the time (in seconds), during which to enforce the action. The default is forever.
`-f <Security Gateway>`	Specifies the Security Gateway / Cluster object, on which to run the operation. **Important** - If you do not specify the target Security Gateway / Cluster object explicitly, this command applies to all managed Security Gateways and Clusters.
`-n <Name>`	Specifies the name for the SAM rule. Default is empty.
`-c "<Comment>"`	Specifies the comment for the SAM rule. Default is empty. You must enclose the text in the double quotes or single quotes.
`-o <Originator>`	Specifies the originator for the SAM rule. Default is "`sam_alert`".

Parameter	Description
`-l {r | a}`	Specifies the log type for connections that match the specified criteria: ■ `r` - Regular ■ `a` - Alert Default is `None`.
`-a {d | r| n | b | q | i}`	Specifies the action to apply on connections that match the specified criteria: ■ `d` - Drop ■ `r` - Reject ■ `n` - Notify ■ `b` - Bypass ■ `q` - Quarantine ■ `i` - Inspect
`-C`	Specifies to close all existing connections that match the criteria.
`-ip`	Specifies to use IP addresses as criteria parameters.
`-eth`	Specifies to use MAC addresses as criteria parameters.
`-src`	Matches the source address of connections.
`-dst`	Matches the destination address of connections.
`-any`	Matches either the source or destination address of connections.
`-srv`	Matches specific source, destination, protocol and port.

Example

See sk110873: How to configure Security Gateway to detect and prevent port scan.

stattest

Description

Check Point AMON client to query SNMP OIDs.

You can use this command as an alternative to the standard SNMP commands for debug purposes - to make sure the applicable SNMP OIDs provide the requested information.

Notes:

- You can run this command only in the Expert mode.
- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Syntax to query a Regular OID

- On a Management Server / Security Gateway / Cluster Member:

```
stattest get [-d] [-h <Host>] [-p <Port>] [-x <Proxy Server>] [-v <VSID>] [-t <Timeout>] <Regular_OID_1> <Regular_OID_2> ...
<Regular_OID_N>
```

- On a Scalable Platform Security Group:

```
g_all stattest get [-d] [-h <Host>] [-p <Port>] [-x <Proxy Server>] [-v <VSID>] [-t <Timeout>] <Regular_OID_1> <Regular_OID_2>
... <Regular_OID_N>
```

Notes:

- These Regular OIDs are specified in the SNMP MIB files.
- For Check Point MIB files, see sk90470.

Syntax to query a Statistical OID

- On a Management Server / Security Gateway / Cluster Member:

```
stattest get [-d] [-h <Host>] [-p <Port>] [-x <Proxy Server>] -l <Polling Interval> -r <Polling Duration> [-v <VSID>] [-t
<Timeout>] <Statistical_OID_1> <Statistical_OID_2> ... <Statistical_OID_N>
```

- On a Scalable Platform Security Group:

```
g_all stattest get [-d] [-h <Host>] [-p <Port>] [-x <Proxy Server>] -l <Polling Interval> -r <Polling Duration> [-v <VSID>] [-t
<Timeout>] <Statistical_OID_1> <Statistical_OID_2> ... <Statistical_OID_N>
```

Notes:

- These Statistical OIDs take some time to "initialize".
- For example, to calculate an average, it is necessary to collect enough samples.
- Check Point statistical OIDs are registered in the `$CPDIR/conf/statistical_oid.conf` file.

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-h <Host>`	Specifies the remote Check Point host to query by its IP address or resolvable hostname.
`-p <Port>`	Specifies the port number, on which the AMON server listens. Default port is 18192.
`-x <Proxy Server>`	Specifies the Proxy Server by its IP address or resolvable hostname. **Note** - Use only when you query a remote host.
`-l <Polling Interval>`	Specifies the time in seconds between queries. **Note** - Use only when you query a Statistical OID.

Parameter	Description
`-r <Polling Duration>`	Specifies the time in seconds, during which to run consecutive queries. **Note** - Use only when you query a Statistical OID.
`-v <VSID>`	On a VSX Gateway, specifies the context of a Virtual Device to query.
`-t <Timeout>`	Specifies the session timeout in milliseconds.
`<Regular_OID_1> <Regular_OID_2> ... <Regular_OID_N>`	Specifies the Regular OIDs to query. **Notes:** ■ OID must not start with period. ■ Separate the OIDs with spaces. ■ You can specify up to 100 OIDs.
`<Statistical_OID_1> <Statistical_OID_2> ... <Statistical_OID_N>`	Specifies the Statistical OIDs to query. **Notes:** ■ OID must not start with period. ■ Separate the OIDs with spaces. ■ You can specify up to 100 OIDs.

Example - Query a Regular OID

Query the CPU Idle utilization at the OID 1.3.6.1.4.1.2620.1.6.7.2.3 (`procIdleTime`).

```
[Expert@HostName]# stattest get 1.3.6.1.4.1.2620.1.6.7.4.2
```

Example - Query a Statistical OID

Query the CPU Idle utilization at the OID 1.3.6.1.4.1.2620.1.6.7.2.3 (`procIdleTime`).

Information is collected with intervals of 5 seconds during 5 seconds

```
[Expert@HostName]# stattest get -l 5 -r 5 1.3.6.1.4.1.2620.1.6.7.2.3
```

tp_collector_cli

Description

This is a light debug tool that runs in the background on the Security Gateways. The tool automatically collects information about the main points in Threat Prevention for each traffic flow.

For any issue, you can examine the "`tp_collector_cli`" output to understand what was the connection flow and understand the area of the issue.

Notes:

- You can run this command in the Expert mode.
- On Scalable Platforms (Maestro and Chassis), you must connect to the applicable Security Group.
- On a VSNext Gateway / Legacy VSX Gateway, you must run this command in the context of the applicable Virtual Gateway / Virtual System:

  ```
  vsenv <ID>
  ```

- This tool saves its history data in the `$FWDIR/log/tp_collector.dat` file.
- This tool saves its log (failures it finds in connections) in the `$FWDIR/log/tp_failures.elg` file.

Syntax for the Expert mode

```
[Expert@GW:0]# tp_collector_cli {-h | --help}
```

```
[Expert@GW:0]# tp_collector_cli
      [--filter <Filter Name 1> [{not^ | contains%}]<Filter Value
1> [<Filter Name 2> [{not^ | contains%}]<Filter Value 2>] ...
[<Filter Name N> {not^}{contains%}<Filter Value N>]]
      [--delim "<Delimiter>"]
      [--input_file <Path>]
      [--last_minutes <Number>]
      [--print_key_names]
```

Parameters

Parameter	Description
`-h` `--help`	Shows the complete built-in help.
`--filter <Filter Name>`	Optional. Specifies the filter name - see the built-in help. Example of general filters: ■ `"Source_ip"` ■ `"Destination_ip"` ■ `"Destination_port"` ■ `"Instance"` ■ `"App"` ■ `"Conn"` ■ `"rule_id"` Example of Threat Prevention filters: ■ `"Action"` ■ `"Final Action"` ■ `"Performance Impact"` ■ `"IOC Verdict"` ■ `"RAD Verdict"` ■ `"TE Verdict"` ■ `"Severity"` ■ `"ZPHI: URL"`

Parameter	Description

`<Filter Value>`	Specifies the filter value.
	Best Practice - To see the values, just rune "`tp_collector_cli`" and copy the values from the applicable fields.
	Optional operators:
	■ `not^<Filter Value>`
	Negates the specified value.
	The output shows all entries except the specified value.
	Example:
	`tp_collector_cli --filter "App" not^CIU`
	■ `contains%<Filter Value>`
	Specifies the partial value (as a wildcard).
	Example 1:
	`tp_collector_cli --filter "App" contains%CI`
	Example 2:
	`tp_collector_cli --filter "CIU info" contains%Online`

`--delim "<Delimiter>"`	Optional.
	Shows the records in the data file and uses the specified string as the delimiter between the columns.
	This makes it easy to parse the output with various tools.
	Example for 3 spaces:
	`tp_collector_cli --delim "   ">`
	Example for the pipeline:
	`tp_collector_cli --delim "|">`

`--print_key_names`	Optional. Shows internal names of various fields (useful for Check Point Support and R&D).
`--input_file <Path>`	Optional. Specifies the path and the name of the data file to read. You can get the `$FWDIR/log/tp_collector.dat` file from one Security Gateway and open it on another Security Gateway. **Note** - Versions of these Security Gateways must be the same.
`--last_minutes <Number>`	Optional. Specifies the number of last minutes, for which to show the information from the data file.

Example output of one record:

```
Time:06/21 09:45:06
Instance:0
Conn:dir 0, 192.168.22.33:45678 -> 172.16.44.55:80 IPP 6
Session:1933
App:CI_AV
File Name:test.deb
Content-Length:8144
Strict Hold:1
Last Buffer Seen:1
rule_id:4
profile_id:1
AV Performed Hold:09:45:06
Accumulated File Size:8144
RAD Verdict:ACCEPT
File Type ID:1100
File MD5:8add8c310e05a8a5243414ef669f19bc
AV Async Response Time:09:45:06
AV Verdict:ACCEPT
Final Action:ACCEPT
Final Async Action Time:09:45:06
Strict Hold Start Sending File:1
```

Example filter 1 - filtering for the application "CI_AV" for the last 5 minutes:

```
tp_collector_cli --filter "App" CI_AV --last_minutes 5
```

Example filter 2 - filtering for the specified time frame:

```
tp_collector_cli --filter "Time_start" "06/21 09:40:00" "Time_end" "06/21 09:50:00"
tp_collector_cli --filter "Time_start" contains%"06/21 09"
```

Example filter 3 - filtering for a specific connection:

You can only filter using the full connection tuple.

```
tp_collector_cli --filter "Conn" "dir 0, 192.168.22.33:45678 -> 172.16.44.55:80 IPP 6"
```

usrchk

Description

Controls the UserCheck daemon (*usrchkd*).

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
usrchk
      hits <options>
      incidents <options>
      debug <options>
```

Syntax on a Scalable Platform Security Group in Gaia gClish

```
usrchk
      hits <options>
      incidents <options>
      debug <options>
```

Syntax on a Scalable Platform Security Group in the Expert mode

```
g_all usrchk
      hits <options>
      incidents <options>
      debug <options>
```

Note - You can also enter partial names of the sub-commands and their options.

Parameters

Parameter	Description
No Parameter	Shows the built-in help. This applies to sub-commands as well. For example, run just the "`usrchk hits`" command.

`hits <options>`	Shows user hits (violations).
	The available options are:
	■ Show user hits:
	• List all existing hits:
	`usrchk hits list all`
	• Show hits for a specified user:
	`usrchk hits list user <UserName>`
	• Show hits for a specified interaction object:
	`usrchk hits list uci <Name of UserCheck Object>`

	■ Clear user hits:
	• Clear all existing hits:
	`usrchk hits clear all`
	• Clear hits for a specified user:
	`usrchk hits clear user <UserName>`
	• Clear hits for a specified interaction object:
	`usrchk hits clear uci <Name of UserCheck Object>`

	■ Database operations:
	• Reload hits from the database:
	`usrchk hits db reload`
	• Update hits changes in the database:
	`usrchk hits db reload update`

Parameter	Description
`incidents <options>`	Sends emails to users about incidents. The available option is: ■ Send emails to users about their expiring email violations: `usrchk incidents expiring`
`debug <options>`	Controls the debug of the UserCheck daemon. The available options are:
	■ Enable the debug: `usrchk debug on` **Important** - After you run this command "`usrchk debug on`", you must run the command "`usrchk debug set ...`" to configure the required filter. **Important** - When you enable the debug, it affects the performance of the *usrchkd* daemon. Make sure to disable the debug after you complete your troubleshooting.
	■ Disable the debug: `usrchk debug off`

	■ Filter which debug logs UserCheck writes to the log file based on the specified Debug Topics and Severity:
	`usrchk debug set <Topic Name> <Severity>`
	The available Debug Topics are:
	• `all`
	• *Check Point Support* provides more specific topics, based on the reported issue
	The available Severities are:
	• `all`
	• `critical`
	• `events`
	• `important`
	• `surprise`
	Best Practice - We recommend to enable all Topics and all Severities. Run:
	`usrchk debug set all all`

	■ Show the UserCheck current debug status: `usrchk debug stat`

Parameter	Description
	■ Unset the specified Debug Topic(s): `usrchk debug unset <Topic Name>`
	■ Reset all debug topics: `usrchk debug reset`
	■ Rotate the UserCheck log files: `usrchk debug`
	■ Show the memory consumption by the *usrchkd* daemon: `usrchk debug memory`
	■ Show and set the number of indentation spaces in the `$FWDIR/log/usrchk.elg` file. `usrchk debug spaces [<0 - 5>]` You can specify the number of spaces: • 0 (this is the default) • 1 • 2 • 3 • 4 • 5

Notes:

- To show all UserCheck objects, run:
  ```
  usrchk hits list all
  ```
- You can run a command that contains "`user <UserName>`" only if:
  - Identity Awareness is enabled on the Security Gateway.
  - User object is used in the same policy rules as UserCheck objects.

ClusterXL Commands

For more information about Check Point cluster, see the *R81.20 ClusterXL Administration Guide*.

ClusterXL Configuration Commands

Description

These commands let you configure internal behavior of the Clustering Mechanism.

Important:

- We do not recommend that you run these commands. These commands must be run automatically only by the Security Gateway or the Check Point Support.
- In a Cluster, you must configure all the Cluster Members in the same way.

Syntax

Notes:

- In Gaia Clish:
  Enter the **`set cluster<ESC><ESC>`** to see all the available commands.
- In Expert mode:
  Run the **`cphaconf`** command see all the available commands.
  You can run the `cphaconf` commands only from the Expert mode.
- Syntax legend:
  1. Curly brackets or braces **{ }**:
     Enclose a list of available commands or parameters, separated by the vertical bar **|**, from which user can enter only one.
  2. Angle brackets **< >**:
     Enclose a variable - a supported value user needs to specify explicitly.
  3. Square brackets or brackets **[ ]**:
     Enclose an optional command or parameter, which user can also enter.
- You can include these commands in scripts to run them automatically.
  The meaning of each command is explained in the next sections.

Table: ClusterXL Configuration Commands

Description of Command	Command in Gaia Clish	Command in Expert Mode
Configure how to show the Cluster Member in local ClusterXL logs - by its Member ID or its Member Name (see *"Configuring the Cluster Member ID Mode in Local Logs" on page 1294*)	`set cluster member idmode {id | name}`	`cphaconf mem_id_mode {id | name}`

Table: ClusterXL Configuration Commands (continued)

Description of Command	Command in Gaia Clish	Command in Expert Mode
Register a single Critical Device (Pnote) on the Cluster Member (see *"Registering a Critical Device" on page 1295*)	`N / A`	`cphaconf set_pnote -d <Name of Device> -t <Timeout in Sec> -s {ok|init|problem} [-p] [-g] register`
Unregister a single Critical Device (Pnote) on the Cluster Member (see *"Unregistering a Critical Device" on page 1299*)	`N / A`	`cphaconf set_pnote -d <Name of Device> [-p] [-g] unregister`
Report (change) a state in a single Critical Device (Pnote) on the Cluster Member (see *"Reporting the State of a Critical Device" on page 1300*)	`N / A`	`cphaconf set_pnote -d <Name of Device> -s {ok|init|problem} [-g] report`
Register several Critical Devices (Pnotes) from a file on the Cluster Member (see *"Registering Critical Devices Listed in a File" on page 1302*)	`N / A`	`cphaconf set_pnote -f <Name of File> [-g] register`
Unregister all Critical Devices (Pnotes) on the Cluster Member (see *"Unregistering All Critical Devices" on page 1304*)	`N / A`	`cphaconf set_pnote -a [-g] unregister`
Configure the Cluster Control Protocol (CCP) Encryption on the Cluster Member (see *"Configuring the Cluster Control Protocol (CCP) Settings" on page 1305*)	`set cluster member ccpenc {off | on}`	`cphaconf ccp_ encrypt {off | on}` `cphaconf ccp_ encrypt_key <Key String>`
Configure the Cluster Forwarding Layer on the Cluster Member (controls the forwarding of traffic between Cluster Members) **Note** - For Check Point use only.	`set cluster member forwarding {off | on}`	`cphaconf forward {off | on}`
Print the current cluster configuration as loaded in the kernel on the Cluster Member (for details, see sk93306)	`N / A`	`cphaconf debug_data`

Table: ClusterXL Configuration Commands (continued)

Description of Command	Command in Gaia Clish	Command in Expert Mode
Start internal failover between subordinate interfaces of specified bond interface - only in Bond High Availability mode (for details, see sk93306)	`N / A`	`cphaconf failover_bond <bond_name>`
Configure what happens during a failover after a Bond already failed over internally (for details, see sk93306)	`N / A`	`cphaconf enable_bond_failover <bond_name>`
Initiate manual cluster failover (see *"Initiating Manual Cluster Failover" on page 1306*)	`set cluster member admin {down | up}`	`clusterXL_admin {down | up}`
Configure the minimal number of required subordinate interfaces for Bond Load Sharing (see *"Configuring the Minimal Number of Required Subordinate Interfaces for Bond Load Sharing" on page 1310*)	`set interface <Bond Name> links <Value>`	`cphaconf bond_ls {set <Bond Name> <Value> | remove <Bond Name>}`
Configuring Link Monitoring on the Cluster Interfaces (see *"Configuring Link Monitoring on the Cluster Interfaces" on page 1313*)	`N / A`	`N / A`
Configuring the Multi-Version Cluster Mechanism (see *"Configuring the Multi-Version Cluster Mechanism" on page 1316*)	`N / A`	`cphaconf mvc {off | on}`
Configuring duration of forced cluster failover in the High Availability mode (see *"Configuring Duration of Forced Failover in High Availability Mode" on page 1317*)	`set cluster force_failover member_id <ID> {time <Minutes> on | off}`	`cphaconf force_failover member_id <ID> {time <Minutes> on | off}`

List of the Gaia Clish "`set cluster`" commands

```
set cluster member admin {down | up} [permanent]
set cluster member ccpenc {off | on}
set cluster member forwarding {off | on}
set cluster member idmode {id | name}
set cluster member mvc {off | on}
set cluster force_failover member_id <ID> {time <Minutes> on |
off}
```

List of the Expert mode "`cphaconf`" commands

Note - Some commands are not applicable to 3rd-party clusters.

```
cphaconf [-D] <options> start
cphaconf stop
cphaconf [-t <Sync IF 1>...] [-d <Non-Monitored IF 1>...] add
cphaconf clear-secured
cphaconf clear-non-monitored
cphaconf debug_data
cphaconf delete_link_local [-vs <VSID>] <IF name>
cphaconf set_link_local [-vs <VSID>] <IF name> <Cluster IP>
cphaconf mem_id_mode {id | name}
cphaconf failover_bond <bond_name>
cphaconf [-s] {set | unset | get} var <Kernel Parameter Name>
[<Value>]
cphaconf bond_ls {set <Bond Name> <Value> | remove <Bond Name>}
cphaconf set_pnote -d <Device> -t <Timeout in sec> -s {ok | init |
problem} [-p] [-g] register
cphaconf set_pnote -f <File> [-g] register
cphaconf set_pnote -d <Device> [-p] [-g] unregister
cphaconf set_pnote -a [-g] unregister
cphaconf set_pnote -d <Device> -s {ok | init | problem} [-g]
report
cphaconf ccp_encrypt {off | on}
cphaconf ccp_encrypt_key <Key String>
cphaconf mvc {on | off}
cphaconf force_failover member_id <ID> {time <Minutes> on | off}
```

Configuring the Cluster Member ID Mode in Local Logs

Important - In a Cluster, you must configure all the Cluster Members in the same way.

Description

This command configures how to show the Cluster Member in the local ClusterXL logs - by its Member ID (default), or its Member Name.

This configuration applies to these local logs:

- `/var/log/messages`
- `dmesg`
- `$FWDIR/log/fwd.elg`

See *"Viewing the Cluster Member ID Mode in Local Logs" on page 1364*.

Syntax

Shell	Command
Gaia Clish	`set cluster member idmode {id | name}`
Expert mode	`cphaconf mem_id_mode {id | name}`

Example

```
[Expert@Member1:0]# cphaprob names

Current member print mode in local logs is set to: ID

[Expert@Member1:0]#
[Expert@Member1:0]# cphaconf mem_id_mode name

Member print mode in local logs: NAME

[Expert@Member1:0]#
[Expert@Member1:0]# cphaprob names

Current member print mode in local logs is set to: NAME

[Expert@Member1:0]#
```

Registering a Critical Device

Important - In a Cluster, you must configure all the Cluster Members in the same way.

Description

You can add a user-defined critical device to the default list of critical devices. Use this command to register <device> as a critical process, and add it to the list of devices that must run for the Cluster Member to be considered active. If <device> fails, then the Cluster Member is seen as failed.

If a Critical Device fails to report its state to the Cluster Member in the configured timeout, the Critical Device, and by design the Cluster Member, are seen as failed.

Define the status of the Critical Device that is reported to ClusterXL upon registration.

This initial status can be one of these:

- **ok** - Critical Device is alive.
- **init** - Critical Device is initializing. The Cluster Member is Down. In this state, the Cluster Member cannot become Active.
- **problem** - Critical Device failed. If this state is reported to ClusterXL, the Cluster Member immediately goes Down. This causes a failover.

Syntax

Shell	Command
Gaia Clish	N / A
Expert mode	`cphaconf set_pnote -d <Name of Critical Device> -t <Timeout in Sec> -s {ok | init | problem} [-p] [-g] register`

Notes:

- The "`-t`" flags specifies how frequently to expect the periodic reports from this Critical Device.
  If no periodic reports should be expected, then enter the value 0 (zero).
- The "`-p`" flag makes these changes permanent (survive reboot).
- The "`-g`" flag applies the command to all configured Virtual Systems.

Restrictions

- Total number of critical devices (pnotes) on Cluster Member is limited to 16.
- Name of any critical device (pnote) on Cluster Member is limited to 15 characters, and must not include white spaces.

Related topics

- *"Viewing Critical Devices" on page 1329*
- *"Reporting the State of a Critical Device" on page 1300*
- *"Registering Critical Devices Listed in a File" on page 1302*
- *"Unregistering a Critical Device" on page 1299*
- *"Unregistering All Critical Devices" on page 1304*

Example use case

This example assumes that all other Critical Devices report their statues as "`ok`".

Do these steps on each Cluster Member:

1. Create a shell script that does these actions:
   a. Examine the used space in the critical disk partitions.
   b. If the used space in these partitions:
      - Is above the threshold, then register a user-defined Critical Device and report its status as "`problem`".

        As a result, the Cluster Member changes its cluster state to "`Down`" (if there is at least one Cluster Member in the status "`Active`").
      - Is below the threshold, then register a user-defined Critical Device and report its status as "`ok`".

        As a result, the Cluster Member changes its cluster state to "`Standby`" or "`Active`".

   Example script syntax:

```
#!/bin/bash

# Get the used % in the partition lv_current
var_lv_current=$(df -h | grep lv_current | awk '{print $5}'|
sed 's/[%]//')
# Get the used % in the partition lv_log
var_lv_log=$(df -h | grep lv_log | awk '{print $5}'| sed 's/
[%]//')

if [ "$var_lv_current" -gt 90 -o "$var_lv_log" -gt 90 ];
    then
        # If the partition is full, then bring the cluster
member down
        $FWDIR/bin/cphaconf set_pnote -d Storage -s problem
report
    else
        # If the partition is free enough, then bring the
cluster member up
        $FWDIR/bin/cphaconf set_pnote -d Storage -s ok report
        $FWDIR/bin/cphaconf set_pnote -d Storage unregister
fi
```

2. Configure a scheduled job to run this shell script at the relevant time intervals.

   See the *R81.20 Gaia Administration Guide*.

Unregistering a Critical Device

Important - In a Cluster, you must configure all the Cluster Members in the same way.

Description

This command unregisters a user-defined Critical Device (Pnote). This means that this device is no longer considered critical.

If a Critical Device was registered with a state "`problem`", before you ran this command, then after you run this command, the status of the Cluster Member depends only on the states of the remaining Critical Devices.

Syntax

Shell	Command
Gaia Clish	`N/A`
Expert mode	`cphaconf set_pnote -d <Name of Critical Device> [-p] [-g] unregister`

Notes:

- The "`-p`" flag makes these changes permanent.
  This means that after you reboot, these Critical Devices remain unregistered.
- The "`-g`" flag applies the command to all configured Virtual Systems.

Related topics

- *"Viewing Critical Devices" on page 1329*
- *"Reporting the State of a Critical Device" on page 1300*
- *"Registering a Critical Device" on page 1295*
- *"Registering Critical Devices Listed in a File" on page 1302*
- *"Unregistering All Critical Devices" on page 1304*

Reporting the State of a Critical Device

Important - In a Cluster, you must configure all the Cluster Members in the same way.

Description

This command manually reports (changes) the state of a Critical Device to ClusterXL.

The reported state can be one of these:

- **ok** - Critical Device is alive.
- **init** - Critical Device is initializing. The Cluster Member is Down. In this state, the Cluster Member cannot become Active.
- **problem** - Critical Device failed. If this state is reported to ClusterXL, the Cluster Member immediately goes Down. This causes a failover.

If a Critical Device fails to report its state to the Cluster Member within the defined timeout, the Critical Device, and by design the Cluster Member, are seen as failed. This is true only for Critical Devices with timeouts. If a Critical Device is registered with the "**-t 0**" parameter, there is no timeout. Until the Critical Device reports otherwise, the state of the Critical Device is considered to be the last reported state.

Syntax

Shell	Command
Gaia Clish	N / A
Expert mode	`cphaconf set_pnote -d <Name of Critical Device> -s {ok | init | problem} [-g] report`

Notes:

- The "`-g`" flag applies the command to all configured Virtual Systems.
- If the "`<Name of Critical Device>`" reports its state as "`problem`", then the Cluster Member reports its state as failed.

Related topics

- *"Viewing Critical Devices" on page 1329*
- *"Registering a Critical Device" on page 1295*
- *"Registering Critical Devices Listed in a File" on page 1302*
- *"Unregistering a Critical Device" on page 1299*
- *"Unregistering All Critical Devices" on page 1304*

Registering Critical Devices Listed in a File

Important - In a Cluster, you must configure all the Cluster Members in the same way.

Description

This command registers all the user-defined Critical Devices listed in the specified file.

This file must be a plain-text ASCII file, with each Critical Device defined on a separate line.

Each definition must contain three parameters, which must be separated by a space or a tab character:

```
<Name of Device> <Timeout> <Status>
```

Where:

Parameter	Description
<Name of Device>	The name of the Critical Device. ■ Maximal name length is 15 characters ■ The name must not include white spaces (space or tab characters).
<Timeout>	If the Critical Device *<Name of Device>* fails to report its state to the Cluster Member within this specified number of seconds, the Critical Device (and by design the Cluster Member), are seen as failed. For no timeout, use the value `0` (zero).
<Status>	The Critical Device *<Name of Device>* reports one of these statuses to the Cluster Member: ■ `ok` - Critical Device is alive. ■ `init`- Critical Device is initializing. The Cluster Member is Down. In this state, the Cluster Member cannot become Active. ■ `problem` - Critical Device failed. If this state is reported to ClusterXL, the Cluster Member immediately goes Down. This causes a failover.

Syntax

Shell	Command
Gaia Clish	N / A
Expert mode	`cphaconf set_pnote -f /<Path>/<Name of File> [-g] register`

Note - The "`-g`" flag applies the command to all configured Virtual Systems.

Related topics

- *"Viewing Critical Devices" on page 1329*
- *"Reporting the State of a Critical Device" on page 1300*
- *"Registering a Critical Device" on page 1295*
- *"Unregistering a Critical Device" on page 1299*
- *"Unregistering All Critical Devices" on page 1304*

Unregistering All Critical Devices

Important - In a Cluster, you must configure all the Cluster Members in the same way.

Description

This command unregisters all critical devices from the Cluster Member.

Syntax

Shell	Command
Gaia Clish	N / A
Expert mode	`cphaconf set_pnote -a [-g] unregister`

Notes:

- The "`-a`" flag specifies that all Pnotes must be unregistered
- The "`-g`" flag applies the command to all configured Virtual Systems

Related topics

- *"Viewing Critical Devices" on page 1329*
- *"Reporting the State of a Critical Device" on page 1300*
- *"Registering a Critical Device" on page 1295*
- *"Registering Critical Devices Listed in a File" on page 1302*
- *"Unregistering a Critical Device" on page 1299*

Configuring the Cluster Control Protocol (CCP) Settings

Important - In a Cluster, you must configure all the Cluster Members in the same way.

Description

Cluster Members configure the Cluster Control Protocol (CCP) mode automatically.

Important - In R81.20, the CCP always runs in the unicast mode.

You can configure the Cluster Control Protocol (CCP) Encryption on the Cluster Members.

See *"Viewing the Cluster Control Protocol (CCP) Settings" on page 1371*.

Syntax for configuring the Cluster Control Protocol (CCP) Encryption

Shell	Command
Gaia Clish	`set cluster member ccpenc {off | on}`
Expert mode	`cphaconf ccp_encrypt {off | on}` `cphaconf ccp_encrypt_key <Key String>`

Initiating Manual Cluster Failover

Description

This command initiates a manual cluster failover (see sk55081).

Syntax

Shell	Command
Gaia Clish	`set cluster member admin {down | up}`
Expert mode	`clusterXL_admin {down | up}`

Example

```
[Expert@Member1:0]# cphaprob state

Cluster Mode:   High Availability (Active Up) with IGMP Membership

ID         Unique Address  Assigned Load   State          Name

1 (local)  11.22.33.245    100%            ACTIVE         Member1
2          11.22.33.246    0%              STANDBY        Member2


Active PNOTEs: None

... ...

[Expert@Member1:0]#

[Expert@Member1:0]# clusterXL_admin down
This command does not survive reboot. To make the change permanent, please run 'set cluster
member admin down/up permanent' in clish or add '-p' at the end of the command in expert mode
Setting member to administratively down state ...
Member current state is DOWN
[Expert@Member1:0]#

[Expert@Member1:0]# cphaprob state

Cluster Mode:   High Availability (Active Up) with IGMP Membership

ID         Unique Address  Assigned Load   State          Name

1 (local)  11.22.33.245    0%              DOWN           Member1
2          11.22.33.246    100%            ACTIVE         Member2


Active PNOTEs: ADMIN

Last member state change event:
   Event Code:                 CLUS-111400
   State change:               ACTIVE -> DOWN
   Reason for state change:    ADMIN_DOWN PNOTE
   Event time:                 Sun Sep  8 19:35:06 2019

Last cluster failover event:
   Transition to new ACTIVE:   Member 1 -> Member 2
   Reason:                     ADMIN_DOWN PNOTE
   Event time:                 Sun Sep  8 19:35:06 2019

Cluster failover count:
   Failover counter:           2
   Time of counter reset:      Sun Sep  8 16:08:34 2019 (reboot)

[Expert@Member1:0]#

[Expert@Member1:0]# clusterXL_admin up
This command does not survive reboot. To make the change permanent, please run 'set cluster
member admin down/up permanent' in clish or add '-p' at the end of the command in expert mode
Setting member to normal operation ...
Member current state is STANDBY
[Expert@Member1:0]#

[Expert@Member1:0]# cphaprob state

Cluster Mode:   High Availability (Active Up) with IGMP Membership

ID         Unique Address  Assigned Load   State          Name

1 (local)  11.22.33.245    0%              STANDBY        Member1
2          11.22.33.246    100%            ACTIVE         Member2


Active PNOTEs: None

Last member state change event:
```

```
   Event Code:                 CLUS-114802
   State change:               DOWN -> STANDBY
   Reason for state change:    There is already an ACTIVE member in the cluster (member 2)
   Event time:                 Sun Sep  8 19:37:03 2019

Last cluster failover event:
   Transition to new ACTIVE:   Member 1 -> Member 2
   Reason:                     ADMIN_DOWN PNOTE
   Event time:                 Sun Sep  8 19:35:06 2019

Cluster failover count:
   Failover counter:           2
   Time of counter reset:      Sun Sep  8 16:08:34 2019 (reboot)

[Expert@Member1:0]#
```

Configuring the Minimal Number of Required Subordinate Interfaces for Bond Load Sharing

Important - In a Cluster, you must configure all the Cluster Members in the same way.

Description

ClusterXL considers a bond in Load Sharing mode to be in the "down" state when fewer than a minimal number of required subordinate interfaces stay in the "up" state.

By default, the minimal number of required subordinate interfaces, which must stay in the "up" state in a bond of **n** subordinate interfaces is **n-1**.

If one more subordinate interface fails (when **n-2** subordinate interfaces stay in the "up" state), ClusterXL considers the bond interface to be in the "down" state, even if the bond contains more than two subordinate interfaces.

If a smaller number of subordinate interfaces can pass the expected traffic, you can configure explicitly the minimal number of required subordinate interfaces.

Divide your maximal expected traffic speed by the speed of your subordinate interfaces and round up the result to find an applicable minimal number of required subordinate interfaces.

Notes:

- Cluster Members save the configuration in the `$FWDIR/conf/cpha_bond_ls_config.conf` file.
- The commands below save the changes in this file.
- Each line in the file has this syntax:

  ```
  <Name of Bond Interface> <Minimal Number of Required Subordinate Interfaces>
  ```

In addition, see *"Viewing Bond Interfaces" on page 1346*.

Syntax to add the minimal number of required subordinate interfaces for a specific Bond interface

Shell	Command
Gaia Clish	`set interface <Name of Bond Interface> links <Minimal Number of Requirement Subordinate Interfaces between 1 and 8>`
Expert mode	`cphaconf bond_ls set <Name of Bond Interface> <Minimal Number of Required Subordinate Interfaces between 1 and 8>`

Syntax to remove the configured minimal number of required subordinate interfaces for a specific Bond interface

Shell	Command
Gaia Clish	`set interface <Name of Bond Interface> links 0`
Expert mode	`cphaconf bond_ls remove <Name of Bond Interface>`

Syntax to see the current configuration of the minimal number of required subordinate interfaces

Shell	Command
Gaia Clish	`show interface <Name of Bond Interface> links`
Expert mode	`cat $FWDIR/conf/cpha_bond_ls_config.conf`

Procedure for Gaia Clish

Step	Instructions
1	Connect to the command line on each Cluster Member.
2	Log in to Gaia Clish.
3	Add or remove the minimal number of required subordinate interfaces for a specific Bond interface: `set interface <Name of Bond Interface> links {Minimal Number of Requirement Subordinate Interfaces> | 0}`
4	Save the configuration: `save config`
5	Examine the configuration: `show interface <Name of Bond Interface> links`
6	In SmartConsole, install the Access Control policy on this cluster object.

Procedure for the Expert mode

Step	Instructions
1	Connect to the command line on each Cluster Member.
2	Log in to the Expert mode.

3	Add or remove the minimal number of required subordinate interfaces for a specific Bond interface:
	`cphaconf bond_ls set <Bond> <Minimal Number of Subordinate Interfaces>`
	`cphaconf bond_ls remove <Bond>`

4	Examine the configuration: `cat $FWDIR/conf/cpha_bond_ls_config.conf`
5	In SmartConsole, install the Access Control policy on this cluster object.

Example for the Expert mode

```
[Expert@Member1:0]# cat $FWDIR/conf/cpha_bond_ls_config.conf
# ... (truncated for brevity) ...
# Example:
# bond0 2

[Expert@Member1:0]#

[Expert@Member1:0]# cphaconf bond_ls set bond1 2
Set operation succeeded

[Expert@Member1:0]# cat $FWDIR/conf/cpha_bond_ls_config.conf
# ... (truncated for brevity) ...
# Example:
# bond0 2

bond1 2
[Expert@Member1:0]#

[Expert@Member1:0]# cphaconf bond_ls remove bond1
Remove operation succeeded

[Expert@Member1:0]#

[Expert@Member1:0]# cat $FWDIR/conf/cpha_bond_ls_config.conf
# ... (truncated for brevity) ...
# Example:
# bond0 2

[Expert@Member1:0]#
```

Configuring Link Monitoring on the Cluster Interfaces

Important - In a Cluster, you must configure all the Cluster Members in the same way.

Description

This procedure configures the Cluster Member to monitor only the physical link on the cluster interfaces (instead of monitoring the Cluster Control Protocol (CCP) packets):

- If a link disappears on the configured interface, the Cluster Member changes the interface's state to **DOWN**.

  This causes the Cluster Member to change its state to **DOWN**.

- If a link appears again on the configured interface, the Cluster Member changes the interface's state back to **UP**.

  This causes the Cluster Member to change its state back to **ACTIVE** or **STANDBY**.

See *"Viewing Cluster State" on page 1323*.

Procedure

Step	Instructions
1	Connect to the command line on the Cluster Member.
2	Log in to the Expert mode.
3	See if the `$FWDIR/conf/cpha_link_monitoring.conf` file already exists: `stat $FWDIR/conf/cpha_link_monitoring.conf`

4	If the `$FWDIR/conf/cpha_link_monitoring.conf` file already exists, create a backup copy:
	`cp -v $FWDIR/conf/cpha_link_monitoring.conf{,_BKP}`
	If the `$FWDIR/conf/cpha_link_monitoring.conf` file does not exist, create it:
	`touch $FWDIR/conf/cpha_link_monitoring.conf`

5	Edit the `$FWDIR/conf/cpha_link_monitoring.conf` file: `vi $FWDIR/conf/cpha_link_monitoring.conf`

6	■ To monitor the link only on specific interfaces:
	Enter the names of the applicable interfaces - each name on a new separate line.
	Example:
	`eth2`
	`eth4`
	■ To monitor the link on all interfaces:
	Enter only this word:
	`all`

7	Save the changes in the file and exit the editor.

Step	Instructions
8	Reboot the Cluster Member. **Important** - This can cause a failover. **Best Practices:** ■ **In High Availability cluster** 1. Perform the configuration steps on all Cluster Members 2. Reboot all the **Standby** Cluster Members 3. Initiate a manual failover on the **Active** Cluster Member 4. Reboot the former **Active** Cluster Member ■ **In Load Sharing Unicast cluster** 1. Perform the configuration steps on all Cluster Members 2. Reboot all the **non-Pivot** Cluster Members 3. Initiate a manual failover on the **Pivot** Cluster Member 4. Reboot the former **Pivot** Cluster Member ■ **In Load Sharing Multicast cluster** 1. Perform the configuration steps on all Cluster Members 2. Reboot all Cluster Members **except one** 3. Initiate a manual failover on the **remaining** Cluster Member 4. Reboot the **remaining** Cluster Member **Note** - See *"Initiating Manual Cluster Failover" on page 1306*.

Configuring the Multi-Version Cluster Mechanism

Description

This command changes the state of the Multi-Version Cluster (MVC) Mechanism - enable or disable it.

Important:

- The MVC Mechanism is *disabled* by default.
- For limitations of the MVC Mechanism, see the *R81.20 Installation and Upgrade Guide* > Chapter *Upgrading Gateways and Clusters* > Section *Upgrading ClusterXL, VSX Cluster, VRRP Cluster* > Section *Multi-Version Cluster Upgrade*.

Syntax

Shell	Command
Gaia Clish	`set cluster member mvc {off	on}`
Expert mode	`cphaconf mvc {off	on}`

Parameters

Parameter	Description
`off`	Disables the MVC Mechanism on this Cluster Member.
`on`	Enables the MVC Mechanism on this Cluster Member.

Notes:

- This command does *not* provide an output. To view the current state of the MVC Mechanism, see *"Viewing the State of the Multi-Version Cluster Mechanism" on page 1372*.
- The change made with this command survives reboot.
- If a specific scenario requires you to disable the MVC Mechanism before the first start of an R81.20 Cluster Member (for example, immediately after an upgrade to R81.20), then disable it before the first policy installation on this Cluster Member.

Configuring Duration of Forced Failover in High Availability Mode

Description

In the ClusterXL High Availability mode, you can force the current Active cluster member to fail over to the specified cluster member for the specified number of minutes.

After the specified duration ends, or after you manually disable the forced failover, the cluster recovers based on the mode you configured in the cluster object:

- **Primary Up** - The cluster fails over to the cluster member that is configured as primary (if it is not currently Active).
- **Active Up** - The current Active cluster member remains Active.

Syntax

Shell	Command
Gaia Clish	`set cluster force_failover member_id <ID> {time <Minutes> on | off}`
Expert mode	`cphaconf force_failover member_id <ID> {time <Minutes> on | off}`

Parameters

Parameter	Description
<ID>	Specifies the ID of the cluster member, to which the current Active cluster member must fail over. See *"Viewing Cluster State" on page 1323*.
`off`	Disables the forced failover.
`on`	Enables the forced failover.

ClusterXL Monitoring Commands

Description

Use the monitoring commands to make sure that the cluster and the Cluster Members work properly, and to define Critical Devices. A Critical Device (also known as a *Problem Notification*, or *pnote*) is a special software device on each Cluster Member, through which the critical aspects for cluster operation are monitored. When the critical monitored component on a Cluster Member fails to report its state on time, or when its state is reported as problematic, the state of that member is immediately changed to 'Down'.

Syntax

Notes:

- In Gaia Clish:
  Enter the **`show cluster<ESC><ESC>`** to see all the available commands.
- In Expert mode:
  Run the **`cphaprob`** command see all the available commands.
  You can run the `cphaprob` commands from Gaia Clish as well.
- Syntax legend:
  1. Curly brackets or braces **{ }**:
     Enclose a list of available commands or parameters, separated by the vertical bar **|**, from which user can enter only one.
  2. Angle brackets **< >**:
     Enclose a variable - a supported value user needs to specify explicitly.
  3. Square brackets or brackets **[ ]**:
     Enclose an optional command or parameter, which user can also enter.
- You can include these commands in scripts to run them automatically.
  The meaning of each command is explained in the next sections.

Table: ClusterXL Monitoring Commands

Description of Command	Command in Gaia Clish	Command in Expert Mode
Show states of Cluster Members and their names (see *"Viewing Cluster State" on page 1323*)	`show cluster state`	`cphaprob [-vs <VSID>] state`
Show Critical Devices (Pnotes) and their states on the Cluster Member (see *"Viewing Critical Devices" on page 1329*)	`show cluster members pnotes {all | problem}`	`cphaprob [-l] [-ia] [-e] list`

Table: ClusterXL Monitoring Commands (continued)

Description of Command	Command in Gaia Clish	Command in Expert Mode
Show cluster interfaces on the cluster member (see *"Viewing Cluster Interfaces" on page 1341*)	`show cluster members interfaces {all | secured | virtual | vlans}`	`cphaprob [-vs all] [-a] [-m] if`
Show cluster bond configuration on the Cluster Member (see *"Viewing Bond Interfaces" on page 1346*)	`show cluster bond {all | name <bond_name>}`	`cphaprob show_bond [<bond_name>]`
Show groups of bonds on the Cluster Member (see *"Viewing Bond Interfaces" on page 1346*)	`N / A`	`cphaprob show_bond_groups`
Show (and reset) cluster failover statistics on the Cluster Member (see *"Viewing Cluster Failover Statistics" on page 1351*)	`show cluster failover [reset {count | history}]`	`cphaprob [-reset {-c | -h}] [-l <count>] show_failover`
Show information about the software version (including hotfixes) on the local Cluster Member and its matches/mismatches with other Cluster Members (see *"Viewing Software Versions on Cluster Members" on page 1353*)	`show cluster release`	`cphaprob release`
Show Delta Sync statistics on the Cluster Member (see *"Viewing Delta Synchronization" on page 1354*)	`show cluster statistics sync [reset]`	`cphaprob [-reset] syncstat`
Show Delta Sync statistics for the Connections table on the Cluster Member (see *"Viewing Cluster Delta Sync Statistics for Connections Table" on page 1362*)	`show cluster statistics transport [reset]`	`cphaprob [-reset] ldstat`
Show the Cluster Control Protocol (CCP) mode on the Cluster Member (see *"Viewing Cluster Interfaces" on page 1341*)	`show cluster members interfaces virtual`	`cphaprob [-vs all] -a if`

Table: ClusterXL Monitoring Commands (continued)

Description of Command	Command in Gaia Clish	Command in Expert Mode
Show the IGMP membership of the Cluster Member (see *"Viewing IGMP Status" on page 1361*)	`show cluster members igmp`	`cphaprob igmp`
Show cluster unique IP's table on the Cluster Member (see *"Viewing Cluster IP Addresses" on page 1363*)	`show cluster members ips` `show cluster members monitored`	`cphaprob tablestat` `cphaprob -m tablestat`
Show the Cluster Member ID Mode in local logs - by Member ID (default) or Member Name (see *"Viewing the Cluster Member ID Mode in Local Logs" on page 1364*)	`show cluster members idmode`	`cphaprob names`
Show interfaces, which the RouteD monitors on the Cluster Member when you configure OSPF (see *"Viewing Interfaces Monitored by RouteD" on page 1365*)	`show ospf interfaces [detailed]`	`cphaprob routedifcs`
Show roles of RouteD daemon on Cluster Members (see *"Viewing Roles of RouteD Daemon on Cluster Members" on page 1366*)	`show cluster roles`	`cphaprob roles`
Show Cluster Correction Statistics (see *"Viewing Cluster Correction Statistics" on page 1367*)	`N / A`	`cphaprob [{-d | -f | -s}] corr`
Show the Cluster Control Protocol (CCP) mode (see *"Viewing the Cluster Control Protocol (CCP) Settings" on page 1371*)	`show cluster members interfaces virtual`	`cphaprob -a if`
Show the Cluster Control Protocol (CCP) Encryption settings (see *"Viewing the Cluster Control Protocol (CCP) Settings" on page 1371*)	`show cluster members ccpenc`	`cphaprob ccp_encrypt`
Shows the state of the Multi-Version Cluster (see *"Viewing the State of the Multi-Version Cluster Mechanism" on page 1372*)	`show cluster members mvc`	`N / A`
Show Full Connectivity Upgrade statistics (see *"Viewing Full Connectivity Upgrade Statistics" on page 1373*)	`N / A`	`cphaprob fcustat`

List of the Gaia Clish "`show cluster`" commands

```
show cluster
      bond
            all
            name <Name of Bond>
      failover
      members
            ccpenc
            idmode
            igmp
            interfaces
                  all
                  secured
                  virtual
                  vlans
            ips
            monitored
            mvc
            pnotes
                  all
                  problem
      release
      roles
      state
      statistics
            sync [reset]
            transport [reset]
```

List of the Expert mode "cphaprob" commands

Note - Some commands are not applicable to 3rd party clusters.

```
cphaprob [-vs <VSID>] state
cphaprob [-reset {-c | -h}] [-l <count>] show_failover
cphaprob names
cphaprob [-reset] [-a] syncstat
cphaprob [-reset] ldstat
cphaprob [-l] [-i[a]] [-e] list
cphaprob [-vs all] [-a] [-m] if
cphaprob show_bond [<bond_name>]
cphaprob show_bond_groups
cphaprob igmp
cphaprob fcustat
cphaprob [-m] tablestat
cphaprob routedifcs
cphaprob roles
cphaprob release
cphaprob ccp_encrypt
cphaprob [{-d | -f | -s}] corr
```

Viewing Cluster State

Description

This command monitors the cluster status (after you set up the cluster).

Syntax

Shell	Command
Gaia Clish	1. `set virtual-system <VSID>` 2. `show cluster state`
Expert mode	`cphaprob [-vs <VSID>] state`

Example

```
Member1> show cluster state

Cluster Mode:   High Availability (Active Up) with IGMP Membership

ID          Unique Address  Assigned Load   State          Name

1 (local)  11.22.33.245    100%            ACTIVE(!)      Member1
2          11.22.33.246    0%              DOWN           Member2


Active PNOTEs: COREXL

Last member state change event:
   Event Code:                 CLUS-116505
   State change:               INIT -> ACTIVE(!)
   Reason for state change:    All other machines are dead (timeout), FULLSYNC PNOTE
   Event time:                 Sun Sep  8 15:28:39 2019
v Cluster failover count:
   Failover counter:           0
   Time of counter reset:      Sun Sep  8 15:28:21 2019 (reboot)

Member1>
```

Description of the "`cphaprob state`" command output fields:

Table: Description of the output fields

Field	Description
Cluster Mode	Can be one of these: ■ Load Sharing (Multicast). ■ Load Sharing (Unicast). ■ High Availability (Primary Up). ■ High Availability (Active Up). ■ Virtual System Load Sharing ■ For third-party clustering products: *Service*, refer to Clustering Definitions and Terms, for more information.
ID	■ In the High Availability mode - indicates the Cluster Member priority, as configured in the cluster object in SmartConsole. ■ In Load Sharing mode - indicates the Cluster Member ID, as configured in the cluster object in SmartConsole.
Unique Address	Usually, shows the IP addresses of the Sync interfaces. In some cases, can show IP addresses of other cluster interfaces.
Assigned Load	■ In the ClusterXL High Availability mode - shows the *Active* Cluster Member with 100% load, and all other *Standby* Cluster Members with 0% load. ■ In ClusterXL Load Sharing modes (Unicast and Multicast) - shows all *Active* Cluster Members with 100% load.
State	■ In the ClusterXL High Availability mode, only one Cluster Member in a fully-functioning cluster must be *ACTIVE*, and the other Cluster Members must be in the *STANDBY* state. ■ In the ClusterXL Load Sharing modes (Unicast and Multicast), all Cluster Members in a fully-functioning cluster must be *ACTIVE*. ■ In 3rd-party clustering configuration, all Cluster Members in a fully-functioning cluster must be *ACTIVE*. This is because this command only reports the status of the Full Synchronization process. See the summary table below.
Name	Shows the names of Cluster Members' objects as configured in SmartConsole.
Active PNOTEs	Shows the Critical Devices that report theirs states as "`problem`" (see *"Viewing Critical Devices" on page 1329*).

Table: Description of the output fields (continued)

Field	Description
Last member state change event	Shows information about the last time this Cluster Member changed its cluster state.
Event Code	Shows an event code. For information, see sk125152.
State change	Shows the previous cluster state and the new cluster state of this Cluster Member.
Reason for state change	Shows the reason why this Cluster Member changed its cluster state.
Event time	Shows the date and the time when this Cluster Member changed its cluster state.
Last cluster failover event	Shows information about the last time a cluster failover occurred.
Transition to new ACTIVE	Shows which Cluster Member became the new *Active*.
Reason	Shows the reason for the last cluster failover.
Event time	Shows the date and the time of the last cluster failover.
Cluster failover count	Shows information about the cluster failovers.
Failover counter	Shows the number of cluster failovers since the boot. Notes: ■ This value survives reboot. ■ This counter is synchronized between Cluster Members.
Time of counter reset	Shows the date and the time of the last counter reset, and the reset initiator.

When you examine the state of the Cluster Member, consider whether it forwards packets, and whether it has a problem that prevents it from forwarding packets. Each state reflects the result of a test on critical devices. This table shows the possible cluster states, and whether or not they represent a problem.

Table: Description of the cluster states

Cluster State	Description	Forwarding packets?	Is this state a problem?
ACTIVE	Everything is OK.	Yes	No
ACTIVE(!) **ACTIVE(!F)** **ACTIVE(!P)** **ACTIVE (!FP)**	A problem was detected, but the Cluster Member still forwards packets, because it is the only member in the cluster, or because there are no other Active members in the cluster. In any other situation, the state of the member is *Down*. ■ `ACTIVE(!)` - See above. ■ `ACTIVE(!F)` - See above. Cluster Member is in the freeze state. ■ `ACTIVE(!P)` - See above. This is the Pivot Cluster Member in Load Sharing Unicast mode. ■ `ACTIVE(!FP)` - See above. This is the Pivot Cluster Member in Load Sharing Unicast mode and it is in the freeze state.	Yes	Yes
DOWN	One of the Critical Devices reports its state as "`problem`" (see *"Viewing Critical Devices" on page 1329*).	No	Yes
LOST	The peer Cluster Member lost connectivity to this local Cluster Member (for example, while the peer Cluster Member is rebooted).	No	Yes

Table: Description of the cluster states (continued)

Cluster State	Description	Forwarding packets?	Is this state a problem?
READY	State *Ready* means that the Cluster Member recognizes itself as a part of the cluster and is literally ready to go into action, but, by design, something prevents it from taking action. Possible reasons that the Cluster Member is not yet Active include: ■ Not all required software components were loaded and initialized yet and/or not all configuration steps finished successfully yet. Before a Cluster Member becomes *Active*, it sends a message to the rest of the Cluster Members, to check if it can become *Active*. In High Availability mode it checks if there is already an Active member and in Load Sharing Unicast mode it checks if there is a Pivot member already. The member remains in the *Ready* state until it receives the response from the rest of the Cluster Members and decides which, which state to choose next (*Active, Standby, Pivot, or non-Pivot*). ■ Software installed on this Cluster Member has a higher version than all the other Cluster Members. For example, when a cluster is upgraded from one version of Check Point Security Gateway to another, and the Cluster Members have different versions of Check Point Security Gateway, the Cluster Members with the new version have the *Ready* state, and the Cluster Members with the previous version have the *Active/Active Attention* state.	No	No

Table: Description of the cluster states (continued)

Cluster State	Description	Forwarding packets?	Is this state a problem?
	This applies only when the Multi-Version Cluster Mechanism is disabled (see *"Viewing the State of the Multi-Version Cluster Mechanism" on page 1372*). See sk42096 for a solution.		
STANDBY	Applies only to a High Availability mode. Means that the Cluster Member waits for an Active Cluster Member to fail in order to start packet forwarding.	No	No
BACKUP	Applies only to a VSX Cluster in Virtual System Load Sharing mode with three or more Cluster Members configured. State of a Virtual System on a third (and so on) VSX Cluster Member.	No	No
INIT	The Cluster Member is in the phase after the boot and until the Full Sync completes.	No	No

Viewing Critical Devices

Description

There are a number of built-in Critical Devices, and the Administrator can define additional Critical Devices.

When a Critical Device reports its state as a "`problem`", the Cluster Member reports its state as "`DOWN`".

To see the list of Critical Devices on a Cluster Member, and of all the other Cluster Members, run the commands listed below on the Cluster Member.

Table: Built-in Critical Devices

Critical Device	Description	Meaning of the "OK" state	Meaning of the "problem" state
`Problem Notification`	Monitors all the Critical Devices.	None of the Critical Devices on this Cluster Member report its state as `problem`.	At least one of the Critical Devices on this Cluster Member reports its state as "`problem`".
`Init`	Monitors if "`HA module`" was initialized successfully. See sk36372.	This Cluster Member receives cluster state information from peer Cluster Members.	
`Interface Active Check`	Monitors the state of cluster interfaces.	All cluster interfaces on this Cluster Member are up (CCP packets are sent and received on all cluster interfaces).	At least one of the cluster interfaces on this Cluster Member is down (CCP packets are not sent and/or received on time).

Table: Built-in Critical Devices (continued)

Critical Device	Description	Meaning of the "OK" state	Meaning of the "problem" state
`Load Balancing Configuration`	Currently is not used (see sk36373).		
`Recovery Delay`	Monitors the state of a Virtual System (see sk92353).	State of a Virtual System can be changed on this Cluster Member.	State of a Virtual System cannot be changed yet on this Cluster Member.
`CoreXL Configuration`	Monitors CoreXL configuration for inconsistencies on all Cluster Members.	Number of configured CoreXL Firewall instances on this Cluster Member is the same as on all peer Cluster Members.	Number of configured CoreXL Firewall instances on this Cluster Member is different from peer Cluster Members. **Important** - A Cluster Member with a greater number of CoreXL Firewall instances changes its state to DOWN.
`Fullsync`	Monitors if Full Sync on this Cluster Member completed successfully.	This Cluster Member completed Full Sync successfully.	This Cluster Member was not able to complete Full Sync.
`Policy`	Monitors if the Security Policy is installed.	This Cluster Member successfully installed Security Policy.	Security Policy is not currently installed on this Cluster Member.

Table: Built-in Critical Devices (continued)

Critical Device	Description	Meaning of the "OK" state	Meaning of the "problem" state
`fwd`	Monitors the Security Gateway process called `fwd`.	`fwd` daemon on this Cluster Member reported its state on time.	`fwd` daemon on this Cluster Member did not report its state on time.
`cphad`	Monitors the ClusterXL process called `cphamcset`. also see the `$FWDIR/log/cphamcset.elg` file.	`cphamcset` daemon on this Cluster Member reported its state on time.	`cphamcset` daemon on this Cluster Member did not report its state on time.
`routed`	Monitors the Gaia process called `routed`.	`routed` daemon on this Cluster Member reported its state on time.	`routed` daemon on this Cluster Member did not report its state on time.
`cvpnd`	Monitors the Mobile Access back-end process called `cvpnd`. This pnote appears if Mobile Access Software Blade is enabled.	`cvpnd` daemon on this Cluster Member reported its state on time.	`cvpnd` daemon on this Cluster Member did not report its state on time.
`ted`	Monitors the Threat Emulation process called `ted`.	`ted` daemon on this Cluster Member reported its state on time.	`ted` daemon on this Cluster Member did not report its state on time.

Table: Built-in Critical Devices (continued)

Critical Device	Description	Meaning of the "OK" state	Meaning of the "problem" state
`VSX`	Monitors all Virtual Systems in VSX Cluster.	On VS0, means that states of all Virtual Systems are not `Down` on this Cluster Member. On other Virtual Systems, means that VS0 is alive on this Cluster Member.	Minimum of blocking states of all Virtual Systems is not "active" (the VSIDs will be printed on the line `Problematic VSIDs:`) on this Cluster Member.
`VSX Config`	Monitors the consistency and health of the VSX configuration.	All Virtual Systems (VS) and Virtual Routers are properly configured and synchronized.	There is a mismatch or inconsistency in the VSX configuration between cluster members.

Table: Built-in Critical Devices (continued)

Critical Device	Description	Meaning of the "OK" state	Meaning of the "problem" state
`Instances`	This Critical Device appears in VSX HA mode (not VSLS) cluster.	The number of CoreXL Firewall instances in the received CCP packet matches the number of loaded CoreXL Firewall instances on this VSX Cluster Member or this Virtual System.	There is a mismatch between the number of CoreXL Firewall instances in the received CCP packet and the number of loaded CoreXL Firewall instances on this VSX Cluster Member or this Virtual System (see sk106912).
`Hibernating`	This pnote appears in VSX VSLS mode cluster with 3 and more Cluster Members. This pnote shows if this Virtual System is in "Backup" (hibernated) state. Also see sk114557.	This Virtual System is in "Backup" (hibernated) state on this Cluster Member.	
`admin_down`	Monitors the Critical Device "`admin_down`".		User ran the `clusterXL_admin down` command on this Cluster Member. See *"The clusterXL_admin Script" on page 1386*.
`host_monitor`	Monitors the Critical Device "`host_monitor`". User executed the `$FWDIR/bin/clusterXL_monitor_ips` script. See *"The clusterXL_monitor_ips Script" on page 1390*.	All monitored IP addresses on this Cluster Member replied to pings.	At least one of the monitored IP addresses on this Cluster Member did not reply to at least one ping.

Table: Built-in Critical Devices (continued)

Critical Device	Description	Meaning of the "OK" state	Meaning of the "problem" state
A name of a user space process (except `fwd`, `routed`, `cvpnd`, `ted`)	Administrator executed the `$FWDIR/bin/clusterXL_monitor_process` script. See *"The clusterXL_monitor_process Script" on page 1394*.	All monitored user space processes on this Cluster Member are running.	At least one of the monitored user space on this Cluster Member processes is not running.

Table: Built-in Critical Devices (continued)

Critical Device	Description	Meaning of the "OK" state	Meaning of the "problem" state
`Local Probing`	Monitors the probing mechanism on the cluster interfaces (see the term **Probing** in the *"Glossary" on page 2025*).	CCP packets are received on all cluster interfaces.	At least one of the cluster interfaces on this Cluster Member does not (or did not) **receive** CCP packets for 5 seconds. The probing started for the network connected to the affected interface.

Table: Built-in Critical Devices (continued)

Critical Device	Description	Meaning of the "OK" state	Meaning of the "problem" state

Syntax

Shell	Command
Gaia Clish	`show cluster members pnotes {all | problem}`
Expert mode	`cphaprob [-l] [-ia] [-e] list`

Where:

Command	Description
`show cluster members pnotes all`	Shows the list of all Critical Devices
`show cluster members pnotes problem`	Shows the list of all the "`Built-in Devices`" and the "`Registered Devices`" that report their state as "problem"
`cphaprob -l`	Shows the list of all Critical Devices
`cphaprob -i list`	When there are no issues on the Cluster Member, shows: `There are no pnotes in problem state` When a Critical Device reports a problem, prints only the Critical Device that reports its state as "`problem`".
`cphaprob -ia list`	When there are no issues on the Cluster Member, shows: `There are no pnotes in problem state` When a Critical Device reports a problem, prints the Critical Device "`Problem Notification`" and the Critical Device that reports its state as "`problem`"
`cphaprob -e list`	When there are no issues on the Cluster Member, shows: `There are no pnotes in problem state` When a Critical Device reports a problem, prints only the Critical Device that reports its state as "`problem`"

Related topics

- *"Reporting the State of a Critical Device" on page 1300*
- *"Registering a Critical Device" on page 1295*
- *"Registering Critical Devices Listed in a File" on page 1302*
- *"Unregistering a Critical Device" on page 1299*
- *"Unregistering All Critical Devices" on page 1304*

Examples

Example 1 - Critical Device '`fwd`'

Critical Device `fwd` reports its state as `problem` because the `fwd` process is down.

```
[Expert@Member1:0]# cphaprob -l list

Built-in Devices:

Device Name: Interface Active Check
Current state: OK

Device Name: Recovery Delay
Current state: OK

Device Name: CoreXL Configuration
Current state: OK

Registered Devices:

Device Name: Fullsync
Registration number: 0
Timeout: none
Current state: OK
Time since last report: 1753.7 sec

Device Name: Policy
Registration number: 1
Timeout: none
Current state: OK
Time since last report: 1753.7 sec

Device Name: routed
Registration number: 2
Timeout: none
Current state: OK
Time since last report: 940.3 sec

Device Name: fwd
Registration number: 3
Timeout: 30 sec
Current state: problem
Time since last report: 1782.9 sec
Process Status: DOWN

Device Name: cphad
Registration number: 4
Timeout: 30 sec
Current state: OK
Time since last report: 1778.3 sec
Process Status: UP

Device Name: VSX
Registration number: 5
Timeout: none
Current state: OK
Time since last report: 1773.3 sec

Device Name: Init
Registration number: 6
Timeout: none
Current state: OK
Time since last report: 1773.3 sec

[Expert@Member1:0]#
```

Example 2 - Critical Device '`CoreXL Configuration`'

Critical Device `CoreXL Configuration` reports its state as `problem` because the numbers of CoreXL Firewall instances do not match between the Cluster Members.

```
[Expert@Member1:0]# cphaprob -l list

Built-in Devices:

Device Name: Interface Active Check
Current state: OK

Device Name: Recovery Delay
Current state: OK

Device Name: CoreXL Configuration
Current state: problem (non-blocking)

Registered Devices:

Device Name: Fullsync
Registration number: 0
Timeout: none
Current state: OK
Time since last report: 1753.7 sec

Device Name: Policy
Registration number: 1
Timeout: none
Current state: OK
Time since last report: 1753.7 sec

Device Name: routed
Registration number: 2
Timeout: none
Current state: OK
Time since last report: 940.3 sec

Device Name: fwd
Registration number: 3
Timeout: 30 sec
Current state: OK
Time since last report: 1782.9 sec
Process Status: UP

Device Name: cphad
Registration number: 4
Timeout: 30 sec
Current state: OK
Time since last report: 1778.3 sec
Process Status: UP

Device Name: VSX
Registration number: 5
Timeout: none
Current state: OK
Time since last report: 1773.3 sec

Device Name: Init
Registration number: 6
Timeout: none
Current state: OK
Time since last report: 1773.3 sec

[Expert@Member1:0]#
```

Viewing Cluster Interfaces

Description

This command shows the state of the Cluster Member interfaces and the virtual cluster interfaces.

ClusterXL treats the interfaces as Critical Devices. ClusterXL makes sure that interfaces can send and receive CCP packets.

ClusterXL also sets the required minimal number of functional interfaces to the largest number of functional interfaces ClusterXL detected since the last reboot. If the number of functional interfaces is less than the required number, ClusterXL declares the Cluster Member as failed and starts a failover. The same applies to the synchronization interfaces, where only good synchronization interfaces are counted.

When an interface is DOWN, it means that the interface cannot receive or send CCP packets, or both. An interface may also be able to receive, but not send CCP packets. The time you see in the command's output is the number of seconds that elapsed since the interface was last able to receive or send a CCP packet.

Syntax

Shell	Command
Gaia Clish	1. `set virtual-system <VSID>` 2. `show cluster members interfaces {all | secured | virtual | vlans}`
Expert mode	`cphaprob [-vs all] [-a] [-m] if`

Where:

Command	Description
`show cluster members interfaces all`	Shows full list of all cluster interfaces: ■ including the number of required interfaces ■ including Network Objective ■ including VLAN monitoring mode, or list of monitored VLAN interfaces
`show cluster members interfaces secured`	Shows only cluster interfaces (Cluster and Sync) and their states: ■ without Network Objective ■ without VLAN monitoring mode ■ without monitored VLAN interfaces
`show cluster members interfaces virtual`	Shows full list of cluster virtual interfaces and their states: ■ including the number of required interfaces ■ including Network Objective ■ without VLAN monitoring mode ■ without monitored VLAN interfaces
`show cluster members interfaces vlans`	Shows only monitored VLAN interfaces
`cphaprob if`	Shows only cluster interfaces (Cluster and Sync) and their states: ■ without Network Objective ■ without VLAN monitoring mode ■ without monitored VLAN interfaces
`cphaprob -a if`	Shows full list of cluster interfaces and their states: ■ including the number of required interfaces ■ including Network Objective ■ without VLAN monitoring mode ■ without monitored VLAN interfaces

Command	Description
`cphaprob -a -m if`	Shows full list of all cluster interfaces and their states: ■ including the number of required interfaces ■ including Network Objective ■ including VLAN monitoring mode, or list of monitored VLAN interfaces

Output

The output of these commands must be identical to the configuration in the cluster object's **Network Management** page in SmartConsole.

Example

```
[Expert@Member1:0]# cphaprob -a -m if

CCP mode: Manual (Unicast)
Required interfaces: 4
Required secured interfaces: 1


Interface Name:      Status:

eth0                 UP
eth1 (S)             UP
eth2 (LM)            UP
bond1 (LS)           UP

S - sync, LM - link monitor, HA/LS - bond type

Virtual cluster interfaces: 3

eth0            192.168.3.247
eth2            44.55.66.247
bond1           77.88.99.247


No VLANs are monitored on the member

[Expert@Member1:0]#
```

Description of the "`cphaprob -a -m if`" command output fields:

Table: Description of the output fields

Field, or Text	Description
CCP mode	Shows the CCP mode. The default mode is `Unicast`. **Important** - In R81.20, the CCP always runs in the unicast mode.

Table: Description of the output fields (continued)

Field, or Text	Description
Required interfaces	Shows the total number of monitored cluster interfaces, including the Sync interface. This number is based on the configuration of the cluster object > **Network Management** page.
Required secured interfaces	Shows the total number of the required Sync interfaces. This number is based on the configuration of the cluster object > **Network Management** page.
Non-Monitored	This means that Cluster Member does not monitor the state of this interface. In SmartConsole, in the cluster object > **Network Management** page, administrator configured the Network Type **Private** for this interface.
UP	This means that Cluster Member monitors the state of this interface. The current cluster state of this interface is UP, which means this interface can send and receive CCP packets. In SmartConsole, in the cluster object > **Network Management** page, administrator configured one of these Network Types for this interface: **Cluster**, **Sync**, or **Cluster + Sync**.
DOWN	This means that Cluster Members monitors the state of this interface. The current cluster state of this interface is DOWN, which means this interface cannot send CCP packets, receive CCP packets, or both. In SmartConsole, in the cluster object > **Network Management** page, administrator configured one of these Network Types for this interface: **Cluster**, **Sync**, or **Cluster + Sync**.
(S)	This interface is a Sync interface. In SmartConsole, in the cluster object > **Network Management** page, administrator configured one of these Network Types for this interface: **Sync**, or **Cluster + Sync**.

Table: Description of the output fields (continued)

Field, or Text	Description
(LM)	This interface is configured in the `$FWDIR/conf/cpha_link_monitoring.conf` file. Cluster Member monitors only the link on this interface (does **not** monitor the received or sent CCP packets). See *"Configuring Link Monitoring on the Cluster Interfaces" on page 1313*.
(HA)	This interface is a Bond interface in High Availability mode.
(LS)	This interface is a Bond interface in Load Sharing mode.
Virtual cluster interfaces	Shows the total number of the configured virtual cluster interfaces. This number is based on the configuration of the cluster object > **Network Management** page.
No VLANs are monitored on the member	Shows the VLAN monitoring mode - there are no VLAN interfaces configured on the cluster interfaces.
Monitoring mode is Monitor all VLANs: All VLANs are monitored	Shows the VLAN monitoring mode - there are some VLAN interfaces configured on the cluster interfaces, and Cluster Member monitors all VLAN IDs.
Monitoring mode is Monitor specific VLAN: Only specified VLANs are monitored	Shows the VLAN monitoring mode - there are some VLAN interfaces configured on the cluster interfaces, and Cluster Member monitors only specific VLAN IDs.

Viewing Bond Interfaces

Description

This command shows the configuration of bond interfaces and their subordinate interfaces.

Syntax

Shell	Command
Gaia Clish	1. `show cluster bond {all | name <bond_name>}` 2. `show bonding groups`
Expert mode	`cphaprob show_bond [<bond_name>]` `cphaprob show_bond_groups`

Where:

Command	Description

`show cluster bond all`
`show bonding groups`
`cphaprob show_bond`
	Shows configuration of all configured bond interfaces

`show cluster bond name <bond_name>` `cphaprob show_bond <bond_name>`	Shows configuration of the specified bond interface
`cphaprob show_bond_groups`	Shows the configured Groups of Bonds and their settings.

Examples

Example 1 - 'cphaprob show_bond'

```
[Expert@Member2:0]# cphaprob show_bond

                                    |Slaves     |Slaves  |Slaves
Bond name  |Mode                |State |configured |link up |required
-----------+--------------------+------+-----------+--------+--------
bond1      | High Availability | UP   | 2         | 2      | 1

Legend:
-------
UP!               - Bond interface state is UP, yet attention is required
Slaves configured - number of slave interfaces configured on the bond
Slaves link up    - number of operational slaves
Slaves required   - minimal number of operational slaves required for bond to be UP

[Expert@Member2:0]#

Member2> show bonding groups
Bonding Interface: 1
    Bond Configuration
        xmit-hash-policy Not configured
        down-delay 200
        primary Not configured
        lacp-rate Not configured
        mode active-backup
        up-delay 200
        mii-interval 100
        Bond Interfaces
            eth3
            eth4
Member2>
```

Description of the output fields for the "`cphaprob show_bond`" and "`show cluster bond all`" commands:

Table: Description of the output fields

Field	Description
Bond name	Name of the Gaia bonding group.
Mode	Bonding mode of this Gaia bonding group. One of these: ■ `High Availability` ■ `Load Sharing`
State	State of the Gaia bonding group: ■ `UP` - Bond interface is fully operational ■ `UP!` - Bond interface state is UP, yet attention is required ■ `DOWN` - Bond interface failed
Slaves configured	Total number of physical subordinate interfaces configured in this Gaia bonding group.

Table: Description of the output fields (continued)

Field	Description
Slaves link up	Number of operational physical subordinate interfaces in this Gaia bonding group.
Slaves required	Minimal number of operational physical subordinate interfaces required for the state of this Gaia bonding group to be UP.

Example 2 - 'cphaprob show_bond <bond_name>'

```
[Expert@Member2:0]# cphaprob show_bond bond1

Bond name:      bond1
Bond mode:      High Availability
Bond status:    UP

Configured slave interfaces: 2
In use slave interfaces:     2
Required slave interfaces:   1

Slave name      | Status          | Link
----------------+-----------------+-------
eth4            | Active          | Yes
eth3            | Backup          | Yes

[Expert@Member2:0]#
```

Description of the output fields for the "`cphaprob show_bond <`*`bond_name`*`>`" and "`show cluster bond name <`*`bond_name`*`>`" commands:

Table: Description of the output fields

Field	Description
Bond name	Name of the Gaia bonding group.
Bond mode	Bonding mode of this Gaia bonding group. One of these: ■ `High Availability` ■ `Load Sharing`
Bond status	Status of the Gaia bonding group. One of these: ■ `UP` - Bond interface is fully operational ■ `UP!` - Bond interface state is UP, yet attention is required ■ `DOWN` - Bond interface failed
Configured slave interfaces	Total number of physical subordinate interfaces configured in this Gaia bonding group.
In use slave interfaces	Number of operational physical subordinate interfaces in this Gaia bonding group.

Table: Description of the output fields (continued)

Field	Description
Required slave interfaces	Minimal number of operational physical subordinate interfaces required for the state of this Gaia bonding group to be UP.
Slave name	Names of physical subordinate interfaces configured in this Gaia bonding group.
Status	Status of physical subordinate interfaces in this Gaia bonding group. One of these: ■ `Active` - In High Availability or Load Sharing bonding mode. This subordinate interface is currently handling traffic. ■ `Backup` - In High Availability bonding mode only. This subordinate interface is ready and can support internal bond failover. ■ `Not Available` - In High Availability or Load Sharing bonding mode. The physical link on this subordinate interface is lost, or this Cluster Member is in status *Down*. The bond cannot failover internally in this state.
Link	State of the physical link on the physical subordinate interfaces in this Gaia bonding group. One of these: ■ `Yes` - Link is present ■ `No` - Link is lost

Example 3 - 'cphaprob show_bond_groups'

```
[Expert@Member2:0]# cphaprob show_bond_groups

                               | Required     | Bonds    | Bonds
Group of bonds name | State    | active bonds | in group | status
--------------------+----------+--------------+----------+--------+
GoB0                | UP       | 1            |          |
                    |          |              | bond1    |   UP
                    |          |              | bond2    |   UP


Legend:
---------
Bonds in group        - a list of the bonds in the bond group
Required active bonds - number of required active bonds
[Expert@Member2:0]#
```

Description of the output fields for the "`cphaprob show_bond_groups`" command:

Table: Description of the output fields

Field	Description
Group of bonds name	Name of the Group of Bonds.
State	State of the Group of Bonds. One of these: ■ `UP` - Group of Bonds is fully operational ■ `DOWN` - Group of Bonds failed
Required active bonds	Number of required active bonds in this Group of Bonds.
Bonds in group	Names of the Gaia bond interfaces configured in this Group of Bonds.
Bonds status	State of the Gaia bond interface. One of these: ■ `UP` - Bond interface is fully operational ■ `DOWN` - Bond interface failed

Viewing Cluster Failover Statistics

Description

This command shows the cluster failover statistics on the Cluster Member:

- Number of failovers that happened
- Failover reason
- The time of the last failover event

Syntax to show the statistics

Shell	Command
Gaia Clish	`show cluster failover`
Expert mode	`cphaprob [-l <number>] show_failover`

Syntax to reset the statistics

Shell	Command
Gaia Clish	`show cluster failover reset {count | history}`
Expert mode	`cphaprob -reset {-c | -h} show_failover`

Parameters

Parameter	Description
`-l <number>`	Specifies how many of last failover events to show (between 1 and 50)
`count` `-c`	Resets the counter of failover events
`history` `-h`	Resets the history of failover events

Example

```
[Expert@Member1:0]# cphaprob show_failover

Last cluster failover event:
   Transition to new ACTIVE:   Member 2 -> Member 1
   Reason:                     ADMIN_DOWN PNOTE
   Event time:                 Sun Sep  8 18:21:44 2019

Cluster failover count:
   Failover counter:           1
   Time of counter reset:      Sun Sep  8 16:08:34 2019 (reboot)


Cluster failover history (last 20 failovers since reboot/reset on Sun Sep  8 16:08:34 2019):

 No. Time:                     Transition:           CPU:  Reason:
 - - -
```

Viewing Software Versions on Cluster Members

Description

This command shows information about the software version (including private hotfixes) on the local Cluster Member and its matches / mismatches with other Cluster Members.

Syntax

Shell	Command
Gaia Clish	`show cluster release`
Expert mode	`cphaprob release`

Example

```
[Expert@Member1:0]# cphaprob release

Release:                R80.40 T136

Kernel build:           994000117
FW1 build:              994000116
FW1 private fixes:      None

ID          SW release

1 (local)   R80.40 T136
2           R80.40 T136

[Expert@Member1:0]#
```

Viewing Delta Synchronization

Heavily loaded clusters and clusters with geographically separated members pose special challenges.

High connection rates, and large distances between the members can lead to delays that affect the operation of the cluster.

Monitor the operation of the State Synchronization mechanism in highly loaded and distributed clusters.

Perform these troubleshooting steps:

1. Examine the Delta Sync statistics counters:

Shell	Command
Gaia Clish	`show cluster statistics sync`
Expert mode	`cphaprob syncstat`

2. Change the values of the applicable synchronization global configuration parameters.
3. Reset the Delta Sync statistics counters:

Shell	Command
Gaia Clish	`show cluster statistics sync reset`
Expert mode	`cphaprob -reset syncstat`

4. Examine the Delta Sync statistics to see if the problem is solved.
5. Solve any identified problem.

Example output of the "`show cluster statistics sync`" and "`cphaprob syncstat`" commands from a Cluster Member:

```
Delta Sync Statistics

Sync status: OK

Drops:
Lost updates.............................  0
Lost bulk update events..................  0
Oversized updates not sent...............  0

Sync at risk:
Sent reject notifications................  0
Received reject notifications............  0

Sent messages:
Total generated sync messages............  26079
Sent retransmission requests.............  0
Sent retransmission updates..............  0
Peak fragments per update................  1

Received messages:
Total received updates...................  3710
Received retransmission requests.........  0

Sync Interface:
Name.....................................  eth1
Link speed...............................  1000Mb/s
Rate.....................................  46000 [Bps]
Peak rate................................  46000 [Bps]
Link usage...............................   0%
Total....................................  376827[KB]

Queue sizes (num of updates):
Sending queue size.......................  512
Receiving queue size.....................  256
Fragments queue size.....................  50

Timers:
Delta Sync interval (ms).................  100

Reset on Sun Sep  8 16:09:15 2019 (triggered by fullsync).
```

Each section of the output is described below.

The "Sync status:" section

This section shows the status of the Delta Sync mechanism. One of these:

- `Sync status: OK`
- `Sync status: Off - Full-sync failure`
- `Sync status: Off - Policy installation failure`
- `Sync status: Off - Cluster module not started`
- `Sync status: Off - SIC failure`
- `Sync status: Off - Full-sync checksum error`
- `Sync status: Off - Full-sync received queue is full`

- Sync status: Off - Release version mismatch
- Sync status: Off - Connection to remote member timed-out
- Sync status: Off - Connection terminated by remote member
- Sync status: Off - Could not start a connection to remote member
- Sync status: Off - cpstart
- Sync status: Off - cpstop
- Sync status: Off - Manually disabled sync
- Sync status: Off - Was not able to start for more than X second
- Sync status: Off - Boot
- Sync status: Off - Connectivity Upgrade (CU)
- Sync status: Off - cphastop
- Sync status: Off - Policy unloaded
- Sync status: Off - Hibernation
- Sync status: Off - OSU deactivated
- Sync status: Off - Sync interface down
- Sync status: Fullsync in progress
- Sync status: Problem (Able to send sync packets, unable to receive sync packets)
- Sync status: Problem (Able to send sync packets, saving incoming sync packets)
- Sync status: Problem (Able to send sync packets, able to receive sync packets)
- Sync status: Problem (Unable to send sync packets, unable to receive sync packets)
- Sync status: Problem (Unable to send sync packets, saving incoming sync packets)
- Sync status: Problem (Unable to send sync packets, able to receive sync packets)

The "Drops:" section

This section shows statistics for drops on the Delta Sync network.

Table: Description of the output fields

Field	Description
Lost updates	Shows how many Delta Sync updates this Cluster Member considers as lost (based on sequence numbers in CCP packets). If this counter shows a value greater than 0, this Cluster Member lost Delta Sync updates. **Possible mitigation:** Increase the size of the Sending Queue and the size of the Receiving Queue: ■ Increase the size of the Sending Queue, if the counter **Received reject notification** is increasing. ■ Increase the size of the Receiving Queue, if the counter **Received reject notification** is not increasing.
Lost bulk update events	Shows how many times this Cluster Member missed Delta Sync updates. (bulk update = twice the size of the local receiving queue) This counter increases when this Cluster Member receives a Delta Sync update with a sequence number much greater than expected. This probably indicates some networking issues that cause massive packet drops. This counter increases when the amount of missed Delta Sync updates is more than twice the local Receiving Queue Size. **Possible mitigation:** ■ If the counter's value is steady, this might indicate a one-time synchronization problem that can be resolved by running manual Full Sync. See sk37029. ■ If the counter's value keeps increasing, probable there are some networking issues. Increase the sizes of both the Receiving Queue and Sending Queue.
Oversized updates not sent	Shows how many oversized Delta Sync updates were discarded before sending them. This counter increases when Delta Sync update is larger than the local Fragments Queue Size. **Possible mitigation:** ■ If the counter's value is steady, increase the size of the Sending Queue. ■ If the counter's value keeps increasing, contact *Check Point Support*.

The "Sync at risk:" section

This section shows statistics that the Sending Queue is at full capacity and rejects Delta Sync retransmission requests.

Table: Description of the output fields

Field	Description
Sent reject notifications	Shows how many times this Cluster Member rejected Delta Sync retransmission requests from its peer Cluster Members, because this Cluster Member does not hold the requested Delta Sync update anymore.
Received reject notification	Shows how many reject notifications this Cluster Member received from its peer Cluster Members.

The "Sent updates:" section

This section shows statistics for Delta Sync updates sent by this Cluster Member to its peer Cluster Members.

Table: Description of the output fields

Field	Description
Total generated sync messages	Shows how many Delta Sync updates were generated. This counts the Delta Sync updates, Retransmission Requests, Retransmission Acknowledgments, and so on.
Sent retransmission requests	Shows how many times this Cluster Member asked its peer Cluster Members to retransmit specific Delta Sync update(s). Retransmission requests are sent when certain Delta Sync updates (with a specified sequence number) are missing, while the sending Cluster Member already received Delta Sync updates with advanced sequences. **Note** - Compare the number of **Sent retransmission requests** to the **Total generated sync messages** of the other Cluster Members. A large counter's value can imply connectivity problems. If the counter's value is unreasonably high (more than 30% of the **Total generated sync messages** of other Cluster Members), contact *Check Point Support* equipped with the entire output and a detailed description of the network topology and configuration.
Sent retransmission updates	Shows how many times this Cluster Member retransmitted specific Delta Sync update(s) at the requests from its peer Cluster Members.

Table: Description of the output fields (continued)

Field	Description
Peak fragments per update	Shows the peak amount of fragments in the Fragments Queue on this Cluster Member (usually, should be 1).

The "Received updates:" section

This section shows statistics for Delta Sync updates that were received by this Cluster Member from its peer Cluster Members.

Table: Description of the output fields

Field	Description
Total received updates	Shows the total number of Delta Sync updates this Cluster Member received from its peer Cluster Members. This counts only Delta Sync updates (not Retransmission Requests, Retransmission Acknowledgments, and others).
Received retransmission requests	Shows how many retransmission requests this Cluster Member received from its peer Cluster Members. A large counter's value can imply connectivity problems. If the counter's value is unreasonably high (more than 30% of the **Total generated sync messages** on this Cluster Member), contact *Check Point Support* equipped with the entire output and a detailed description of the network topology and configuration.

The "Queue sizes (num of updates):" section

This section shows the sizes of the Delta Sync queues.

Table: Description of the output fields

Field	Description
Sending queue size	Shows the size of the cyclic queue, which buffers all the Delta Sync updates that were already sent until it receives an acknowledgment from the peer Cluster Members. This queue is needed for retransmitting the requested Delta Sync updates. Each Cluster Member has one Sending Queue. Default: 512 Delta Sync updates, which is also the minimal value.

Table: Description of the output fields (continued)

Field	Description
Receiving queue size	Shows the size of the cyclic queue, which buffers the received Delta Sync updates in two cases: ■ When Delta Sync updates are missing, this queue is used to hold the remaining received Delta Sync updates until the lost Delta Sync updates are retransmitted (Cluster Members must keep the order, in which they save the Delta Sync updates in the kernel tables). ■ This queue is used to re-assemble a fragmented Delta Sync update. Each Cluster Member has one Receiving Queue. Default: 256 Delta Sync updates, which is also the minimal value.
Fragments queue size	Shows the size of the queue, which is used to prepare a Delta Sync update before moving it to the Sending Queue. Notes: ■ This queue must be smaller than the Sending Queue. ■ This queue must be significantly smaller than the Receiving Queue. Default: 50 Delta Sync updates, which is also the minimal value.

The "Timers:" section

This section shows the Delta Sync timers.

Field	Description
Delta Sync interval (ms)	Shows the interval at which this Cluster Member sends the Delta Sync updates from its Sending Queue. The base time unit is 100ms (or 1 *tick*). Default: 100 ms, which is also the minimum value. See *Increasing the Sync Timer*.

The "Reset on XXX (triggered XXX)" section

Shows the date and the time of last statistics reset.

In parentheses, it shows how the last statistics was triggered - "`manually`", or "`by fullsync`".

Viewing IGMP Status

Description

This command shows the IGMP membership status.

Syntax

Shell	Command
Gaia Clish	`show cluster members igmp`
Expert mode	`cphaprob igmp`

Example

```
[Expert@Member1:0]# cphaprob igmp

IGMP Membership: Enabled
Supported Version: 2
Report Interval [sec]: 60

IGMP queries are replied only by Operating System

Interface        Host Group      Multicast Address  Last ver.  Last Query[sec]
-------------------------------------------------------------------------------
eth0             224.168.3.247   01:00:5e:28:03:f7     N/A        N/A
eth1             224.22.33.250   01:00:5e:16:21:fa     N/A        N/A
eth2             224.55.66.247   01:00:5e:37:42:f7     N/A        N/A

[Expert@Member1:0]#
```

Viewing Cluster Delta Sync Statistics for Connections Table

Description

This command shows Delta Sync statistics about the operations performed in the Connections Kernel Table (id 8158).

The output shows operations such as creating a new connection (`SET`), updating a connection (`REFRESH`), deleting a connection (`DELETE`), and so on.

Syntax

Shell	Command
Gaia Clish	`show cluster statistics transport [reset]`
Expert mode	`cphaprob [-reset] ldstat`

The "`reset`" flag resets the kernel statistics, which were collected since the last reboot or reset.

Example

```
[Expert@Member1:0]# cphaprob ldstat

Operand              Calls     Bytes     Average   Ratio %
-----------------------------------------------------------
ERROR                0         0         0         0
SET                  354       51404     145       33
RENAME               0         0         0         0
REFRESH              1359      70668     52        46
DELETE               290       10440     36        6
SLINK                193       12352     64        8
UNLINK               0         0         0         0
MODIFYFIELDS         91        7280      80        4
RECORD DATA CONN     0         0         0         0
COMPLETE DATA CONN   0         0         0         0

Total bytes sent: 161292 (0 MB) in 1797 packets. Average 89

[Expert@Member1:0]#
```

Viewing Cluster IP Addresses

Description

This command shows the IP addresses and interfaces of the Cluster Members.

Syntax to see all interfaces

Shell	Command
Gaia Clish	`show cluster members ips`
Expert mode	`cphaprob tablestat`

Syntax to see only the monitored interfaces

Shell	Command
Gaia Clish	`show cluster members monitored`
Expert mode	`cphaprob -m tablestat`

Example

Note - To see name of interfaces that correspond to numbers in the "**Interface**" column, run the *"fw ctl iflist" on page 1102* command.

```
[Expert@Member1:0]# cphaprob tablestat

----   Unique IP's Table  ----

Member          Interface       IP-Address
-----------------------------------------

(Local)
0               1               192.168.3.245
0               2               11.22.33.245
0               3               44.55.66.245

1               1               192.168.3.246
1               2               11.22.33.246
1               3               44.55.66.246

-----------------------------------------


[Expert@Member1:0]#
[Expert@Member1:0]# fw ctl iflist
1 : eth0
2 : eth1
3 : eth2
[Expert@Member1:0]#
```

Viewing the Cluster Member ID Mode in Local Logs

Description

This command shows how the local ClusterXL logs show the Cluster Member - by its Member ID (default), or its Member Name.

See *"Configuring the Cluster Member ID Mode in Local Logs" on page 1294*.

Syntax

Shell	Command
Gaia Clish	`show cluster members idmode`
Expert mode	`cphaprob names`

Example

```
[Expert@Member1:0]# cphaprob names

Current member print mode in local logs is set to: ID

[Expert@Member1:0]#
```

Viewing Interfaces Monitored by RouteD

Description

This command shows the interfaces, which the RouteD daemon monitors on the Cluster Member when you configure OSPF.

The idea is that if you configure OSPF, Cluster Member monitors these interfaces and does not bring up the Cluster Member unless RouteD daemon says it is OK to bring up the Cluster Member. This is used mainly in ClusterXL High Availability Primary Up configuration to avoid premature failbacks.

Syntax

Shell	Command
Gaia Clish	`show ospf interfaces [detailed]`
Expert mode	`cphaprob routedifcs`

Example 1

```
[Expert@Member1:0]# cphaprob routedifcs

No interfaces are registered.

[Expert@Member1:0]#
```

Example 2

```
[Expert@Member1:0]# cphaprob routedifcs

Monitored interfaces registered by routed:

eth0
[Expert@Member1:0]#
```

Viewing Roles of RouteD Daemon on Cluster Members

Description

This command shows on which Cluster Member the RouteD daemon runs as a Master.

Notes:

- In ClusterXL High Availability, the RouteD daemon must run as a *Master* only on the Active Cluster Member.
- In ClusterXL Load Sharing, the RouteD daemon must run as a *Master* only on one of the Active Cluster Members and as a Non-Master on all other Cluster Members.
- In VRRP Cluster, the RouteD daemon must run as a *Master* only on the VRRP Master Cluster Member.

Syntax

Shell	Command
Gaia Clish	`show cluster role`
Expert mode	`cphaprob roles`

Example

```
[Expert@Member1:0]# cphaprob roles

ID         Role

1 (local)  Master
2          Non-Master

[Expert@Member1:0]#
```

Viewing Cluster Correction Statistics

Background

The Cluster Correction Layer (CCL) is a mechanism that deals with asymmetric connections - when a client-to-server connection passes through one Cluster Member, and the server-to-client connection arrives at another Cluster Member.

The CCL provides stickiness for connections by "correcting" the packets to the correct Cluster Member (that processed the client-to-server connection):

- In most cases, the CCL makes the correction from the CoreXL SND instances.
- In some cases (like Dynamic Routing, or VPN), the CCL makes the correction from the CoreXLFirewall instances or from SecureXL.

Note - For more information about CoreXL, see the *R81.20 Performance Tuning Administration Guide*.

Description

This command shows the statistics counters for the Cluster Correction Layer (CCL) on each Cluster Member.

The counters are reset in these cases:

- Dring each boot.
- When Check Point services are stopped and started.

Syntax

Shell	Command
Gaia Clish	N / A
Expert mode	`cphaprob [{-d | -f | -s}] corr`

Where:

Command	Description
`cphaprob corr`	Shows Cluster Correction Layer (CCL) statistics for all traffic.
`cphaprob -d corr`	Shows Cluster Correction Layer (CCL) statistics for CoreXL SND instances only.
`cphaprob -f corr`	Shows Cluster Correction Layer (CCL) statistics for CoreXL Firewall instances only.
`cphaprob -s corr`	Shows Cluster Correction Layer (CCL) statistics for SecureXL only.

Notes:

- In the output of "`cphaprob -d corr`", this row does not appear:
  `Local asymmetric conns:`
- In the output, these rows appear only on Scalable Platforms:
  - `ICMP ERROR forwarded packets:`
  - `ICMP ERROR forwarded bytes:`
  - `VS Stateless forwarded packets:`
  - `VS Stateless forwarded bytes:`
- In some cases, ClusterXL needs to send some data along with the corrected packet (for example, in VPN).
  For such packets, the output counters show "`with metadata`".

Calculating how much traffic is corrected out of total traffic on each Cluster Member

Large percentage values indicate a large number of assymetic connections that arrive at a cluster.

1. Get the output for the Cluster Correction Statistics (CCL) counters.
2. Copy the values of these CCL counters:
   - `Sent packets`
   - `Received packets`
3. Run:

   ```
   cpview
   ```

4. At the top, click **Network** > **Interfaces** >**Traffic**.
   a. In the section "`RX Traffic`", refer to the column "`packets`" > refer to the row "`TOTAL`".
   b. In the section "`TX Traffic`", refer to the column "`packets`" > refer to the row "`TOTAL`".
5. Calculate the percentage of the corrected received packets:

   ```
   (CCL "Received packets" x 100%) / (CPView "RX Traffic"
   packets)
   ```

6. Calculate the percentage of the corrected transmitted packets:

   ```
   (CCL "Sent packets" x 100%) / (CPView "TX Traffic" packets)
   ```

Example 1 - CCL statistics for all traffic

```
[Expert@Member1:0]# cphaprob corr

Cluster Correction Stats (All Traffic):
-------------------------------------------------------
Sent packets:                   0 (0 with metadata)
Sent bytes:                     0
Received packets:               0 (0 with metadata)
Received bytes:                 0
Send errors:                    0
Receive errors:                 0
Local asymmetric conns:         0
ICMP ERROR forwarded packets:   0
ICMP ERROR forwarded bytes:     0
VS Stateless forwarded packets: 0
VS Stateless forwarded bytes:   0
[Expert@Member1:0]#
```

Example 2 - CCL statistics for CoreXL SND instances only

```
[Expert@Member1:0]# cphaprob -d corr

Cluster Correction Stats (Dispatcher Corrections only):
-------------------------------------------------------
Sent packets:                   0 (0 with metadata)
Sent bytes:                     0
Received packets:               0 (0 with metadata)
Received bytes:                 0
Send errors:                    0
Receive errors:                 0
[Expert@Member1:0]#
```

Example 3 - CCL statistics for CoreXL Firewall instances only

```
[Expert@Member1:0]# cphaprob -f corr

Cluster Correction Stats (Firewall instances only):
---------------------------------------------------
Sent packets:                   0 (0 with metadata)
Sent bytes:                     0
Received packets:               0 (0 with metadata)
Received bytes:                 0
Send errors:                    0
Receive errors:                 0
Local asymmetric conns:         0
[Expert@Member1:0]#
```

Example 4 - CCL statistics for SecureXL only

```
[Expert@Member1:0]# cphaprob -s corr

Getting stats for SXL device 0, may take a few seconds...

Cluster Correction Stats (SXL Devices only):
----------------------------------------------------
Sent packets:                   0 (0 with metadata)
Sent bytes:                     0
Received packets:               0 (0 with metadata)
Received bytes:                 0
Send errors:                    0
Receive errors:                 0
Local asymmetric conns:         0
[Expert@Member1:0]#
```

Viewing the Cluster Control Protocol (CCP) Settings

Description

- You can view the Cluster Control Protocol (CCP) mode on the Cluster Members.
- You can view the Cluster Control Protocol (CCP) Encryption on the Cluster Members - enabled or disabled (and the encryption key).

See *"Configuring the Cluster Control Protocol (CCP) Settings" on page 1305*

Syntax for viewing the Cluster Control Protocol (CCP) mode

Shell	Command
Gaia Clish	`show cluster members interfaces virtual`
Expert mode	`cphaprob -a if`

Important - In R81.20, the CCP always runs in the unicast mode.

Syntax for viewing the Cluster Control Protocol (CCP) Encryption

Shell	Command
Gaia Clish	`show cluster members ccpenc`
Expert mode	`cphaprob ccp_encrypt` `cphaprob ccp_encrypt_key`

Viewing the State of the Multi-Version Cluster Mechanism

Description

This command shows the state of the Multi-Version Cluster (MVC) Mechanism - enabled (`ON`) or disabled (`OFF`).

See *"Configuring the Multi-Version Cluster Mechanism" on page 1316*.

Syntax

Shell	Command
Gaia Clish	`show cluster members mvc`
Expert mode	`cphaprob mvc`

Example

```
Member1> show cluster members mvc

ON

Member1>
```

Viewing Full Connectivity Upgrade Statistics

Description

This command shows the Full Connectivity Upgrade statistics when you upgrade between minor versions.

Syntax

Shell	Command
Gaia Clish	N / A
Expert mode	`cphaprob fcustat`

Example

```
[Expert@Member1:0]# cphaprob fcustat

During FCU.....................   no
Connection module map..........   none

Table id map (remote->local).....   none

Table handlers ..................
        8151 --> 0x0x7f97c421d860 (sip_state)
        8158 --> 0x0x7f97c43d8e30 (connections)
LD handlers.....................
        ok - 0
        failed - 0

Global handlers .................   none

[Expert@Member1:0]#
```

cpconfig

Description

This command starts the Check Point Configuration Tool.

This tool configures specific settings for the installed Check Point products.

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms (Maestro and Chassis), you must connect to the applicable Security Group.

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpconfig
```

Syntax on a Scalable Platform Security Group in Gaia gClish or the Expert mode

```
cpconfig
```

Menu Options

Note - The options shown depend on the configuration and installed products.

Menu Option	Description
Licenses and contracts	Manages Check Point licenses and contracts on this Security Gateway or Cluster Member.
SNMP Extension	Obsolete. Do **not** use this option anymore. To configure SNMP, see the *R81.20 Gaia Administration Guide* - Chapter *System Management* - Section *SNMP*.
PKCS#11 Token	Register a cryptographic token, for use by Gaia Operating System. See details of the token, and test its functionality.
Random Pool	Configures the RSA keys, to be used by Gaia Operating System.

Menu Option	Description
Secure Internal Communication	Manages SIC on the Security Gateway or Cluster Member. This change requires a restart of Check Point services on the Security Gateway or Cluster Member. For more information, see: ■ The *R81.20 Security Management Administration Guide*. ■ sk65764: How to reset SIC.
Enable cluster membership for this gateway	Enables the cluster membership on the Security Gateway. This change requires a reboot of the Security Gateway. For more information, see the: ■ *R81.20 Installation and Upgrade Guide*. ■ *R81.20 ClusterXL Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (Maestro and Chassis).
Disable cluster membership for this gateway	Disables the cluster membership on the Security Gateway. This change requires a reboot of the Security Gateway. For more information, see the: ■ *R81.20 Installation and Upgrade Guide*. ■ *R81.20 ClusterXL Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (Maestro and Chassis).
Enable Check Point Per Virtual System State	Enables Virtual System Load Sharing on the VSX Cluster Member. For more information, see the *R81.20 VSX Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (Maestro and Chassis).
Disable Check Point Per Virtual System State	Disables Virtual System Load Sharing on the VSX Cluster Member. For more information, see the *R81.20 VSX Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (Maestro and Chassis).

Menu Option	Description
Enable Check Point ClusterXL for Bridge Active/Standby	Enables Check Point ClusterXL for Bridge mode. This change requires a reboot of the Cluster Member. For more information, see the: ■ *R81.20 Installation and Upgrade Guide*. ■ *R81.20 ClusterXL Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (Maestro and Chassis).
Disable Check Point ClusterXL for Bridge Active/Standby	Disables Check Point ClusterXL for Bridge mode. This change requires a reboot of the Cluster Member. For more information, see the: ■ *R81.20 Installation and Upgrade Guide*. ■ *R81.20 ClusterXL Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (Maestro and Chassis).
Check Point CoreXL	Manages CoreXL and Firewall mode on the Security Gateway / Cluster Member / Scalable Platform Security Group. After all changes in CoreXL configuration, you must reboot the Security Gateway / Cluster Member / Security Group. For more information, see the *R81.20 Performance Tuning Administration Guide*.
Automatic start of Check Point Products	Shows and controls which of the installed Check Point products start automatically during boot.
Exit	Exits from the Check Point Configuration Tool.

Example 1 - Menu on a single Security Gateway

```
[Expert@MySingleGW:0]# cpconfig
This program will let you re-configure
your Check Point products configuration.


Configuration Options:
----------------------
(1) Licenses and contracts
(2) SNMP Extension
(3) PKCS#11 Token
(4) Random Pool
(5) Secure Internal Communication
(6) Enable cluster membership for this gateway
(7) Check Point CoreXL
(8) Automatic start of Check Point Products

(9) Exit

Enter your choice (1-9) :
```

Example 2 - Menu on a Cluster Member

```
[Expert@MyClusterMember:0]# cpconfig
This program will let you re-configure
your Check Point products configuration.


Configuration Options:
----------------------
(1) Licenses and contracts
(2) SNMP Extension
(3) PKCS#11 Token
(4) Random Pool
(5) Secure Internal Communication
(6) Disable cluster membership for this gateway
(7) Enable Check Point Per Virtual System State
(8) Enable Check Point ClusterXL for Bridge Active/Standby
(9) Check Point CoreXL
(10) Automatic start of Check Point Products

(11) Exit

Enter your choice (1-11) :
```

cphastart

Description

Starts the cluster configuration on a Cluster Member after it was stopped with the *"cphastop" on page 1379* command.

Best Practice - To start a Cluster Member, use the *"cpstart" on page 1018* command.

Note - This command does **not** initiate a Full Synchronization on the Cluster Member.

Syntax

```
cphastart
        [-h]
        [-d]
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.

`-d`	Runs the command in debug mode.
	Use only if you troubleshoot the command itself.
	Best Practice - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
	Refer to:
	■ These lines in the output file:
	`prepare_command_args: -D ... start`
	`/opt/CPsuite-R81.20/fw1/bin/cphaconf clear-secured`
	`/opt/CPsuite-R81.20/fw1/bin/cphaconf -D ...`
	`(truncated here for brevity)``... start`
	■ The `$FWDIR/log/cphastart.elg` log file.

cphastop

Description

Stops the cluster software on a Cluster Member.

Best Practice - To stop a Cluster Member, use the *"cpstop" on page 1029* command.

Notes:

- This command stops the Cluster Member from passing traffic.
- This command stops the State Synchronization between this Cluster Member and its peer Cluster Members.
- After you run this command, you can still open connections directly to this Cluster Member.
- To start the cluster software, run the *"cphastart" on page 1378* command.

Syntax

```
cphastop
```

cp_conf fullha

Important - This command does **not** apply to Scalable Platforms (Maestro and Chassis).

Description

Manages the state of the Full High Availability Cluster:

- Enables the Full High Availability Cluster
- Disables the Full High Availability Cluster
- Deletes the Full High Availability peer
- Shows the Full High Availability state

Important - To configure a Full High Availability cluster, follow the *R81.20 Installation and Upgrade Guide*.

Syntax

```
cp_conf fullha
      enable
      del_peer
      disable
      state
```

Parameters

Parameter	Description
`enable`	Enables the Full High Availability on this computer.
`del_peer`	Deletes the Full High Availability peer from the configuration.
`disable`	Disables the Full High Availability on this computer.
`state`	Shows the Full High Availability state on this computer.

Example

```
[Expert@Cluster_Member:0]# cp_conf fullha state
FullHA is currently enabled
[Expert@Cluster_Member:0]#
```

cp_conf ha

Important - This command does **not** apply to Scalable Platforms (Maestro and Chassis).

Description

Enables or disables cluster membership on this Security Gateway.

Important - This command is for Check Point use only. To configure cluster membership, you must use the *"cpconfig" on page 996* command.
For more information, see the *R81.20 ClusterXL Administration Guide*.

Syntax

```
cp_conf ha {enable | disable} [norestart]
```

Parameters

Parameter	Description
`enable`	Enables cluster membership on this Security Gateway. This command is equivalent to the option **Enable cluster membership for this gateway** in the *"cpconfig" on page 996* menu.
`disable`	Disables cluster membership on this Security Gateway. This command is equivalent to the option **Disable cluster membership for this gateway** in the *"cpconfig" on page 996* menu.
`norestart`	**Optional:** Specifies to apply the configuration change without the restart of Check Point services. The new configuration takes effect only after reboot.

Example 1 - Enable the cluster membership without restart of Check Point services

```
[Expert@MyGW:0]# cp_conf ha enable norestart

Cluster membership for this gateway was enabled successfully
Important: This change will take effect after reboot.

[Expert@MyGW:0]#
```

Example 2 - Disable the cluster membership without restart of Check Point services

```
[Expert@MyGW:0]# cp_conf ha disable norestart
cpwd_admin:
Process CPHAMCSET process has been already terminated

Cluster membership for this gateway was disabled successfully
Important: This change will take effect after reboot.

[Expert@MyGW:0]#
```

fw hastat

Description

Shows information about Check Point computers in High Availability configuration and their states.

Note - This command is outdated. On cluster members, run the Gaia Clish command "`show cluster state`", or the Expert mode command "`cphaprob state`".

Note - This command is outdated. On Management Servers, run the *"cpstat" on page 209* command.

Syntax

```
fw hastat [<Target1>] [<Target2>] ... [<TargetN>]
```

Parameters

Parameter	Description
<*Target1*> <*Target2*> ... <*TargetN*>	Specifies the Check Point computers to query. If you run this command on the Management Server, you can enter the applicable IP address, or the resolvable HostName of the managed Security Gateway or Cluster Member. If you do not specify the target, the command queries the local computer.

Example - Querying the cluster members from the Management Server

```
[Expert@MGMT:0]# fw hastat 192.168.3.52
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.52 1 active OK
[Expert@MGMT:0]#

[Expert@MGMT:0]# fw hastat 192.168.3.53
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.53 2 stand-by OK
[Expert@MGMT:0]#

[Expert@MGMT:0]# fw hastat 192.168.3.52 192.168.3.53
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.52 1 active OK
192.168.3.53 2 stand-by OK
[Expert@MGMT:0]#
```

Example - Querying the local Cluster Member

```
[Expert@Member1:0]# fw hastat
HOST NUMBER HIGH AVAILABILITY STATE MACHINE STATUS
192.168.3.52 1 active OK
[Expert@Member1:0]#
```

fwboot ha_conf

Description

Configures the cluster mechanism during boot.

Important - This command is for Check Point use only.

Notes:

- You must run this command from the Expert mode.
- Refer to these related commands:
  - *"fw defaultgen" on page 1117*
  - *"fwboot bootconf" on page 1253*
  - *"control_bootsec" on page 973*
  - *"comp_init_policy" on page 965*
- To install a cluster, see the *R81.20 Installation and Upgrade Guide*.
- To configure a cluster , see the *R81.20 Installation and Upgrade Guide* and *R81.20 ClusterXL Administration Guide*.

Syntax

```
[Expert@HostName:0]# $FWDIR/boot/fwboot ha_conf
```

The clusterXL_admin Script

Description

You can use the **clusterXL_admin** script to initiate a manual fail-over from a Cluster Member.

Location of this script on your Cluster Members is:

```
$FWDIR/bin/clusterXL_admin
```

Script Workflow

This shell script does one of these:

- Registers a Critical Device called "`admin_down`" and reports the state of that Critical Device as "`problem`".

  This gracefully changes the state of the Cluster Member to "`DOWN`".

- Reports the state of the registered Critical Device "`admin_down`" as "`ok`".

  This gracefully changes the state of the Cluster Member to "`UP`".

  Then, the script unregisters the Critical Device "`admin_down`".

For more information, see sk55081.

Example

```
#! /bin/csh -f
#
# The script will cause the machine to get into down state, thus the member will not filter
packets.
# It will supply a simple way to initiate a failover by registering a new device in problem
state when
# a failover is required and will unregister the device when wanting to return to normal
operation.
# USAGE:
# clusterXL_admin <up|down>

set PERSISTENT = ""

# checking number of arguments
if ( $#argv > 2 || $#argv < 1 ) then
        echo "clusterXL_admin : Invalid Argument Count"
        echo "Usage: clusterXL_admin <up|down> [-p]"
        exit 1
else if ( "$1" != "up" && "$1" != "down" ) then
        echo "clusterXL_admin : Invalid Argument ($1)"
        echo "Usage: clusterXL_admin <up|down> [-p]"
        exit 1
else if ( $#argv == 2 ) then
        if ( "$2" != "-p" ) then
                echo "clusterXL_admin : Invalid Argument ($2)"
                echo "Usage: clusterXL_admin <up|down> [-p]"
                exit 1
        endif
        set PERSISTENT = "-p"
endif

#checking if cpha is started
$FWDIR/bin/cphaprob stat | grep "Cluster" > /dev/null
if ($status) then
        echo "HA is not started"
        exit 1
endif

# Inform the user that the command can run with persistent mode.
if ("$PERSISTENT" != "-p") then
        echo "This command does not survive reboot. To make the change permanent, please run
'set cluster member admin down/up permanent' in clish or add '-p' at the end of the command in
expert mode"
endif

if ( $1 == "up" ) then
        echo "Setting member to normal operation ..."
        $FWDIR/bin/cphaconf set_pnote -d admin_down $PERSISTENT unregister > & /dev/null
        if ( `uname` == 'IPSO' ) then
                sleep 5
        else
                sleep 1
        endif

        set stateArr = `$FWDIR/bin/cphaprob stat | grep "local"`

        $FWDIR/bin/cphaprob stat | egrep "Sync only|Bridge Mode" > /dev/null
        #If it's third party or bridge mode, use column 4 , otherwise 5
        if ($status) then
                set state = $stateArr[5]
        else
                set state = $stateArr[4]
        endif

        echo "Member current state is $state"
        if (($state != "Active" && $state != "Standby") && ($state != "ACTIVE" && $state !=
"STANDBY" && $state != "ACTIVE(!)")) then
                echo "Operation failed: member is still down, please run 'show cluster members
pnotes problem' in clish or 'cphaprob list' in expert mode for further details"
        endif
        exit 0
endif
```

```
if ( $1 == "down" ) then
        echo "Setting member to administratively down state ..."
        $FWDIR/bin/cphaconf set_pnote -d admin_down -t 0 -s problem $PERSISTENT register > &
/dev/null
        sleep 1

        set stateArr = `$FWDIR/bin/cphaprob stat | grep "local"`

        $FWDIR/bin/cphaprob stat | egrep "Sync only|Bridge Mode" > /dev/null
        #If it's third party or bridge mode, use column 4 , otherwise 5
        if ($status) then
                set state = $stateArr[5]
        else
                set state = $stateArr[4]
        endif

        echo "Member current state is $state"
        if ( $state == "Active attention" || $state == "ACTIVE(!)" ) then
                echo "All the members within the cluster have problem/s and the local member was
chosen to become active"
        else
                if ( $state != "Down" && $state != "DOWN" ) then
                        echo "Operation failed: member is still down, please run 'show cluster
members pnotes problem' in clish or 'cphaprob list' in expert mode for further details"
                endif
        endif
        exit 0
else
        echo "clusterXL_admin : Invalid Option ($1)"
        echo "Usage: clusterXL_admin <up|down> [-p]"
        exit 1
endif
```

The clusterXL_monitor_ips Script

Description

You can use the **clusterXL_monitor_ips** script to ping a list of predefined IP addresses and change the state of the Cluster Member to `DOWN` or `UP` based on the replies to these pings. For this script to work, you must write the IP addresses in the `$FWDIR/conf/cpha_hosts` file - each IP address on a separate line. This file does not support comments or spaces.

Location of this script on your Cluster Members is:

```
$FWDIR/bin/clusterXL_monitor_ips
```

Script Workflow

1. Registers a Critical Device called "`host_monitor`" with the status "`ok`".
2. Starts to send pings to the list of predefined IP addresses in the `$FWDIR/conf/cpha_hosts` file.
3. While the script receives responses to its pings, it does not change the status of that Critical Device.
4. If the script does not receive a response to even one ping, it reports the state of that Critical Device as "`problem`".

   This gracefully changes the state of the Cluster Member to `DOWN`.

   If the script receives responses to its pings again, it changes the status of that Critical Device to "`ok`" again.

For more information, see sk35780.

Important - You must do these changes on all Cluster Members.

Example

```
#!/bin/sh
#
# The script tries to ping the hosts written in the file $FWDIR/conf/cpha_hosts. The names (must
be resolveable) ot the IPs of the hosrs must be written in seperate lines.
# the file must not contain anything else.
# We ping the given hosts every number of seconds given as parameter to the script.
# USAGE:
# cpha_monitor_ips X silent
# where X is the number of seconds between loops over the IPs.
# if silent is set to 1, no messages will appear on the console
#
# We initially register a pnote named "host_monitor" in the problem notification mechanism
# when we detect that a host is not responding we report the pnote to be in "problem" state.
# when ping succeeds again - we report the pnote is OK.

silent=0

if [ -n "$2" ]; then
        if [ $2 -le 1 ]; then
                silent=$2
        fi
fi
hostfile=$FWDIR/conf/cpha_hosts
arch=`uname -s`
if [ $arch = "Linux" ]
then
        #system is linux
        ping="ping -c 1 -w 1"
else
        ping="ping"
fi
$FWDIR/bin/cphaconf set_pnote -d host_monitor -t 0 -s ok register
TRUE=1
while [ "$TRUE" ]
do
        result=1
        for hosts in `cat $hostfile`
        do
              if [ $silent = 0 ]
                then
                        echo "pinging $hosts using command $ping $hosts"
              fi
                if [ $arch = "Linux" ]
                then
                        $ping $hosts > /dev/null 2>&1
                else
                        $ping $hosts $1 > /dev/null 2>&1
                fi
                status=$?
                if [ $status = 0 ]
                then
                     if [ $silent = 0 ]
                        then
                            echo " $hosts is alive"
                     fi
                else
                     if [ $silent = 0 ]
                        then
                            echo " $hosts is not responding "
                     fi
                        result=0
                fi
        done
        if [ $silent = 0 ]
           then
                echo "done pinging"
        fi
        if [ $result = 0 ]
        then
              if [ $silent = 0 ]
              then
                  echo " Cluster member should be down!"
```

```
                fi
                  $FWDIR/bin/cphaconf set_pnote -d host_monitor -s problem report
        else
                if [ $silent = 0 ]
                then
                          echo " Cluster member seems fine!"
                fi
                  $FWDIR/bin/cphaconf set_pnote -d host_monitor -s ok report
        fi
        if [ "$silent" = 0 ]
        then
                  echo "sleeping"
        fi
        sleep $1
        echo "sleep $1"
done
```

The clusterXL_monitor_process Script

Description

You can use the **clusterXL_monitor_process** script to monitor if the specified user space processes run, and cause cluster fail-over if these processes do not run. For this script to work, you must write the correct case-sensitive names of the monitored processes in the `$FWDIR/conf/cpha_proc_list` file - each process name on a separate line. This file does not support comments or spaces.

Location of this script on your Cluster Members is:

```
$FWDIR/bin/clusterXL_monitor_process
```

Script Workflow

1. Registers Critical Devices (with the status "`ok`") called as the names of the processes you specified in the `$FWDIR/conf/cpha_proc_list` file.
2. While the script detects that the specified process runs, it does not change the status of the corresponding Critical Device.
3. If the script detects that the specified process do not run anymore, it reports the state of the corresponding Critical Device as "`problem`".

   This gracefully changes the state of the Cluster Member to "`DOWN`".

   If the script detects that the specified process runs again, it changes the status of the corresponding Critical Device to "`ok`" again.

For more information, see sk92904.

Important - You must do these changes on all Cluster Members.

Example

```
#!/bin/sh
#
# This script monitors the existance of processes in the system. The process names should be
written
# in the $FWDIR/conf/cpha_proc_list file one every line.
#
# USAGE :
# cpha_monitor_process X silent
# where X is the number of seconds between process probings.
# if silent is set to 1, no messages will appear on the console.
#
#
# We initially register a pnote for each of the monitored processes
# (process name must be up to 15 charachters) in the problem notification mechanism.
# when we detect that a process is missing we report the pnote to be in "problem" state.
# when the process is up again - we report the pnote is OK.

if [ "$2" -le 1 ]
then
        silent=$2
else
        silent=0
fi
if [ -f $FWDIR/conf/cpha_proc_list ]
then
        procfile=$FWDIR/conf/cpha_proc_list
else
        echo "No process file in $FWDIR/conf/cpha_proc_list "
        exit 0
fi

arch=`uname -s`

for process in `cat $procfile`
do
        $FWDIR/bin/cphaconf set_pnote -d $process -t 0 -s ok -p register > /dev/null 2>&1
done

while [ 1 ]
do

        result=1

        for process in `cat $procfile`
        do
                ps -ef  | grep $process | grep -v grep > /dev/null 2>&1

                status=$?

                if [ $status = 0 ]
                then
                         if [ $silent = 0 ]
                            then
                                  echo " $process is alive"
                        fi
#                       echo "3, $FWDIR/bin/cphaconf set_pnote -d $process -s ok report"
                        $FWDIR/bin/cphaconf set_pnote -d $process -s ok report
                else
                      if [ $silent = 0 ]
                         then
                                echo " $process is down"
                         fi

                     $FWDIR/bin/cphaconf set_pnote -d $process -s problem report
                      result=0
                fi

        done

        if [ $result = 0 ]

        then
```

```
                if [ $silent = 0 ]
                    then
                  echo " One of the monitored processes is down!"
                fi
         else
                if [ $silent = 0 ]
                    then
                        echo " All monitored processes are up "
              fi

        fi
        if [ "$silent" = 0 ]
        then
                echo "sleeping"
        fi

       sleep $1

done
```

SecureXL Commands

For more information about SecureXL, see:

- *R81.20 Performance Tuning Administration Guide* - Chapter *SecureXL*.
- sk98722 - ATRG: SecureXL.

'fwaccel' and 'fwaccel6'

Description

The "`fwaccel`" commands control the acceleration for IPv4 traffic.

The "`fwaccel6`" commands control the acceleration for IPv6 traffic.

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms (Maestro and Chassis), you must connect to the applicable Security Group.

Syntax for IPv4

Syntax for IPv4 on a Security Gateway / ClusterXL - in Gaia Clish and the Expert mode

```
fwaccel help
```

```
fwaccel
      cfg <options>
      conns <options>
      dbg <options>
      dos <options>
      feature <options>
      off <options>
      on <options>
      ranges <options>
      stat <options>
      stats <options>
      synatk <options>
      tab <options>
      templates <options>
      ver
```

Syntax for IPv4 on a Scalable Platform Security Group - in Gaia gClish

```
fwaccel help
```

```
fwaccel
      cfg <options>
      conns <options>
      dbg <options>
      dos <options>
      feature <options>
      off <options>
      on <options>
      ranges <options>
      stat <options>
      stats <options>
      synatk <options>
      tab <options>
      templates <options>
      ver
```

Syntax for IPv4 on a Scalable Platform Security Group - in the Expert mode

```
g_fwaccel help
```

```
g_fwaccel
      cfg <options>
      conns <options>
      dbg <options>
      dos <options>
      feature <options>
      off <options>
      on <options>
      ranges <options>
      stat <options>
      stats <options>
      synatk <options>
      tab <options>
      templates <options>
      ver
```

Syntax for IPv6

Syntax for IPv6 on a Security Gateway / ClusterXL - in Gaia Clish and the Expert mode

```
fwaccel6 help
```

```
fwaccel6
      conns <options>
      dbg <options>
      dos <options>
      feature <options>
      off <options>
      on <options>
      ranges <options>
      stat <options>
      stats <options>
      synatk <options>
      tab <options>
      templates <options>
      ver
```

Syntax for IPv6 on a Scalable Platform Security Group - in Gaia gClish

```
fwaccel6 help
```

```
fwaccel6
      conns <options>
      dbg <options>
      dos <options>
      feature <options>
      off <options>
      on <options>
      ranges <options>
      stat <options>
      stats <options>
      synatk <options>
      tab <options>
      templates <options>
      ver
```

Syntax for IPv6 on a Scalable Platform Security Group - in the Expert mode

```
g_fwaccel6 help
```

```
g_fwaccel6
      conns <options>
      dbg <options>
      dos <options>
      feature <options>
      off <options>
      on <options>
      ranges <options>
      stat <options>
      stats <options>
      synatk <options>
      tab <options>
      templates <options>
      ver
```

Parameters and Options

Parameter and Options	Description
`help`	Shows the built-in help.
`-i <SecureXL ID>`	Specifies the SecureXL instance ID (for IPv4 only).
`cfg <options>`	Controls the SecureXL acceleration parameters (for IPv4 only). See *"fwaccel cfg" on page 1404*.
`conns <options>`	Shows all connections that pass through SecureXL. See *"fwaccel conns" on page 1408*.
`dbg <options>`	Controls the *"SecureXL Debug" on page 1577*. See *"fwaccel dbg" on page 1578*.
`dos <options>`	Controls the Rate Limiting for DoS Mitigation in SecureXL. See *"fwaccel dos" on page 1426*.
`feature <options>`	Controls the specified SecureXL features. See *"fwaccel feature" on page 1450*.
`off <options>`	Stops the acceleration on-the-fly. This does **not** survive reboot. See *"fwaccel off" on page 1454*.

Parameter and Options	Description
`on <options>`	Starts the acceleration on-the-fly, if it was previously stopped. See *"fwaccel on" on page 1459*.
`ranges <options>`	Shows the loaded ranges. See *"fwaccel ranges" on page 1464*.
`stat <options>`	Shows the SecureXL status. See *"fwaccel stat" on page 1471*.
`stats <options>`	Shows the acceleration statistics. See *"fwaccel stats" on page 1473*.
`synatk <options>`	Controls the Accelerated SYN Defender. See *"fwaccel synatk" on page 1492*.
`tab <options>`	Shows the contents of the specified SecureXL table. See *"fwaccel tab" on page 1518*.
`templates <options>`	Shows the SecureXL templates. See *"fwaccel templates" on page 1521*.
`ver`	Shows the SecureXL and FireWall version. See *"fwaccel ver" on page 1526*.

fwaccel cfg

Description

The "`fwaccel cfg`" command controls the SecureXL acceleration parameters (for IPv4 only).

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms (Maestro and Chassis), you must connect to the applicable Security Group.
- These commands do not provide output. You cannot see the currently configured values.
- Changes made with these commands do **not** survive reboot.

Syntax

Syntax on a Security Gateway / ClusterXL - in Gaia Clish and the Expert mode

```
fwaccel cfg
      -h
      -a {<Number of Interface> | <Name of Interface> | reset}
      -b {on | off}
      -c <Number>
      -d <Number>
      -e <Number>
      -i {on | off}
      -l <Number>
      -m <Seconds>
      -p {on | off}
      -r <Number>
      -v <Seconds>
      -w {on | off}
```

Syntax on a Scalable Platform Security Group - in Gaia gClish

```
fwaccel cfg
      -h
      -a {<Number of Interface> | <Name of Interface> | reset}
      -b {on | off}
      -c <Number>
      -d <Number>
      -e <Number>
      -i {on | off}
      -l <Number>
      -m <Seconds>
      -p {on | off}
      -r <Number>
      -v <Seconds>
      -w {on | off}
```

Syntax on a Scalable PlatformSecurity Group - in the Expert mode

```
g_fwaccel cfg
      -h
      -a {<Number of Interface> | <Name of Interface> | reset}
      -b {on | off}
      -c <Number>
      -d <Number>
      -e <Number>
      -i {on | off}
      -l <Number>
      -m <Seconds>
      -p {on | off}
      -r <Number>
      -v <Seconds>
      -w {on | off}
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in help.

Parameter	Description

`-a <Number of Interface>`
`-a <Name of Interface>`
`-a reset`
	■ `-a <Number of Interface>`
	Configures the SecureXL not to accelerate traffic on the interface specified by its internal number in Check Point kernel.
	■ `-a <Name of Interface>`
	Configures the SecureXL not to accelerate traffic on the interface specified by its name.
	■ `-a reset`
	Configures the SecureXL to accelerate traffic on all interfaces (resets the non-accelerated configuration).
	
	Notes:
	■ This command does not support Falcon Acceleration Cards.
	■ To see the required information about the interfaces, run these commands in the specified order:
	"fw getifs" on page 1126
	"fw ctl iflist" on page 1102
	■ To see if the "`fwaccel cfg -a ...`" command failed, run this command:
	`tail -n 10 /var/log/messages`

`-b {on | off}`	Controls the SecureXL Drop Templates match (sk66402): ■ `on` - Enables the SecureXL Drop Templates match ■ `off` - Disables the SecureXL Drop Templates match **Note** - In R81.20, SecureXL does not support this parameter yet..
`-c <Number>`	Configures the maximal number of connections, when SecureXL disables the templates.
`-d <Number>`	Configures the maximal number of delete retries.
`-e <Number>`	Configures the maximal number of general errors.
`-i {on | off}`	Configures SecureXL to ignore API version mismatch: ■ `on` - Ignore API version mismatch. ■ `off` - Do not ignore API version mismatch (this is the default).

Parameter	Description
`-l <Number>`	Configures the maximal number of entries in the SecureXL templates database. Valid values are: ■ 0 - To disable the limit (this is the default). ■ Between 10 and 524288 - To configure the limit. **Important** - If you configure a limit, you must stop and start the acceleration for this change to take effect. Run the *"fwaccel off" on page 1454* command and then the *"fwaccel on" on page 1459* command.
`-m <Seconds>`	Configures the timeout for entries in the SecureXL templates database. Valid values are: ■ 0 - To disable the timeout (this is the default). ■ Between 10 and 524288 - To configure the timeout.
`-p {on | off}`	Configures the offload of Connection Templates (if possible): ■ `on` - Enables the offload of new templates (this is the default). ■ `off` - Disables the offload of new templates.
`-r <Number>`	Configures the maximal number of retries for SecureXL API calls.
`-v <Seconds>`	Configures the interval between SecureXL statistics request. Valid values are: ■ 0 - To disable the interval. ■ 1 and greater - To configure the interval.
`-w {on | off}`	Configures the support for warnings about the IPS protection **Sequence Verifier**: ■ `on` - Enable the support for these warnings. ■ `off` - Disables the support for these warnings.

fwaccel conns

Description

The "`fwaccel conns`" and "`fwaccel6 conns`" commands show the list of the SecureXL connections on the local Security Gateway, or Cluster Member.

Warning - If the number of concurrent connections is large, when you run these commands, they can consume memory and CPU at very high level (see sk118716).

Syntax for IPv4

```
fwaccel conns
      -h
      -f <filter>
      -m <Number of Entries>
      -s
      -z
```

Syntax for IPv6

```
fwaccel6 conns
      -h
      -f <Filter>
      -m <Number of Entries>
      -s
      -z
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in help.

Parameter	Description

`-f <Filter>`	Shows the SecureXL Connections Table entries based on the specified filter flags.
	Notes:
	■ To see the available filter flags, run:
	`fwaccel conns -h`
	■ Each filter flag is one letter - capital, or small.
	■ You can specify more than one flag.
	For example:
	`fwaccel conns -f AaQq`

Parameter	Description
	Available filter flags are: ■ `A` - Shows accounted connections (for which SecureXL counted the number of packets and bytes). ■ `a` - Shows not accounted connections. ■ `C` - Shows encrypted (VPN) connections. ■ `c` - Shows clear-text (not encrypted) connections. ■ `F` - Shows connections that SecureXL forwarded to Firewall. **Note** - In R81.20, SecureXL does not support this parameter. ■ `f` - Shows cut-through connections (which SecureXL accelerated). Note - In R81.20, SecureXL does not support this parameter. ■ `H` - Shows connections offloaded to the acceleration card. **Note** - R81.20, does not support the acceleration card (Known Limitation PMTR-18774). ■ `h` - Shows connections created in the SAM card. **Note** - R81.20, does not support the SAM card (Known Limitation PMTR-18774). ■ `H` - Shows connections created in the NVIDIA ConnectX 100G QSFP28 2-port Card. ■ `L` - Shows connections, for which SecureXL created links in its connections table (Server-to-Client entries for the original Client-to-Server entry). ■ `l` - Shows connections, for which SecureXL did not create links in its connections table. ■ `N` - Shows connections that undergo NAT. **Note** - In R81.20, SecureXL does not support this parameter. ■ `n` - Shows connections that do not undergo NAT. **Note** - R81.20, SecureXL does not support this parameter. ■ `Q` - Shows connections that undergo QoS. ■ `q` - Shows connections that do not undergo QoS. ■ `S` - Shows connections that undergo PXL. ■ `s` - Shows connections that do not undergo PXL. ■ `U` - Shows unidirectional connections. ■ `u` - Shows bidirectional connections.
`-m <`*`Number of Entries`*`>`	Specifies the maximal number of connections to show. **Note** - In R81.20, SecureXL does not support this parameter.
`-s`	Shows the summary of SecureXL Connections Table (number of connections). **Warning** - Depending on the number of current connections, might consume memory at very high level.

Parameter	Description
`-z`	Shows the summary of connections that are not accelerated in hardware. **Notes:** ■ This applies only to supported Check Point appliances that support LightSpeed hardware acceleration in 10/25/40/100G QSFP28 Ports. See the *LightSpeed 10/25/40/100G QSFP28 Ports Administration Guide*. ■ To see additional information, run the CPView tool (*"cpview" on page 41*) and go to **Advanced** > **SecureXL** > **LightSpeed2Host-Reasons**.

Example - Default output from a non-VSX Gateway

```
[Expert@MyGW:0]# fwaccel conns
Source          SPort Destination     DPort PR Flags     C2S i/f S2C i/f   Inst Identity
--------------- ----- --------------- ----- -- ----------- ------- ------- ---- -------
      1.1.1.200 50586       1.1.1.100 18191  6 F..............  2/2     2/-     3        0
  192.168.0.244 35925   192.168.0.242 18192  6 F..............  1/1     -/-     1        0
   192.168.0.93   257   192.168.0.242 53932  6 F..............  1/1     1/-     0        0
  192.168.0.242    22   172.30.168.15 57914  6 F..............  1/1     -/-     2        0
  192.168.0.244 34773   192.168.0.242 18192  6 F..............  1/1     -/-     2        0
   192.168.0.88   138   192.168.0.255   138 17 F..............  1/1     -/-     0        0
      1.1.1.100 18191       1.1.1.200 55336  6 F..............  2/2     2/-     4        0
  192.168.0.242 18192   192.168.0.244 38567  6 F..............  1/1     -/-     4        0
  192.168.0.242 53932    192.168.0.93   257  6 F..............  1/1     1/-     0        0
  192.168.0.242 18192   192.168.0.244 62714  6 F..............  1/1     -/-     1        0
  192.168.0.244 33558   192.168.0.242 18192  6 F..............  1/1     -/-     5        0
      1.1.1.200 36359       1.1.1.100 18191  6 F..............  2/2     2/-     5        0
      1.1.1.200 55336       1.1.1.100 18191  6 F..............  2/2     2/-     4        0
  192.168.0.242 60756    192.168.0.93   257  6 F..............  1/1     1/-     4        0
      1.1.1.100 18191       1.1.1.200 36359  6 F..............  2/2     2/-     5        0
      1.1.1.100 18191       1.1.1.200 50586  6 F..............  2/2     2/-     3        0
  192.168.0.244 38567   192.168.0.242 18192  6 F..............  1/1     -/-     4        0
  192.168.0.242 18192   192.168.0.244 32877  6 F..............  1/1     -/-     5        0
  192.168.0.242 53806   192.168.47.45    53 17 F..............  1/1     1/-     3        0
  192.168.0.242 18192   192.168.0.244 33558  6 F..............  1/1     -/-     5        0
  172.30.168.15 57914   192.168.0.242    22  6 F..............  1/1     -/-     2        0
  192.168.0.255   138    192.168.0.88   138 17 F..............  1/1     -/-     0        0
   192.168.0.93   257   192.168.0.242 60756  6 F..............  1/1     1/-     4        0
      1.1.1.200 18192       1.1.1.100 37964  6 F..............  2/2     -/-     1        0
      1.1.1.100 37964       1.1.1.200 18192  6 F..............  2/2     -/-     1        0
  192.168.0.244 32877   192.168.0.242 18192  6 F..............  1/1     -/-     5        0
  192.168.0.242 18192   192.168.0.244 34773  6 F..............  1/1     -/-     2        0
  192.168.0.242 18192   192.168.0.244 35925  6 F..............  1/1     -/-     1        0
  192.168.47.45    53   192.168.0.242 53806 17 F..............  1/1     1/-     3        0
  192.168.0.244 62714   192.168.0.242 18192  6 F..............  1/1     -/-     1        0

Idx Interface
--- ---------
  0 lo
  1 eth0
  2 eth1

Total number of connections: 30
[Expert@MyGW:0]#
```

fwaccel dbg

Description

The *fwaccel dbg* command controls the SecureXL debug. See *"SecureXL Debug Procedure" on page 1592*.

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms (Maestro and Chassis), you must connect to the applicable Security Group.
- If you do **not** use the complete debug procedure with the "`fw ctl kdebug`" command,
  and SecureXL works in Kernel Mode (KPPAK), then Security Gateway writes the debug outputs to these files:
  - `$FWDIR/log/fwk.elg` - Processing of traffic in the Firewall module
  - `/var/log/messages` - Additional information
- If you do **not** use the complete debug procedure with the "`fw ctl kdebug`" command,
  and SecureXL works in User Mode (UPPAK), then Security Gateway writes the debug outputs to these files:
  - `$FWDIR/log/fwk.elg` - Processing of traffic in the Firewall module
  - `/var/log/usim_x86.elg` - Processing of traffic in SecureXL
  - `/var/log/messages` - Processing of traffic in the ADP module (NVIDIA ConnectX 100G Cards)

Syntax in Gaia Clish or the Expert mode on a Security Gateway / ClusterXL:

```
fwaccel dbg
      -h
      -m <Name of SecureXL Debug Module>
      all
      + <Debug Flags>
      - <Debug Flags>
      reset
      -f {"<5-Tuple Debug Filter>" | reset}
      list
      resetall
```

Syntax in Gaia gClish on a Scalable Platform Security Group:

```
fwaccel dbg
      -h
      -m <Name of SecureXL Debug Module>
      all
      + <Debug Flags>
      - <Debug Flags>
      reset
      -f {"<5-Tuple Debug Filter>" | reset}
      list
      resetall
```

Syntax in the Expert mode on a Scalable Platform Security Group:

```
g_fwaccel dbg
      -h
      -m <Name of SecureXL Debug Module>
      all
      + <Debug Flags>
      - <Debug Flags>
      reset
      -f {"<5-Tuple Debug Filter>" | reset}
      list
      resetall
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in help.
`-m <Name of SecureXL Debug Module>`	Specifies the name of the SecureXL debug module. To see the list of available debug modules, run: `fwaccel dbg`
`all`	Enables all debug flags for the specified debug module.

Parameter	Description
`+ <Debug Flags>`	Enables the specified debug flags for the specified debug module: Syntax: `+ Flag1 [Flag2 Flag3 ... FlagN]` **Note** - You must press the space bar key after the plus (+) character.
`- <Debug Flags>`	Disables all debug flags for the specified debug module. Syntax: `- Flag1 [Flag2 Flag3 ... FlagN]` **Note** - You must press the space bar key after the minus (-) character.
`reset`	Resets all debug flags for the specified debug module to their default state.
`-f "<5-Tuple Debug Filter>"`	Configures the debug filter to show only debug messages that contain the specified connection. The filter is a string of five numbers separated with commas: `"<Source IP Address>,<Source Port>,<Destination IP Address>,<Destination Port>,<Protocol Number>"` **Notes:** ■ You can configure only one debug filter at one time. ■ You can use the asterisk "*" as a wildcard for an IP Address, Port number, or Protocol number. ■ For more information, see *IANA Service Name and Port Number Registry* and *IANA Protocol Numbers*.
`-f reset`	Resets the current debug filter.
`list`	Shows all enabled debug flags in all debug modules.
`resetall`	Reset all debug flags for all debug modules to their default state.

Enabling SecureXL debug flags during boot

From R81.20, you can configure SecureXL debug to start during boot.

Important - In a Cluster, you must configure all the Cluster Members in the same way.

Procedure

Step	Instructions
1	Connect to the command line on the Security Gateway / each Cluster Member. On Scalable Platforms (Maestro and Chassis), you must connect to the applicable Security Group.
2	Log in to the Expert mode.

3	Create the require configuration files:
	■ To collect the debug for IPv4 traffic:
	`touch $FWDIR/conf/fwaccel_dbg_flags.cfg`
	■ To collect the debug for IPv6 traffic:
	`touch $FWDIR/conf/fwaccel6_dbg_flags.cfg`

4	Edit the applicable configuration file:
	■ To collect the debug for IPv4 traffic:
	`vi $FWDIR/conf/fwaccel_dbg_flags.cfg`
	■ To collect the debug for IPv6 traffic:
	`vi $FWDIR/conf/fwaccel6_dbg_flags.cfg`

5	Configure the applicable debug modules and the debug flags (see *R81.20 Security Gateway Guide*).
	Write each debug module and its flags on a separate line:
	`<Name of Debug Module #1> <Flag1> <Flag2> <Flag3> ... <FlagN>`
	`<Name of Debug Module #2> <Flag1> <Flag2> <Flag3> ... <FlagN>`
	Example:
	`default conn nat`
	`pkt drop nat`

6	Save the changes in the file and exit the editor.

Step	Instructions

7	On the Scalable Platform Security Group, you must copy the updated file to all Security Group Members:
	`asg_cp2blades $FWDIR/conf/fwaccel_dbg_flags.cfg`
	`asg_cp2blades $FWDIR/conf/fwaccel6_dbg_flags.cfg`

8	Reboot the Security Gateway / each Cluster Member / all Security Group Members.
9	Wait for the issue to occur.
10	Connect to the command line on the Security Gateway / each Cluster Member. On Scalable Platforms (Maestro and Chassis), you must connect to the applicable Security Group.
11	Log in to the Expert mode.

12	Reset all the SecureXL debug flags in all SecureXL debug modules:
	■ On the Security Gateway / each Cluster Member:
	`fwaccel dbg resetall`
	■ On the Scalable Platform Security Group:
	`g_fwaccel dbg resetall`

13	Remove all entries from the configuration files:
	■ On the Security Gateway / each Cluster Member:
	`echo '' > $FWDIR/conf/fwaccel_dbg_flags.cfg`
	`echo '' > $FWDIR/conf/fwaccel6_dbg_flags.cfg`
	■ On the Scalable Platform Security Group:
	`echo '' > $FWDIR/conf/fwaccel_dbg_flags.cfg`
	`asg_cp2blades $FWDIR/conf/fwaccel_dbg_flags.cfg`
	`echo '' > $FWDIR/conf/fwaccel6_dbg_flags.cfg`
	`asg_cp2blades $FWDIR/conf/fwaccel6_dbg_flags.cfg`

Step	Instructions
14	Collect the output files. If SecureXL works in Kernel Mode (KPPAK): ■ `$FWDIR/log/fwk.elg` ■ `/var/log/messages` If SecureXL works in User Mode (UPPAK): ■ `$FWDIR/log/fwk.elg` ■ `/var/log/usim_x86.elg` ■ `/var/log/messages`

Examples

Example 1 - Default output

```
[Expert@MyGW:0]# fwaccel dbg
Usage: fwaccel dbg [-m <...>] [resetall | reset | list | all | +/- <flags>]
   -m <module>             - module of debugging
   -h                      - this help message
   resetall                - reset all debug flags for all modules
   reset                   - reset all debug flags for module
   all                     - set all debug flags for module
   list                    - list all debug flags for all modules
   -f reset | "<5-tuple>"  - filter debug messages
   + <flags>               - set the given debug flags
   - <flags>               - unset the given debug flags

Debug flags can be enabled at boot by adding them to
$FWDIR/conf/fwaccel_dbg_flags.cfg and $FWDIR/conf/fwaccel6_dbg_flags.cfg.
The file format is one line per module.

For example, to enable "tcp_state" and "routing" for the "pkt" module:
    echo "pkt tcp_state routing" >> $FWDIR/conf/fwaccel_dbg_flags.cfg

List of available modules and flags:

Module: default (default)
init drv tag lock cpdrv routing kdrv tcp_sv svm iter conn htab del update acct conf stat
queue ioctl corr util rngs relations ant conn_app rngs_print infra_ids offload nat

Module: db
get save del tmpl tmo init ant profile nmr nmt warning

Module: api
init add update del acct conf stat vpn notif tmpl sv pxl qos gtp infra tmpl_info upd_conf
upd_if_inf add_sa del_sa del_all_sas misc get_features get_tab get_stat reset_stat tag long_
ver del_all_tmpl get_state upd_link_sel

Module: pkt
f2f frag spoof acct notif tcp_state tcp_state_pkt sv cpls routing drop pxl qos user deliver
vlan pkt nat wrp corr caf bhm geneve sctp

Module: infras
reorder pm

Module: tmpl
dtmpl_get dtmpl_notif tmpl

Module: vpn
vpnpkt linksel routing vpn ls

Module: nac
db db_get pkt pkt_ex signature offload idnt ioctl nac

Module: cpaq
init client server exp cbuf opreg transport transport_utils broadcast

Module: synatk
init conf conn log pkt proxy state msg

Module: adp
rt nh eth heth wrp inf mbs bpl bplinf mbeinf if drop bond xmode ipsctl ac_print cpfifo qconf
qcomm filter packet mcast hw_offload hw_expn rte_api

Module: dos
fw1-cfg fw1-pkt sim-cfg sim-pkt detailed-pkt detailed-cfg drop cache

Module: gtp
pkt policy tables api drop notif general
```

```
Module: usdisp
error conn packet api msg state packet_err counter event quota ioctl lock clb uid queue
fwstats cachetab vpn temp_conns prio route dumbo

Module: dpdk_lib


Module: dpdk_pmd


Module: dpdk_other


[Expert@MyGW:0]#
```

Example 2 - Enabling and disabling of debug flags

```
[Expert@MyGW:0]# fwaccel dbg -m default + conn
Debug flags updated.
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dbg list

[Expert@MyGW:0]# fwaccel dbg list
 Module: default (400)
conn

Module: db (0)


Module: api (0)


Module: pkt (0)


Module: infras (0)


Module: tmpl (0)


Module: vpn (0)


Module: nac (0)


Module: cpaq (0)


Module: synatk (0)


Module: adp (0)


Module: dos (0)


Module: gtp (0)


Module: usdisp (0)


Module: dpdk_lib (0)


Module: dpdk_pmd (0)


Module: dpdk_other (0)


Debug filter not set.
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dbg -m default - conn
Debug flags updated.
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel dbg list

Module: default (0)


Module: db (0)


Module: api (0)


Module: pkt (0)


Module: infras (0)


Module: tmpl (0)


Module: vpn (0)


Module: nac (0)


Module: cpaq (0)


Module: synatk (0)


Module: adp (0)


Module: dos (0)


Module: gtp (0)


Module: usdisp (0)


Module: dpdk_lib (0)


Module: dpdk_pmd (0)


Module: dpdk_other (0)


Debug filter not set.
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dbg -m default reset
Debug flags updated.
[Expert@MyGW:0]#
```

Example 3 - Resetting all debug flags in all debug modules

```
[Expert@MyGW:0]# fwaccel dbg resetall
Debug state was reset to default.
[Expert@MyGW:0]#
```

Example 4 - Configuring debug filter for an SSH connection from 192.168.20.30 to 172.16.40.50

```
[Expert@MyGW:0]# fwaccel dbg -f 192.168.20.30,*,172.16.40.50,22,6
Debug filter was set.
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dbg list

... ...

Debug filter: "<*,*,*,*,*>"
[Expert@MyGW:0]#
```

fwaccel dos

Description

The *fwaccel dos* and *fwaccel6 dos* commands control the Rate Limiting for DoS mitigation techniques in SecureXL on the local Security Gateway, or Cluster Member.

Important:

- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Syntax for IPv4

```
fwaccel dos
      allow <options>
      config <options>
      deny <options>
      pbox <options>
      rate <options>
      stats <options>
```

Syntax for IPv6

```
fwaccel6 dos
      allow <options>
      config <options>
      deny <options>
      pbox <options>
      rate <options>
      stats <options>
```

Parameters

Parameter	Description
`allow <options>`	Configures the allow-list for source IP addresses in the SecureXL Penalty Box. See *"fwaccel dos whitelist" on page 1428*.

Parameter	Description
`config <options>`	Controls the DoS mitigation configuration in SecureXL. See *"fwaccel dos config" on page 1432*.
`deny <options>`	Controls the IP deny-list in SecureXL. See *"fwaccel dos deny" on page 1438*.
`pbox <options>`	Controls the Penalty Box whitelist in SecureXL. See *"fwaccel dos pbox" on page 1441*.
`rate <options>`	Shows and installs the Rate Limiting policy in SecureXL. See *"fwaccel dos rate" on page 1446*.
`stats <options>`	Shows and clears the DoS real-time statistics in SecureXL. See *"fwaccel dos stats" on page 1448*.

fwaccel dos whitelist

Description

The *fwaccel dos allow* command configures the allow-list for source IP addresses in the SecureXL Penalty Box.

This allow-list overrides which packet the SecureXL Penalty Box drops.

Important:

- This command supports only IPv4.
- In VSX mode, you must go to the context of an applicable Virtual System.In Gaia Clish, run: `set virtual-system <VSID>`In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.
- This allow-list overrides entries in the blacklist.
  Before you use a 3rd-party or automatic blacklists, add trusted networks and hosts to the allow-list to avoid outages.
- This allow-list unblocks IP Options and IP fragments from trusted sources when you explicitly configure one these SecureXL features:
  - `--enable-drop-opts`
  - `--enable-drop-frags`

  See the *"fwaccel dos config" on page 1432* command.

Notes:

- To allow-list the Rate Limiting policy, refer to the bypass action of the `fw samp` command.
  For example, `fw samp -a b ...`
  For more information about the `fw sam_policy` command, see the *R81.20 Performance Tuning Administration Guide* - Chapter *SecureXL Commands and Debug* - Section *fw sam_policy*.
- This command is similar to the "`fwaccel dos pbox allow`" command (see *"fwaccel dos pbox" on page 1441*).
- Also, see the *"fwaccel synatk allow" on page 1503* command.

Syntax for IPv4

```
fwaccel dos allow
      -a <IPv4 Address>[/<Subnet Prefix>]
      -d <IPv4 Address>[/<Subnet Prefix>]
      -F
      -l /<Path>/<Name of File>
      -L
      -s
```

Parameters

Parameter	Description
No Parameters	Shows the applicable built-in usage.

`-a <IPv4 Address> [/<Subnet Prefix>]`	Adds the specified IP address to the Penalty Box allow-list.
	■ `<IPv4 Address>`
	Can be an IPv4 address of a network or a host.
	■ `<Subnet Prefix>`
	Must specify the length of the subnet mask in the format `/<bits>`.
	Optional for a host IPv4 address.
	Mandatory for a network IPv4 address.
	Range - from /1 to /32.
	Important - If you do not specify the subnet prefix explicitly, this command uses the subnet prefix /32.
	Examples:
	■ For a host:
	`192.168.20.30`
	`192.168.20.30/32`
	■ For a network:
	`192.168.20.0/24`

`-d <IPv4 Address> [/<Subnet Prefix>]`	Removes the specified IPv4 address from the Penalty Box allow-list. ■ `<IPv4 Address>` Can be an IPv4 address of a network or a host. ■ `<Subnet Prefix>` Optional. Must specify the length of the subnet mask in the format `/<bits>`. Optional for a host IPv4 address. Mandatory for a network IPv4 address. Range - from /1 to /32. **Important** - If you do not specify the subnet prefix explicitly, this command uses the subnet prefix /32.
`-F`	Removes (flushes) all entries from the Penalty Box allow-list.

Parameter	Description
`-l /<Path>/<Name of File>`	Loads the Penalty Box allow-list entries from the specified plain-text file. **Note** - To replace the current allow-list with the contents of a new file, use both the "`-F`" and "`-l`" parameters on the same command line. **Important:** ■ You must manually create and configure this file with the `touch` or `vi` command. ■ You must assign at least the read permission to this file with the `chmod a+r` command. ■ Each entry in this file must be on a separate line. ■ Each entry in this file must be in this format: `<IPv4 Address>[/<Subnet Prefix>]` ■ SecureXL ignores empty lines and lines that start with the # character in this file.
`-L`	Loads the DoS allow-list entries from the plain-text file with a predefined name: `$FWDIR/conf/dos-allow-list-v4.conf` Security Gateway automatically runs this command "`fwaccel dos allow -L`" during each boot. **Note** - To replace the current allow-list with the contents of a new file, use both the "`-F`" and "`-L`" parameters on the same command line. **Important:** ■ This file does not exist by default. ■ You must manually create and configure this file with the `touch` or `vi` command. ■ You must assign at least the read permission to this file with the `chmod a+r` command. ■ Each entry in this file must be on a separate line. ■ Each entry in this file must be in this format: `<IPv4 Address>[/<Subnet Prefix>]` ■ SecureXL ignores empty lines and lines that start with the # character in this file.
`-s`	Shows the current Penalty Box allow-list entries.

Example 1 - Adding a host IP address without optional subnet prefix

```
[Expert@MyGW:0]# fwaccel dos allow -a 192.168.20.40
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos allow -s
192.168.20.40/32
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos allow -F
[Expert@MyGW:0]# fwaccel dos allow -s
[Expert@MyGW:0]#
```

Example 2 - Adding a host IP address with optional subnet prefix

```
[Expert@MyGW:0]# fwaccel dos allow -a 192.168.20.40/32
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos allow -s
192.168.20.40/32
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos allow -F
[Expert@MyGW:0]# fwaccel dos allow -s
[Expert@MyGW:0]#
```

Example 3 - Adding a network IP address with mandatory subnet prefix

```
[Expert@MyGW:0]# fwaccel dos allow -a 192.168.20.0/24
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos allow -s
192.168.20.0/24
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos allow -F
[Expert@MyGW:0]# fwaccel dos allow -s
[Expert@MyGW:0]#
```

Example 4 - Deleting an entry

```
[Expert@MyGW:0]# fwaccel dos allow -a 192.168.20.40/32
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos allow -a 192.168.20.70/32
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos allow -s
192.168.20.40/32
192.168.20.70/32
[Expert@MyGW:0]# fwaccel dos allow -d 192.168.20.70/32
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos allow -s
192.168.20.40/32
[Expert@MyGW:0]#
```

fwaccel dos config

Description

The *fwaccel dos config* and *fwaccel6 dos config* commands control the global configuration parameters of the Rate Limiting for DoS mitigation in SecureXL.

These global parameters apply to all configured Rate Limiting rules.

Important:

- In VSX mode, you must go to the context of an applicable Virtual System.In Gaia Clish, run: `set virtual-system <VSID>`In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Syntax for IPv4

```
fwaccel dos config
      get
      set
            {--disable-blacklists | --enable-blacklists}
            {--disable-drop-frags | --enable-drop-frags}
            {--disable-drop-opts | --enable-drop-opts}
            {--disable-internal | --enable-internal}
            {--disable-log-drops | --enable-log-drops}
            {--disable-log-pbox | --enable-log-pbox}
            {--disable-monitor | --enable-monitor}
            {--disable-pbox | --enable-pbox}
            {--disable-rate-limit | --enable-rate-limit}
            {--disable-rule-cache | --enable-rule-cache}
            {-n <NOTIF_RATE> | --notif-rate <NOTIF_RATE>}
            {-p <PBOX_RATE> | --pbox-rate <PBOX_RATE>}
            {-t <PBOX_TMO> | --pbox-tmo <PBOX_TMO>}
```

Syntax for IPv6

```
fwaccel6 dos config
      get
      set
            {--disable-blacklists | --enable-blacklists}
            {--disable-drop-frags | --enable-drop-frags}
            {--disable-drop-opts | --enable-drop-opts}
            {--disable-internal | --enable-internal}
            {--disable-log-drops | --enable-log-drops}
            {--disable-log-pbox | --enable-log-pbox}
            {--disable-monitor | --enable-monitor}
            {--disable-pbox | --enable-pbox}
            {--disable-rate-limit | --enable-rate-limit}
            {--disable-rule-cache | --enable-rule-cache}
            {-n <NOTIF_RATE> | --notif-rate <NOTIF_RATE>}
            {-p <PBOX_RATE> | --pbox-rate <PBOX_RATE>}
            {-t <PBOX_TMO> | --pbox-tmo <PBOX_TMO>}
```

Parameters and Options

Parameter or Option	Description
No Parameters	Shows the applicable built-in usage.
`get`	Shows the configuration parameters.
`set <options>`	Configuration the parameters.
`--disable-blacklists`	Disables the IP blacklists. This is the default configuration.
`--disable-drop-frags`	Disables the drops of all fragmented packets. This is the default configuration. **Important** - This option applies to only VSX, and only for traffic that arrives at a Virtual System through a Virtual Switch (packets received through a Warp interface). From R80.20, IP Fragment reassembly occurs in SecureXL before the Warp-jump from a Virtual Switch to a Virtual System. To block IP fragments, the Virtual Switch must be configured with this option. Otherwise, this has no effect, because the IP fragments would already be reassembled when they arrive at the Virtual System's Warp interface.

Parameter or Option	Description
`--disable-drop-opts`	Disables the drops of all packets with IP options. This is the default configuration.
`--disable-internal`	Disables the enforcement on internal interfaces. This is the default configuration.
`--disable-log-drops`	Disables the notifications when the DoS module drops a packet due to rate limiting policy.
`--disable-log-pbox`	Disables the notifications when administrator adds an IP address to the penalty box.
`--disable-monitor`	Disables the monitor-only mode. This is the default configuration. This command affects all Rate Limiting features. Also, see the *"fwaccel dos deny" on page 1438* command.
`--disable-pbox`	Disables the IP penalty box. This is the default configuration. Also, see the *"fwaccel dos pbox" on page 1441* command.
`--disable-rate-limit`	Disables the enforcement of the rate limiting policy. This is the default configuration.
`--disable-rule-cache`	Disables the caching of Rate Limiting rule matches. This optimizes the performance for large numbers of connections-per-second.
`--enable-blacklists`	Enables IP blacklists. Also, see the *"fwaccel dos deny" on page 1438* command.
`--enable-drop-frags`	Enables the drops of all fragmented packets.
`--enable-drop-opts`	Enables the drops of all packets with IP options.
`--enable-internal`	Enables the enforcement on internal interfaces.
`--enable-log-drops`	Enables the notifications when the DoS module drops a packet due to rate limiting policy. This is the default configuration.

Parameter or Option	Description
`--enable-log-pbox`	Enables the notifications when administrator adds an IP address to the penalty box. This is the default configuration.
`--enable-monitor`	Enables the monitor-only mode (accepts all packets that otherwise are dropped). This command affects all Rate Limiting features. Also, see the *"fwaccel dos deny" on page 1438* command.
`--enable-pbox`	Enables the IP penalty box. Also, see the *"fwaccel dos pbox" on page 1441* command.
`--enable-rate-limit`	Enables the enforcement of the rate limiting policy. **Important** - After you run this command, you must install the Access Control policy.
`--enable-rule-cache`	Enables the caching of Rate Limiting rule matches. This optimizes the performance for large numbers of packets-per-connection. This is the default configuration.
`-n <NOTIF_RATE>` `--notif-rate <NOTIF_RATE>`	Configures the maximal number of drop notifications per second for each SecureXL device. Range: 0 - (2^{32}-1) Default: 100
`-p <PBOX_RATE>` `--pbox-rate <PBOX_RATE>`	Configures the minimal number of reported dropped packets before SecureXL adds a source IPv4 address to the penalty box. Range: 0 - (2^{32}-1) Default: 500
`-t <PBOX_TMO>` `--pbox-tmo <PBOX_TMO>`	Configures the number of seconds until SecureXL removes an IP is from the penalty box. Range: 0 - (2^{32}-1) Default: 180

Example 1 - Get the current DoS configuration on a non-VSX Gateway

```
[Expert@MyGW:0]# fwaccel dos config get
   rate limit: disabled (without policy)
         pbox: disabled
   blacklists: disabled
log blacklist: disabled
   drop frags: disabled
    drop opts: disabled
     internal: disabled
      monitor: disabled
    log drops: disabled
     log pbox: disabled
   notif rate: 100 notifications/second
    pbox rate: 500 packets/second
     pbox tmo: 180 seconds
[Expert@MyGW:0]#
```

Example 2 - Enabling the Penalty Box on a non-VSX Gateway

```
[Expert@MyGW:0]# fwaccel dos config set --enable-pbox
OK
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos config get
   rate limit: disabled (without policy)
         pbox: enabled
   blacklists: disabled
   drop frags: disabled
    drop opts: disabled
     internal: disabled
      monitor: disabled
    log drops: enabled
     log pbox: enabled
   notif rate: 100 notifications/second
    pbox rate: 500 packets/second
     pbox tmo: 180 seconds
[Expert@MyGW:0]#
```

Making the configuration persistent

The settings defined with the "`fwaccel dos config set`" and the "`fwaccel6 dos config set`" commands return to their default values during each reboot. To make these settings persistent, add the applicable commands to these configuration files:

File	Description

`$FWDIR/conf/fwaccel_dos_rate_on_install`	This shell script for IPv4 must contain only the "`fwaccel dos config set`" commands:
	`#!/bin/bash`
	`fwaccel dos config set <options>`

`$FWDIR/conf/fwaccel6_dos_rate_on_install`	This shell script for IPv6 must contain only the "`fwaccel6 dos config set`" commands:
	`#!/bin/bash`
	`fwaccel6 dos config set <options>`

Important - Do not include the *"fw sam_policy" on page 1527* commands in these configuration files. The configured Rate Limiting policy survives reboot. If you add the "`fw sam_policy`" commands, the rate policy installer runs in an infinite loop.

Notes:

- To create or edit these files, log in to the Expert mode.
- On VSX Gateway, before you create these files, go to the context of an applicable Virtual System:
  `vsenv <VSID>`
- If these files do not already exist, create them with one of these commands:
  - `touch $FWDIR/conf/<Name of File>`
  - `vi $FWDIR/conf/<Name of File>`
- These files must start with the "`#!/bin/bash`" line.
- These files must end with a new empty line.
- After you edit these files, you must assign the execute permission to them:
  `chmod +x $FWDIR/conf/<Name of File>`

Example of a `$FWDIR/conf/fwaccel_dos_rate_on_install` file:

```
#!/bin/bash
fwaccel dos config set --enable-internal
fwaccel dos config set --enable-pbox
```

fwaccel dos deny

Description

The *fwaccel dos deny* and *fwaccel6 dos deny* commands control the IP deny-list in SecureXL.

The deny-list blocks all traffic to and from the specified IP addresses.

The deny-list drops occur in SecureXL, which is more efficient than an Access Control Policy to drop the packets.

Important:

- In VSX mode, you must go to the context of an applicable Virtual System.In Gaia Clish, run: `set virtual-system <VSID>`In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.
- To enforce the IP deny-list in SecureXL, you must first enable the IP deny-lists. See these commands:
  - *"fwaccel dos config" on page 1432*
  - *"fw sam_policy" on page 1527* (configures more granular rules)

Syntax for IPv4

```
fwaccel dos deny
      -a <IPv4 Address>
      -d <IPv4 Address>
      -F
      -M {on | off}
      -m
      -N "<Name of IP Deny-list>"
      -n
      -s
```

Syntax for IPv6

```
fwaccel6 dos deny
      -a <IPv6 Address>
      -d <IPv6 Address>
      -F
      -M {on | off}
      -m
      -N "<Name of IP Deny-list>"
      -n
      -s
```

Parameters

Parameter	Description
No Parameters	Shows the applicable built-in usage.
`-a <IP Address>`	Adds the specified IP address to the deny-list. To add more than one IP address, run this command for each applicable IP address.
`-d <IP Address>`	Removes the specified IP addresses from the deny-list. To remove more than one IP address, run this command for each applicable IP address.
`-F`	Removes (flushes) all IP addresses from the IP deny-list.
`-M {on | off}`	Enables (`on`) or disables (`off`) the monitor-only mode for the IP deny-list. By default, the monitor-only mode is disabled. In the monitor-only mode you can test the IP deny-list without blocking the traffic. This command affects only the IP deny-list (does not affect the `fw samp` rules, etc.).
`-m`	Shows the current status of the monitor-only mode for the IP deny-list (enabled or disabled).
`-N "<Name of IP Deny-list>"`	Configures the name for the IP deny-list. This name appears in the Security Gateway logs. **Notes:** ■ Maximal length is 79 characters. ■ You must only use ASCII characters.
`-n`	Shows the configured name for the IP deny-list.
`-s`	Shows the configured deny-list.

Example from a non-VSX Gateway

```
[Expert@MyGW:0]# fwaccel dos deny -s
The deny list is empty
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos deny -a 1.1.1.1
Adding 1.1.1.1
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos deny -s
1.1.1.1
[Expert@MyGW:0]# fwaccel dos deny -a 2.2.2.2
Adding 2.2.2.2
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos deny -s
2.2.2.2
1.1.1.1
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos deny -d 2.2.2.2
Deleting 2.2.2.2
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos deny -s
1.1.1.1
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos deny -F
All deny list entries deleted
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos deny -s
The deny list is empty
[Expert@MyGW:0]#
```

fwaccel dos pbox

Description

The *fwaccel dos pbox* command controls the Penalty Box allow-list in SecureXL.

The SecureXL Penalty Box is a mechanism that performs an early drop of packets that arrive from suspected sources. The purpose of this feature is to allow the Security Gateway to cope better under high traffic load, possibly caused by a DoS/DDoS attack.

The SecureXL Penalty Box detects clients that send packets, which the Access Control Policy drops, and clients that violate the IPS protections. If the SecureXL Penalty Box detects a specific client frequently, it puts that client in a penalty box. From that point, SecureXL drops all packets that arrive from the blocked source IP address.

The Penalty Box allow-list in SecureXL configures the source IP addresses, which the SecureXL Penalty Box never blocks.

Important:

- This command supports only IPv4.
- In VSX mode, you must go to the context of an applicable Virtual System.In Gaia Clish, run: `set virtual-system <VSID>`In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.
- To enforce the Penalty Box in SecureXL, you must first enable the Penalty Box. See these commands:
  - *"fwaccel dos config" on page 1432*
  - *"fwaccel dos whitelist" on page 1428*
  - *"fwaccel synatk allow" on page 1503*
- In a Scalable Platform, the same SecureXL command must run on all Security Group Members.
  Therefore, you must run the SecureXL commands in either Gaia gClish, or Expert mode.
  - In Gaia gClish, run the "`fwaccel ...`" and "`fwaccel6 ...`" commands.
  - In the Expert mode, run the "`g_fwaccel ...`" and "`g_fwaccel6 ...`" commands.
- In a Scalable Platform, when you add a new Security Group Member to a Security Group, the new Security Group Member pulls the "`$FWDIR/conf/pbox-whitelist-v4.conf`" configuration file.

Syntax for IPv4

```
fwaccel dos pbox
      allow
            -a <IPv4 Address>[/<Subnet Prefix>]
            -d <IPv4 Address>[/<Subnet Prefix>]
            -F
            -l /<Path>/<Name of File>
            -L
            -s
      flush
```

Parameters

Parameter	Description
No Parameters	Shows the applicable built-in usage.
`allow <options>`	Configures the allow-list for source IP addresses in the SecureXL Penalty Box. **Important** - This allow-list overrides which packet the SecureXL Penalty Box drops. Before you use a 3rd-party or automatic blacklists, add trusted networks and hosts to the allow-list to avoid outages. **Note** - This command is similar to the *"fwaccel dos whitelist" on page 1428* command.

Parameter	Description

`allow -a <IPv4 Address>[/<Subnet Prefix>]`	Adds the specified IP address to the Penalty Box allow-list.
	■ *<IPv4 Address>*
	Can be an IP address of a network or a host.
	■ *<Subnet Prefix>*
	Must specify the length of the subnet mask in the format `/<bits>`.
	Optional for a host IP address.
	Mandatory for a network IP address.
	Range - from /1 to /32.
	Important - If you do not specify the subnet prefix explicitly, this command uses the subnet prefix /32.
	Examples:
	■ For a host:
	`192.168.20.30`
	`192.168.20.30/32`
	■ For a network:
	`192.168.20.0/24`

`allow -d <IPv4 Address>[/<Subnet Prefix>]`	Removes the specified IP address from the Penalty Box allow-list. ■ *<IPv4 Address>* Can be an IP address of a network or a host. ■ *<Subnet Prefix>* Optional. Must specify the length of the subnet mask in the format `/<bits>`. Optional for a host IP address. Mandatory for a network IP address. Range - from /1 to /32. **Important** - If you do not specify the subnet prefix explicitly, this command uses the subnet prefix /32.
`allow -F`	Removes (flushes) all entries from the Penalty Box allow-list.

Parameter	Description
`allow -l /<Path>/<Name of File>`	Loads the Penalty Box allow-list entries from the specified plain-text file. **Important:** ■ You must manually create and configure this file with the `touch` or `vi` command. ■ You must assign at least the read permission to this file with the `chmod a+r` command. ■ Each entry in this file must be on a separate line. ■ Each entry in this file must be in this format: *<IPv4 Address>*[/*<Subnet Prefix>*] ■ SecureXL ignores empty lines and lines that start with the # character in this file.
`allow -L`	Loads the Penalty Box allow-list entries from the plain-text file with a predefined name: `$FWDIR/conf/pbox-allow-list-v4.conf` Security Gateway automatically runs this command "`fwaccel dos pbox allow -L`" during each boot. **Important:** ■ This file does not exist by default. ■ You must manually create and configure this file with the `touch` or `vi` command. ■ You must assign at least the read permission to this file with the `chmod a+r` command. ■ Each entry in this file must be on a separate line. ■ Each entry in this file must be in this format: *<IPv4 Address>*[/*<Subnet Prefix>*] ■ SecureXL ignores empty lines and lines that start with the # character in this file.
`allow -s`	Shows the current Penalty Box allow-list entries.
`flush`	Removes (flushes) all source IP addresses from the Penalty Box.

Example 1 - Adding a host IP address without optional subnet prefix

```
[Expert@MyGW:0]# fwaccel dos pbox allow -a 192.168.20.40
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos pbox allow -s
192.168.20.40/32
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos pbox allow -F
[Expert@MyGW:0]# fwaccel dos pbox allow -s
[Expert@MyGW:0]#
```

Example 2 - Adding a host IP address with optional subnet prefix

```
[Expert@MyGW:0]# fwaccel dos pbox allow -a 192.168.20.40/32
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos pbox allow -s
192.168.20.40/32
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos pbox allow -F
[Expert@MyGW:0]# fwaccel dos pbox allow -s
[Expert@MyGW:0]#
```

Example 3 - Adding a network IP address with mandatory subnet prefix

```
[Expert@MyGW:0]# fwaccel dos pbox allow -a 192.168.20.0/24
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos pbox allow -s
192.168.20.0/24
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos pbox allow -F
[Expert@MyGW:0]# fwaccel dos pbox allow -s
[Expert@MyGW:0]#
```

Example 4 - Deleting an entry

```
[Expert@MyGW:0]# fwaccel dos pbox allow -a 192.168.20.40/32
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos pbox allow -a 192.168.20.70/32
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos pbox allow -s
192.168.20.40/32
192.168.20.70/32
[Expert@MyGW:0]# fwaccel dos pbox allow -d 192.168.20.70/32
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dos pbox allow -s
192.168.20.40/32
[Expert@MyGW:0]#
```

fwaccel dos rate

Description

The *fwaccel dos rate* and *fwaccel6 dos rate* commands show and install the Rate Limiting policy in SecureXL.

Important:

- In VSX mode, you must go to the context of an applicable Virtual System.In Gaia Clish, run: `set virtual-system <VSID>`In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Syntax for IPv4

```
fwaccel dos rate
      get '<Rule UID>'
      install
```

Syntax for IPv6

```
fwaccel6 dos rate
      get '<Rule UID>'
      install
```

Parameters

Parameter	Description
No Parameters	Shows the applicable built-in usage.
`get '<Rule UID>'`	Shows information about the rule specified by its Rule UID or its zero-based rule index. The quote marks and angle brackets (`'<...>'`) are mandatory.
`install`	Installs a new rate limiting policy. **Important** - This command requires input from the *stdin*. To use this command, run: `fw sam_policy get -l -k req_type -t in -v quota | fwaccel dos rate install` For more information about the "`fw sam_policy`" command, see *"fw sam_policy" on page 1527*.

Notes

- If you install a new rate limiting policy with more than one rule, it automatically enables the rate limiting feature.

  To disable the rate limiting feature manually, run this command (see *"fwaccel dos config" on page 1432*):

  ```
  fwaccel dos config set --disable-rate-limit
  ```

- To delete the current rate limiting policy, install a new policy with zero rules.

fwaccel dos stats

Description

The *fwaccel dos stats* and *fwaccel6 dos stats* commands show and clear the DoS real-time statistics in SecureXL.

Important:

- In VSX mode, you must go to the context of an applicable Virtual System.In Gaia Clish, run: `set virtual-system <VSID>`In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Syntax for IPv4

```
fwaccel stats
      clear
      get
```

Syntax for IPv6

```
fwaccel6 dos stats
      clear
      get
```

Parameters

Parameter	Description
No Parameters	Shows the applicable built-in usage.
`clear`	Clears the real-time statistics counters.
`get`	Shows the real-time statistics counters.

Example - Get the current DoS statistics

```
[Expert@MyGW:0]# fwaccel dos stats get

Firewall Instances in Aggregate:
    Memory Usage:                       0
    Total Active Connections:  (FW connection limiting inactive)
    New Connections/Second:    (FW connection limiting inactive)
    Number of Elements in Tables:
        Penalty Box Violating IPs:                      0
        Rate Limit Source Only Tracks:                  0
        Rate Limit Source and Service Tracks:           0
        Rate Limit Dest Only Tracks:                    0
        Rate Limit Dest and Service Tracks:             0

SecureXL:
    Memory Usage:                       0
    Packets/Second:                     (rate limiting inactive)
    Bytes/Second:                       (rate limiting inactive)
    Reasons Packets Dropped:
        IP Fragment:          0
        IP Option:            0
        Penalty Box:          0
        Deny List:            0
        Rate Limit:           0
    Number of Elements in Tables:
        Penalty Box:                                    0
        Non-Empty Deny Lists:                           0
        Deny List IPs:                                  0
        Rate Limit Matches:                             0
        Rate Limit Source Only Tracks:                  0
        Rate Limit Source and Service Tracks:           0
        Rate Limit Dest Only Tracks:                    0
        Rate Limit Dest and Service Tracks:             0
[Expert@MyGW:0]#
```

fwaccel feature

Description

The *fwaccel feature* and *fwaccel6 feature* commands enable and disable the specified SecureXL features.

Important:

- If you disable a SecureXL feature, SecureXL does not accelerate the applicable traffic anymore.
- This change does **not** survive reboot.
- In VSX Gateway, this change is global and applies to all Virtual Systems.
- In a Cluster, you must configure all the Cluster Members in the same way.

Syntax for IPv4

```
fwaccel feature <Name of Feature>
      get
      off
      on
```

Syntax for IPv6

```
fwaccel6 feature <Name of Feature>
      get
      off
      on
```

Parameters

Parameter	Description
No Parameters	Shows the applicable built-in usage.
<Name of Feature>	Specifies the SecureXL feature. R81.20 SecureXL supports only this feature: ■ Name: `sctp` ■ Description: Stream Control Transmission Protocol (SCTP) - see sk35113
`get`	Shows the current state of the specified SecureXL feature.
`off`	Disables the specified SecureXL feature. This means that SecureXL does not accelerate the applicable traffic anymore.
`on`	Enables the specified SecureXL feature. This means that SecureXL accelerates the applicable traffic again.

Disabling the '`sctp`' feature permanently

See *"Working with Kernel Parameters" on page 2021*.

1. Add this line to the `$FWDIR/boot/modules/fwkern.conf` file:

   ```
   sim_sctp_disable_by_default=1
   ```

2. Reboot.

Example 1 - Default output

```
[Expert@MyGW:0]# fwaccel feature
Usage: fwaccel feature <name> {on|off|get}

Available features: sctp
[Expert@MyGW:0]#
```

Example 2 - Disabling and enabling a feature

```
[Expert@MyGW:0]# fwaccel feature sctp get
sim_sctp_disable_by_default = 0
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel feature sctp off
Set operation succeeded
[Expert@MyGW:0]# fwaccel feature sctp get
sim_sctp_disable_by_default = 1
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel feature sctp on
Set operation succeeded
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel feature sctp get
sim_sctp_disable_by_default = 0
[Expert@MyGW:0]#
```

fwaccel ip_mr_cache

Description

The *fwaccel ip_mr_cache* command shows the IPv4 multicast routing cache when SecureXL works in the User Mode.

Syntax for IPv4

```
fwaccel [-i <SecureXL ID>] ip_mr_cache
```

Parameters

Parameter	Description
`-i <SecureXL ID>`	Specifies the SecureXL instance ID (for IPv4 only).

Example

```
[Expert@MyGW:0]# fwaccel ip_mr_cache
Group           Origin          Iif     Wrong    Last Used  Flags      Refcount  Oifs
[Expert@MyGW:0]#
```

fwaccel off

Description

The *fwaccel off* and *fwaccel6 off* commands stop the SecureXL on-the-fly.

Starting from R80.20, you can stop the SecureXL only *temporarily*. The SecureXL starts automatically when you start Check Point services (with the *"cpstart" on page 1018* command), or reboot the Security Gateway.

Important:

- Disable the SecureXL only for debug purposes, if Check Point Support explicitly instructs you to do so.
- If you disable the SecureXL, this change does **not** survive reboot.
  SecureXL remains disabled until you enable it again on-the-fly, or reboot the Security Gateway.
- If you disable the SecureXL, this change applies only to new connections that arrive after you disable the acceleration.
  SecureXL continues to accelerate the connections that are already accelerated.
  Other non-connection oriented processing continues to function (for example, virtual defragmentation, VPN decrypt).
- On a VSX Gateway:
  - If you wish to stop the acceleration only for a specific Virtual System, go to the context of that Virtual System.
    In Gaia Clish, run: `set virtual-system <VSID>`
    In Expert mode, run: `vsenv <VSID>`
  - If you wish to stop the acceleration for all Virtual Systems, you must use the "`-a`" parameter.
    In this case, it does not matter from which Virtual System context you run this command.
- In a Cluster, you must configure all the Cluster Members in the same way.

Syntax for IPv4

```
fwaccel off [-a] [-q]
```

Syntax for IPv6

```
fwaccel6 off [-a] [-q]
```

Parameters

Parameter	Description
`-a`	On a VSX Gateway, stops acceleration on all Virtual Systems.
`-q`	Suppresses the output (does not show a returned output).

Possible returned output

- `SecureXL device disabled`
- `SecureXL device is not active`
- `Failed to disable SecureXL device`
- `fwaccel_off: failed to set process context <VSID>`

Example 1 - Output from a non-VSX Gateway

```
[Expert@MyGW:0]# fwaccel off
SecureXL device disabled.
[Expert@MyGW:0]#
```

Example 2 - Output from a VSX Gateway for a specific Virtual System

```
[Expert@MyVSXGW:1]# vsx stat -v
VSX Gateway Status
==================
Name:            VSX2_192.168.3.242
Access Control Policy: VSX_GW_VSX
Installed at:    17Sep2018 13:17:14
Threat Prevention Policy: <No Policy>
SIC Status:      Trust

Number of Virtual Systems allowed by license:          25
Virtual Systems [active / configured]:                  2 / 2
Virtual Routers and Switches [active / configured]:     0 / 0
Total connections [current / limit]:                    4 / 44700

Virtual Devices Status
======================

 ID  | Type &amp;amp; Name     | Access Control Policy | Installed at    | Threat Prevention Policy
| SIC Stat
-----+--------------------+-----------------------+-----------------+--------------------------
+---------
   1 | S VS1              | VS1_Policy            | 17Sep2018 12:47 | <No Policy>
| Trust
   2 | S VS2              | VS2_Policy            | 17Sep2018 12:47 | <No Policy>
| Trust

Type: S - Virtual System, B - Virtual System in Bridge mode,
      R - Virtual Router, W - Virtual Switch.

[Expert@MyVSXGW:1]#
[Expert@MyVSXGW:1]# vsenv 1
Context is set to Virtual Device VS1 (ID 1).
[Expert@MyVSXGW:1]#
[Expert@MyVSXGW:1]# fwaccel stat
+-------------------------------------------------------------------------------+
|Id|Name     |Status     |Interfaces               |Features                     |
+-------------------------------------------------------------------------------+
|0 |KPPAK    |enabled    |eth1,eth2,eth3           |Acceleration,Cryptography    |
|  |         |           |                         |                             |
|  |         |           |                         |Crypto: Tunnel,UDPEncap,MD5, |
|  |         |           |                         |SHA1,3DES,DES,AES-128,AES-256,|
|  |         |           |                         |ESP,LinkSelection,DynamicVPN,|
|  |         |           |                         |NatTraversal,AES-XCBC,SHA256,|
|  |         |           |                         |SHA384,SHA512                |
+-------------------------------------------------------------------------------+

Accept Templates : enabled
Drop Templates   : disabled
NAT Templates    : enabled
LightSpeed Accel : disabled
[Expert@MyVSXGW:1]#

[Expert@MyVSXGW:1]# fwaccel off
SecureXL device disabled. (Virtual ID 1)
[Expert@MyVSXGW:1]#
[Expert@MyVSXGW:1]# fwaccel stat
+-------------------------------------------------------------------------------+
|Id|Name     |Status     |Interfaces               |Features                     |
+-------------------------------------------------------------------------------+
|0 |KPPAK    |disabled   |eth1,eth2,eth3           |Acceleration,Cryptography    |
|  |         |           |                         |                             |
|  |         |           |                         |Crypto: Tunnel,UDPEncap,MD5, |
|  |         |           |                         |SHA1,3DES,DES,AES-128,AES-256,|
|  |         |           |                         |ESP,LinkSelection,DynamicVPN,|
|  |         |           |                         |NatTraversal,AES-XCBC,SHA256,|
|  |         |           |                         |SHA384,SHA512                |
+-------------------------------------------------------------------------------+
```

```
Accept Templates : enabled
Drop Templates   : disabled
NAT Templates    : enabled
LightSpeed Accel : disabled
[Expert@MyVSXGW:1]#
```

Example 3 - Output from a VSX Gateway for all Virtual Systems

```
[Expert@MyVSXGW:1]# vsx stat -v
VSX Gateway Status
==================
Name:            VSX2_192.168.3.242
Access Control Policy: VSX_GW_VSX
Installed at:    17Sep2018 13:17:14
Threat Prevention Policy: <No Policy>
SIC Status:      Trust

Number of Virtual Systems allowed by license:          25
Virtual Systems [active / configured]:                  2 / 2
Virtual Routers and Switches [active / configured]:     0 / 0
Total connections [current / limit]:                    4 / 44700

Virtual Devices Status
======================

 ID  | Type &amp;amp; Name     | Access Control Policy | Installed at    | Threat Prevention Policy
| SIC Stat
-----+---------------------+-----------------------+-----------------+--------------------------
+---------
   1 | S VS1               | VS1_Policy            | 17Sep2018 12:47 | <No Policy>
| Trust
   2 | S VS2               | VS2_Policy            | 17Sep2018 12:47 | <No Policy>
| Trust

Type: S - Virtual System, B - Virtual System in Bridge mode,
      R - Virtual Router, W - Virtual Switch.

[Expert@MyVSXGW:1]#
[Expert@MyVSXGW:1]# vsenv 1
Context is set to Virtual Device VS1 (ID 1).
[Expert@MyVSXGW:1]#
[Expert@MyVSXGW:1]# fwaccel off -a
SecureXL device disabled. (Virtual ID 0)
SecureXL device disabled. (Virtual ID 1)
SecureXL device disabled. (Virtual ID 2)
[Expert@MyVSXGW:1]#
```

fwaccel on

Description

The *fwaccel on* and *fwaccel6 on* commands start the acceleration on-the-fly, if it was previously stopped with the *fwaccel off* or *fwaccel6 off* command (see *"fwaccel off" on page 1454*).

Important:

- On a VSX Gateway:
  - If you wish to start the acceleration only for a specific Virtual System, go to the context of that Virtual System.
    In Gaia Clish, run: `set virtual-system <VSID>`
    In Expert mode, run: `vsenv <VSID>`
  - If you wish to start the acceleration for all Virtual Systems, you must use the "`-a`" parameter.
    In this case, it does not matter from which Virtual System context you run this command.
- In a Cluster, you must configure all the Cluster Members in the same way.

Syntax for IPv4

```
fwaccel on [-a] [-q]
```

Syntax for IPv6

```
fwaccel6 on [-a] [-q]
```

Parameters

Parameter	Description
`-a`	On a VSX Gateway, starts the acceleration on all Virtual Systems.
`-q`	Suppresses the output (does not show a returned output).

Possible returned output

- `SecureXL device is enabled.`
- `Failed to start SecureXL.`
- `No license for SecureXL.`
- `SecureXL is disabled by the firewall. Please try again later.`

- The installed SecureXL device is not compatible with the installed firewall (version mismatch).
- The SecureXL device is in the process of being stopped. Please try again later.
- SecureXL cannot be started while "flows" are active.
- SecureXL is already started.
- SecureXL will be started after a policy is loaded.
- fwaccel: Failed to check FloodGate-1 status. Acceleration will not be started.
- FW-1: SecureXL acceleration cannot be started while QoS is running in express mode.

  Please disable FloodGate-1 express mode or SecureXL.
- FW-1: SecureXL acceleration cannot be started while QoS is running with citrix printing rule.

  Please remove the citrix printing rule to enable SecureXL.
- FW-1: SecureXL acceleration cannot be started while QoS is running with UAS rule.

  Please remove the UAS rule to enable SecureXL.
- FW-1: SecureXL acceleration cannot be started while QoS is running.

  Please remove the QoS blade to enable SecureXL.
- Failed to enable SecureXL device
- fwaccel_on: failed to set process context <*VSID*>

Example 1 - Output from a non-VSX Gateway

```
[Expert@MyGW:0]# fwaccel on
SecureXL device is enabled.
[Expert@MyGW:0]#
```

Example 2 - Output from a VSX Gateway for a specific Virtual System

```
[Expert@MyVSXGW:1]# vsx stat -v
VSX Gateway Status
==================
Name:            VSX2_192.168.3.242
Access Control Policy: VSX_GW_VSX
Installed at:    17Sep2018 13:17:14
Threat Prevention Policy: <No Policy>
SIC Status:      Trust

Number of Virtual Systems allowed by license:          25
Virtual Systems [active / configured]:                  2 / 2
Virtual Routers and Switches [active / configured]:     0 / 0
Total connections [current / limit]:                    4 / 44700

Virtual Devices Status
======================

 ID  | Type &amp;amp; Name     | Access Control Policy | Installed at    | Threat Prevention Policy
| SIC Stat
-----+---------------------+-----------------------+-----------------+--------------------------
+---------
   1 | S VS1               | VS1_Policy            | 17Sep2018 12:47 | <No Policy>
| Trust
   2 | S VS2               | VS2_Policy            | 17Sep2018 12:47 | <No Policy>
| Trust

Type: S - Virtual System, B - Virtual System in Bridge mode,
      R - Virtual Router, W - Virtual Switch.

[Expert@MyVSXGW:1]#
[Expert@MyVSXGW:1]# vsenv 1
Context is set to Virtual Device VS1 (ID 1).
[Expert@MyVSXGW:1]#
[Expert@MyVSXGW:1]# fwaccel stat
+-------------------------------------------------------------------------------+
|Id|Name     |Status     |Interfaces               |Features                     |
+-------------------------------------------------------------------------------+
|0 |KPPAK    |disabled   |eth1,eth2,eth3           |Acceleration,Cryptography    |
|  |         |           |                         |                             |
|  |         |           |                         |Crypto: Tunnel,UDPEncap,MD5, |
|  |         |           |                         |SHA1,3DES,DES,AES-128,AES-256,|
|  |         |           |                         |ESP,LinkSelection,DynamicVPN,|
|  |         |           |                         |NatTraversal,AES-XCBC,SHA256,|
|  |         |           |                         |SHA384,SHA512                |
+-------------------------------------------------------------------------------+

Accept Templates : enabled
Drop Templates   : disabled
NAT Templates    : enabled
LightSpeed Accel : disabled
[Expert@MyVSXGW:1]#

[Expert@MyVSXGW:1]# fwaccel on
SecureXL device enabled. (Virtual ID 1)
[Expert@MyVSXGW:1]#
[Expert@MyVSXGW:1]# fwaccel stat
+-------------------------------------------------------------------------------+
|Id|Name     |Status     |Interfaces               |Features                     |
+-------------------------------------------------------------------------------+
|0 |KPPAK    |enabled    |eth1,eth2,eth3           |Acceleration,Cryptography    |
|  |         |           |                         |                             |
|  |         |           |                         |Crypto: Tunnel,UDPEncap,MD5, |
|  |         |           |                         |SHA1,3DES,DES,AES-128,AES-256,|
|  |         |           |                         |ESP,LinkSelection,DynamicVPN,|
|  |         |           |                         |NatTraversal,AES-XCBC,SHA256,|
|  |         |           |                         |SHA384,SHA512                |
+-------------------------------------------------------------------------------+
```

```
Accept Templates : enabled
Drop Templates   : disabled
NAT Templates    : enabled
LightSpeed Accel : disabled
[Expert@MyVSXGW:1]#
```

Example 3 - Output from a VSX Gateway for all Virtual Systems

```
[Expert@MyVSXGW:1]# vsx stat -v
VSX Gateway Status
==================
Name:            VSX2_192.168.3.242
Access Control Policy: VSX_GW_VSX
Installed at:    17Sep2018 13:17:14
Threat Prevention Policy: <No Policy>
SIC Status:      Trust

Number of Virtual Systems allowed by license:          25
Virtual Systems [active / configured]:                  2 / 2
Virtual Routers and Switches [active / configured]:     0 / 0
Total connections [current / limit]:                    4 / 44700

Virtual Devices Status
======================

 ID  | Type &amp;amp; Name     | Access Control Policy | Installed at    | Threat Prevention Policy
| SIC Stat
-----+---------------------+-----------------------+-----------------+--------------------------
+---------
   1 | S VS1               | VS1_Policy            | 17Sep2018 12:47 | <No Policy>
| Trust
   2 | S VS2               | VS2_Policy            | 17Sep2018 12:47 | <No Policy>
| Trust

Type: S - Virtual System, B - Virtual System in Bridge mode,
      R - Virtual Router, W - Virtual Switch.

[Expert@MyVSXGW:1]#
[Expert@MyVSXGW:1]# vsenv 1
Context is set to Virtual Device VS1 (ID 1).
[Expert@MyVSXGW:1]#
[Expert@MyVSXGW:1]# fwaccel on -a
[Expert@MyVSXGW:1]#
```

fwaccel ranges

Description

The *fwaccel ranges* and *fwaccel6 ranges* commands show the SecureXL loaded ranges:

- Ranges of Rule Base source IP addresses
- Ranges of Rule Base destination IP addresses
- Ranges of Rule Base destination ports and protocols

The Security Gateway creates these ranges during the policy installation. The Firewall creates and offloads ranges to SecureXL when any of these features is enabled:

- Rulebase ranges for Drop Templates
- Anti-Spoofing enforcement ranges on per-interface basis
- NAT64 ranges
- NAT46 ranges

These ranges are related to matching of connections to SecureXL Drop Templates. These ranges represent the **Source**, **Destination** and **Service** columns of the Rule Base.

These ranges are not exactly the same as the Rule Base, because as there are objects that cannot be represented as real (deterministic) IP addresses. For example, Domain objects and Dynamic objects. The Security Gateway converts such non-deterministic objects to "Any" IP address.

In addition, implied rules are represented in these ranges, except for some specific implied rules.

You can use these commands for troubleshooting.

Syntax for IPv4

```
fwaccel ranges
      -h
      -a
      -l
      -p <Range ID>
      -s <Range ID>
```

Syntax for IPv6

```
fwaccel6 ranges
      -h
      -a
      -l
      -p <Range ID>
      -s <Range ID>
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in usage.
`-a` *or* No Parameters	Shows the full information for all loaded ranges. **Note** - In the list of SecureXL Drop Templates (output of the *"fwaccel templates" on page 1521* command), each Drop Template is assembled from ranges indexes. To see mapping between range index and the range itself, run this command "`fwaccel ranges -a`". This way you understand better the practical ranges for Drop Templates and when it is appropriate to use them.
`-l`	Shows the list of loaded ranges: ■ 0 - Ranges of Rule Base source IP addresses ■ 1 - Ranges of Rule Base destination IP addresses ■ 2 - Ranges of Rule Base destination ports and protocols
`-p <Range ID>`	Shows the full information for the specified range.
`-s <Range ID>`	Shows the summary information for the specified range.

Examples

Example 1 - Show the list of ranges from a non-VSX Gateway

```
[Expert@MyGW:0]# fwaccel ranges -l
SecureXL device 0:
        0 Rule base source ranges (ip):
        1 Rule base destination ranges (ip):
        2 Rule base dport ranges (port, proto):
[Expert@MyGW:0]#
```

Example 2 - Show the full information for all loaded ranges from a non-VSX Gateway

```
[Expert@MyGW:0]# fwaccel ranges
SecureXL device 0:
    Rule base source ranges (ip):
        (0) 0.0.0.0 - 192.168.204.0
        (1) 192.168.204.1 - 192.168.204.1
        (2) 192.168.204.2 - 192.168.204.39
        (3) 192.168.204.40 - 192.168.204.40
        (4) 192.168.204.41 - 192.168.254.39
        (5) 192.168.254.40 - 192.168.254.40
        (6) 192.168.254.41 - 255.255.255.255
    Rule base destination ranges (ip):
        (0) 0.0.0.0 - 192.168.204.0
        (1) 192.168.204.1 - 192.168.204.1
        (2) 192.168.204.2 - 192.168.204.39
        (3) 192.168.204.40 - 192.168.204.40
        (4) 192.168.204.41 - 192.168.254.39
        (5) 192.168.254.40 - 192.168.254.40
        (6) 192.168.254.41 - 255.255.255.255
    Rule base dport ranges (port, proto):
        (0) 0, 0 - 138, 6
        (1) 139, 6 - 139, 6
        (2) 140, 6 - 18189, 6
        (3) 18190, 6 - 18190, 6
        (4) 18191, 6 - 18191, 6
        (5) 18192, 6 - 18192, 6
        (6) 18193, 6 - 19008, 6
        (7) 19009, 6 - 19009, 6
        (8) 19010, 6 - 136, 17
        (9) 137, 17 - 138, 17
        (10) 139, 17 - 65535, 65535
[Expert@MyGW:0]#
```

Example 3 - Show the full information for the specified range from a non-VSX Gateway

```
[Expert@MyGW:0]# fwaccel ranges -p 0
SecureXL device 0:
    Rule base source ranges (ip):
        (0) 0.0.0.0 - 192.168.204.0
        (1) 192.168.204.1 - 192.168.204.1
        (2) 192.168.204.2 - 192.168.204.39
        (3) 192.168.204.40 - 192.168.204.40
        (4) 192.168.204.41 - 192.168.254.39
        (5) 192.168.254.40 - 192.168.254.40
        (6) 192.168.254.41 - 255.255.255.255
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel ranges -p 1
SecureXL device 0:
    Rule base destination ranges (ip):
        (0) 0.0.0.0 - 192.168.204.0
        (1) 192.168.204.1 - 192.168.204.1
        (2) 192.168.204.2 - 192.168.204.39
        (3) 192.168.204.40 - 192.168.204.40
        (4) 192.168.204.41 - 192.168.254.39
        (5) 192.168.254.40 - 192.168.254.40
        (6) 192.168.254.41 - 255.255.255.255
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel ranges -p 2
SecureXL device 0:
    Rule base dport ranges (port, proto):
        (0) 0, 0 - 138, 6
        (1) 139, 6 - 139, 6
        (2) 140, 6 - 18189, 6
        (3) 18190, 6 - 18190, 6
        (4) 18191, 6 - 18191, 6
        (5) 18192, 6 - 18192, 6
        (6) 18193, 6 - 19008, 6
        (7) 19009, 6 - 19009, 6
        (8) 19010, 6 - 136, 17
        (9) 137, 17 - 138, 17
        (10) 139, 17 - 65535, 65535
[Expert@MyGW:0]#
```

Example 4 - Show the summary information for the specified range from a non-VSX Gateway

```
[Expert@MyGW:0]# fwaccel ranges -s 0
SecureXL device 0:
    List name "Rule base source ranges (ip):", ID 0, Number of ranges 7
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel ranges -s 1
SecureXL device 0:
    List name "Rule base destination ranges (ip):", ID 1, Number of ranges 7
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel ranges -s 2
SecureXL device 0:
    List name "Rule base dport ranges (port, proto):", ID 2, Number of ranges 11
[Expert@MyGW:0]#
```

Example 5 - Show the list of ranges from a VSX Gateway

```
[Expert@MyVSXGW:2]# vsenv 0
Context is set to Virtual Device VSX2_192.168.3.242 (ID 0).
[Expert@MyVSXGW:0]# fwaccel ranges -l
SecureXL device 0:
        0 Anti spoofing ranges eth0:
        1 Anti spoofing ranges eth1:
[Expert@MyVSXGW:0]# vsenv 1
Context is set to Virtual Device VS1 (ID 1).
[Expert@MyVSXGW:1]# fwaccel ranges -l
SecureXL device 0:
        0 Anti spoofing ranges eth3:
        1 Anti spoofing ranges eth2.52:
[Expert@MyVSXGW:1]# vsenv 2
Context is set to Virtual Device VS2 (ID 2).
[Expert@MyVSXGW:2]# fwaccel ranges -l
SecureXL device 0:
        0 Anti spoofing ranges eth4:
        1 Anti spoofing ranges eth2.53:
[Expert@MyVSXGW:2]#
```

Example 6 - Show the full information for all loaded ranges from a VSX Gateway

```
[Expert@MyVSXGW:2]# vsenv 0
Context is set to Virtual Device VSX2_192.168.3.242 (ID 0).
[Expert@MyVSXGW:0]# fwaccel ranges
SecureXL device 0:
    Anti spoofing ranges eth0:
        (0) 0.0.0.0 - 10.20.29.255
        (1) 10.20.31.0 - 126.255.255.255
        (2) 128.0.0.0 - 192.168.2.255
        (3) 192.168.3.1 - 192.168.3.241
        (4) 192.168.3.243 - 192.168.3.254
        (5) 192.168.4.0 - 223.255.255.255
        (6) 240.0.0.0 - 255.255.255.254
    Anti spoofing ranges eth1:
        (0) 10.20.30.1 - 10.20.30.241
        (1) 10.20.30.243 - 10.20.30.254
[Expert@MyVSXGW:0]#
[Expert@MyVSXGW:1]# vsenv 1
Context is set to Virtual Device VS1 (ID 1).
[Expert@MyVSXGW:1]# fwaccel ranges
SecureXL device 0:
    Anti spoofing ranges eth3:
        (0) 40.50.60.0 - 40.50.60.255
        (1) 192.168.196.17 - 192.168.196.17
        (2) 192.168.196.19 - 192.168.196.30
    Anti spoofing ranges eth2.52:
        (0) 70.80.90.0 - 70.80.90.255
        (1) 192.168.196.1 - 192.168.196.1
        (2) 192.168.196.3 - 192.168.196.14
[Expert@MyVSXGW:1]#
[Expert@MyVSXGW:1]# vsenv 2
Context is set to Virtual Device VS2 (ID 2).
[Expert@MyVSXGW:2]# fwaccel ranges
SecureXL device 0:
    Anti spoofing ranges eth4:
        (0) 100.100.100.0 - 100.100.100.255
        (1) 192.168.196.17 - 192.168.196.17
        (2) 192.168.196.19 - 192.168.196.30
    Anti spoofing ranges eth2.53:
        (0) 192.168.196.1 - 192.168.196.1
        (1) 192.168.196.3 - 192.168.196.14
        (2) 200.200.200.0 - 200.200.200.255
[Expert@MyVSXGW:2]#
```

Example 7 - Show the summary information for the specified range from a VSX Gateway

```
[Expert@MyVSXGW:2]# vsenv 1
Context is set to Virtual Device VS1 (ID 1).
[Expert@MyVSXGW:1]#
[Expert@MyVSXGW:1]# fwaccel ranges -s 0
SecureXL device 0:
    List name "Anti spoofing ranges eth3:", ID 0, Number of ranges 3
[Expert@MyVSXGW:1]#
[Expert@MyVSXGW:1]# fwaccel ranges -s 1
SecureXL device 0:
    List name "Anti spoofing ranges eth2.52:", ID 1, Number of ranges 3
[Expert@MyVSXGW:1]#
[Expert@MyVSXGW:1]# fwaccel ranges -s 2
SecureXL device 0:
        The requested range table is empty
[Expert@MyVSXGW:1]#
[Expert@MyVSXGW:1]# vsenv 2
Context is set to Virtual Device VS2 (ID 2).
[Expert@MyVSXGW:1]#
[Expert@MyVSXGW:2]# fwaccel ranges -s 0
SecureXL device 0:
    List name "Anti spoofing ranges eth4:", ID 0, Number of ranges 3
[Expert@MyVSXGW:1]#
[Expert@MyVSXGW:2]# fwaccel ranges -s 1
SecureXL device 0:
    List name "Anti spoofing ranges eth2.53:", ID 1, Number of ranges 3
[Expert@MyVSXGW:1]#
[Expert@MyVSXGW:2]# fwaccel ranges -s 2
SecureXL device 0:
        The requested range table is empty
[Expert@MyVSXGW:2]#
```

fwaccel stat

Description

The *fwaccel stat* and *fwaccel6 stat* commands show this information on the Security Gateway, or Cluster Member:

Shows this information:

Column	Information
Id	Always 0.
Name	SecureXL mode (KPPAK or UPPAK).
Status	Enabled or Disabled.
Interfaces	Names of accelerated interfaces.
Features	Names of accelerated features.

In addition, these command show the status of these features (enabled or disabled):

- SecureXL Accept Templates.
- SecureXL Drop Templates.
- SecureXL NAT Templates.
- SecureXL status of LightSpeed Acceleration.

Syntax for IPv4

```
fwaccel stat
```

Syntax for IPv6

```
fwaccel6 stat
```

Example

- This output is from a Security Gateway (non-VSX).
- SecureXL works in the Kernel Mode (KPPAK) mode.
- SecureXL is enabled.
- SecureXL accelerates the interfaces eth0 and eth1.

```
[Expert@MyGW:0]# fwaccel stat
+-------------------------------------------------------------------------------+
|Id|Name     |Status     |Interfaces               |Features                     |
+-------------------------------------------------------------------------------+
|0 |KPPAK    |enabled    |eth0,eth1                |Acceleration,Cryptography    |
|  |         |           |                         |                             |
|  |         |           |                         |Crypto: Tunnel,UDPEncap,MD5, |
|  |         |           |                         |SHA1,3DES,DES,AES-128,AES-256,|
|  |         |           |                         |ESP,LinkSelection,DynamicVPN, |
|  |         |           |                         |NatTraversal,AES-XCBC,SHA256, |
|  |         |           |                         |SHA384,SHA512                |
+-------------------------------------------------------------------------------+

Accept Templates : enabled
Drop Templates   : disabled
NAT Templates    : enabled
LightSpeed Accel : disabled
[Expert@MyGW:0]#
```

fwaccel stats

Description

The *fwaccel stats* and *fwaccel6 stats* commands show acceleration statistics for IPv4 on the local Security Gateway, or Cluster Member.

Syntax for IPv4

```
fwaccel stats
      [-c]
      [-d]
      [-l]
      [-m]
      [-n]
      [-o]
      [-p]
      [-q]
      [-r]
      [-s]
      [-x]
```

Syntax for IPv6

```
fwaccel6 stats
      [-c]
      [-d]
      [-l]
      [-m]
      [-n]
      [-o]
      [-p]
      [-q]
      [-r]
      [-s]
      [-x]
```

Parameters

Parameter	Description
`-c`	Shows the statistics for Cluster Correction.
`-d`	Shows the statistics for drops from device.
`-l`	Shows the statistics in legacy mode - as one table.
`-m`	Shows the statistics for multicast traffic.
`-n`	Shows the statistics for Identity Awareness (NAC).
`-o`	Shows the statistics for Reorder Infrastructure. **Note** - Scalable Platforms do not support this parameter.
`-p`	Shows the statistics for SecureXL violations (F2F packets).
`-q`	Shows the statistics notifications the SecureXL sent to the Firewall.
`-r`	Resets all the counters.
`-s`	Shows the statistics summary only.
`-x`	Shows the statistics for PXL. **Note** - PXL is the technology name for combination of SecureXL and PSL (Passive Streaming Library).

In addition, see:

- *"Description of the Statistics Counters in the "fwaccel stats" Output" on page 1475*
- *"Example Outputs on the "fwaccel stats" Commands" on page 1484*

Description of the Statistics Counters in the "fwaccel stats" Output

The "Accelerated Path" section

Counter	Description
`accel packets`	Number of accelerated packets.
`accel bytes`	Number of accelerated bytes.
`outbound packets`	Number of outbound packets.
`outbound bytes`	Number of outbound bytes.
`conns created`	Number of connections the SecureXL created.
`conns deleted`	Number of connections the SecureXL deleted.
`C total conns`	Total number of connections the SecureXL currently handles.
`C templates`	*Not in use* Total number of SecureXL templates the SecureXL currently handles.
`C TCP conns`	Number of TCP connections the SecureXL currently handles.
`C non TCP conns`	Number of non-TCP connections the SecureXL currently handles.
`conns from templates`	*Not in use* Number of connections the SecureXL created from SecureXL templates.
`nat conns`	Number of NAT connections.
`dropped packets`	Number of packets the SecureXL dropped.
`dropped bytes`	Number of bytes the SecureXL dropped.
`nat templates`	*Not in use*
`port alloc templates`	*Not in use*
`conns from nat tmpl`	*Not in use*
`port alloc conns`	*Not in use*

Counter	Description
`fragments received`	Number of received fragments.
`fragments transmit`	Number of transmitted fragments.
`fragments dropped`	Number of dropped fragments.
`fragments expired`	Number of expired fragments.
`IP options stripped`	Number of packets, from SecureXL stripped IP options.
`IP options restored`	Number of packets, in which SecureXL restored IP options.
`IP options dropped`	Number of packets with IP options that SecureXL dropped.
`corrs created`	Number of corrections the SecureXL made.
`corrs deleted`	Number of corrections the SecureXL deleted.
`C corrections`	Number of corrections the SecureXL currently handles.
`corrected packets`	Number of corrected packets.
`corrected bytes`	Number of corrected bytes.

The "Accelerated VPN Path" section

Counter	Description
`C crypt conns`	Number of encrypted connections the SecureXL currently handles.
`enc bytes`	Number of encrypted traffic bytes.
`dec bytes`	Number of decrypted traffic bytes.
`ESP enc pkts`	Number of ESP encrypted packets.
`ESP enc err`	Number of ESP encryption errors.
`ESP dec pkts`	Number of ESP decrypted packets.
`ESP dec err`	Number of ESP decryption errors.
`ESP other err`	Number of ESP general errors.
`espudp enc pkts`	*Not in use*
`espudp enc err`	*Not in use*
`espudp dec pkts`	*Not in use*
`espudp dec err`	*Not in use*
espudp other err	*Not in use*

The "Medium Streaming Path" section

Counter	Description
`PXL packets`	Number of PXL packets. PXL is combination of SecureXL and Passive Streaming Library (PSL), which is an IPS infrastructure that transparently listens to TCP traffic as network packets, and rebuilds the TCP stream out of these packets. Passive Streaming can listen to all TCP traffic, but process only the data packets, which belong to a previously registered connection.
`PXL async packets`	Number of PXL packets the SecureXL handled asynchronously.
`PXL bytes`	Number of PXL bytes.
`C PXL conns`	Number of PXL connections the SecureXL currently handles.
`C PXL templates`	*Not in use* Number of PXL templates.
`PXL FF conns`	Number of PXL Fast Forward connections.
`PXL FF packets`	Number of PXL Fast Forward packets.
`PXL FF bytes`	Number of PXL Fast Forward bytes.
`PXL FF acks`	Number of PXL Fast Forward acknowledgments.

The "Inline Streaming Path" section

Counter	Description
`PSL Inline packets`	Number of accelerated PSL packets.
`PSL Inline bytes`	Number of accelerated PSL bytes.
`CPAS Inline packets`	Number of accelerated CPAS packets.
`CPAS Inline bytes`	Number of accelerated CPAS bytes.

The "QoS General Information" section

Counter	Description
`Total QoS Conns`	Total number of QoS connections.
`QoS Classify Conns`	Number of classified QoS connections.
`QoS Classify flow`	Number of classified QoS flows.
`Reclassify QoS polic`	Number of reclassify QoS requests.

The "Firewall QoS Path" section

Counter	Description
`Enqueued IN packets`	Number of waiting packets in Firewall QoS inbound queue.
`Enqueued OUT packets`	Number of waiting packets in Firewall QoS outbound queue.
`Dequeued IN packets`	Number of processed packets in Firewall QoS inbound queue.
`Dequeued OUT packets`	Number of processed packets in Firewall QoS outbound queue.
`Enqueued IN bytes`	Number of waiting bytes in Firewall QoS inbound queue.
`Enqueued OUT bytes`	Number of waiting bytes in Firewall QoS outbound queue.
`Dequeued IN bytes`	Number of processed bytes in Firewall QoS inbound queue.
`Dequeued OUT bytes`	Number of processed bytes in Firewall QoS outbound queue.

The "Firewall QoS Path" section

Counter	Description
`Enqueued IN packets`	Number of waiting packets in SecureXL QoS inbound queue.
`Enqueued OUT packets`	Number of waiting packets in SecureXL QoS outbound queue.
`Dequeued IN packets`	Number of processed packets in SecureXL QoS inbound queue.
`Dequeued OUT packets`	Number of processed packets in SecureXL QoS outbound queue.
`Enqueued IN bytes`	Number of waiting bytes in SecureXL QoS inbound queue.
`Enqueued OUT bytes`	Number of waiting bytes in SecureXL QoS outbound queue.
`Dequeued IN bytes`	Number of processed bytes in SecureXL QoS inbound queue.
`Dequeued OUT bytes`	Number of processed bytes in SecureXL QoS outbound queue.

The "Firewall Path" section

Counter	Description
`F2F packets`	Number of packets that SecureXL forwarded to the Firewall kernel in Slow Path.
`F2F bytes`	Number of bytes that SecureXL forwarded to the Firewall kernel in Slow Path.
`TCP violations`	Number of packets, which are in violation of the TCP state.
`C anticipated conns`	Number of anticipated connections SecureXL currently handles.
`port alloc f2f`	*Not in use*
`F2V conn match pkts`	Number of packets that matched a SecureXL connection and SecureXL forwarded to the Firewall kernel.
`F2V packets`	Number of packets that SecureXL forwarded to the Firewall kernel and the Firewall re-injected back to SecureXL.
`F2V bytes`	Number of bytes that SecureXL forwarded to the Firewall kernel and the Firewall re-injected back to the SecureXL.

The "GTP" section

Counter	Description
`gtp tunnels created`	Number of created GTP tunnels.
`gtp tunnels`	Number of GTP tunnels the SecureXL currently handles.
`gtp accel pkts`	Number of accelerated GTP packets.
`gtp f2f pkts`	Number of GTP packets the SecureXL forwarded to the Firewall kernel.
`gtp spoofed pkts`	Number of spoofed GTP packets.
`gtp in gtp pkts`	Number of GTP-in-GTP packets.
`gtp signaling pkts`	Number of signaling GTP packets.
`gtp tcpopt pkts`	Number of GTP packets with TCP Options.
`gtp apn err pkts`	Number of GTP packets with APN errors.

The "General" section

Counter	Description
`memory used`	*Not in use*
`free memory`	*Not in use*
`C used templates`	*Not in use*
`pxl tmpl conns`	*Not in use*
`C conns from tmpl`	*Not in use* Number of current connections that SecureXL created from SecureXL Templates.
`C tcp handshake conn`	Number of current TCP connections that are not yet established.
`C tcp established co`	Number of established TCP connections the SecureXL currently handles.
`C tcp closed conns`	Number of closed TCP connections the SecureXL currently handles.
`C tcp pxl handshake`	Number of not yet established PXL TCP connections the SecureXL currently handles.
`C tcp pxl establishe`	Number of established PXL TCP connections the SecureXL currently handles.
`C tcp pxl closed con`	Number of closed PXL TCP connections the SecureXL currently handles.
`outbound pxl packets`	*Not in use*

Example Outputs on the "fwaccel stats" Commands

Example: fwaccel stats -s

Example of statistics summary:

```
Accelerated conns/Total conns : 0/0 (0%)
Accelerated pkts/Total pkts   : 0/8 (0%)
F2Fed pkts/Total pkts         : 8/8 (100%)
F2V pkts/Total pkts           : 0/8 (0%)
CPASXL pkts/Total pkts        : 0/8 (0%)
PSLXL pkts/Total pkts         : 0/8 (0%)
QOS inbound pkts/Total pkts   : 0/8 (0%)
QOS outbound pkts/Total pkts  : 0/8 (0%)
Corrected pkts/Total pkts     : 0/8 (0%)
```

Example: fwaccel stats

Example of the default output:

```
Name                          Value         Name                          Value
---------------------------  ------------  ---------------------------  ------------

Accelerated Path
-------------------------------------------------------------------------------
accel packets                           0    accel bytes                           0
outbound packets                        0    outbound bytes                        0
conns created                           0    conns deleted                         0
C total conns                           0    C TCP conns                           0
C non TCP conns                         0    nat conns                             0
dropped packets                         0    dropped bytes                         0
fragments received                      0    fragments transmit                    0
fragments dropped                       0    fragments expired                     0
IP options stripped                     0    IP options restored                   0
IP options dropped                      0    corrs created                         0
corrs deleted                           0    C corrections                         0
corrected packets                       0    corrected bytes                       0

Accelerated VPN Path
-------------------------------------------------------------------------------
C crypt conns                           0    enc bytes                             0
dec bytes                               0    ESP enc pkts                          0
ESP enc err                             0    ESP dec pkts                          0
ESP dec err                             0    ESP other err                         0
espudp enc pkts                         0    espudp enc err                        0
espudp dec pkts                         0    espudp dec err                        0
espudp other err                        0

Medium Streaming Path
-------------------------------------------------------------------------------
CPASXL packets                          0    PSLXL packets                         0
CPASXL async packets                    0    PSLXL async packets                   0
CPASXL bytes                            0    PSLXL bytes                           0
C CPASXL conns                          0    C PSLXL conns                         0
CPASXL conns created                    0    PSLXL conns created                   0
PXL FF conns                            0    PXL FF packets                        0
PXL FF bytes                            0    PXL FF acks                           0
PXL no conn drops                       0

Inline Streaming Path
-------------------------------------------------------------------------------
PSL Inline packets                      0    PSL Inline bytes                      0
CPAS Inline packets                     0    CPAS Inline bytes                     0

QoS Paths
-------------------------------------------------------------------------------
QoS General Information:
------------------------
Total QoS Conns                         0    QoS Classify Conns                    0
QoS Classify flow                       0    Reclassify QoS policy                 0

FireWall QoS Path:
------------------
Enqueued IN packets                     0    Enqueued OUT packets                  0
Dequeued IN packets                     0    Dequeued OUT packets                  0
Enqueued IN bytes                       0    Enqueued OUT bytes                    0
Dequeued IN bytes                       0    Dequeued OUT bytes                    0

Accelerated QoS Path:
---------------------
Enqueued IN packets                     0    Enqueued OUT packets                  0
Dequeued IN packets                     0    Dequeued OUT packets                  0
Enqueued IN bytes                       0    Enqueued OUT bytes                    0
Dequeued IN bytes                       0    Dequeued OUT bytes                    0

Firewall Path
-------------------------------------------------------------------------------
F2F packets                         35324    F2F bytes                       1797781
TCP violations                          0    F2V conn match pkts                   0
F2V packets                             0    F2V bytes                             0
```

```
GTP
-------------------------------------------------------------------------------
gtp tunnels created                     0    gtp tunnels                        0
gtp accel pkts                          0    gtp f2f pkts                       0
gtp spoofed pkts                        0    gtp in gtp pkts                    0
gtp signaling pkts                      0    gtp tcpopt pkts                    0
gtp apn err pkts                        0

General
-------------------------------------------------------------------------------
memory used                      38798784    C tcp handshake conns              0
C tcp established conns                 0    C tcp closed conns                 0
C tcp pxl handshake conns               0    C tcp pxl established conns        0
C tcp pxl closed conns                  0    outbound cpasxl packets            0
outbound pslxl packets                  0    outbound cpasxl bytes              0
outbound pslxl bytes                    0    DNS DoR stats                      0

(*) Statistics marked with C refer to current value, others refer to total value
```

Example: fwaccel stats -c

Example of statistics for Cluster Correction:

```
Cluster Correction stats:

 Name                    Value          Name                     Value
----------------------  ------------   ----------------------  ------------
Sent pkts (total)                0    Sent with metadata                0
Received pkts (total)            0    Received with metadata            0
Sent bytes                       0    Received bytes                    0
Send errors                      0    Receive errors                    0
```

Example: fwaccel stats -d

Example of statistics for drops from device:

```
Reason                Value              Reason                Value
--------------------  ---------------    --------------------  ---------------
general reason                   0    CPASXL decision                   0
PSLXL decision                   0    clr pkt on vpn                    0
encrypt failed                   0    drop template                     0
decrypt failed                   0    interface down                    0
cluster error                    0    XMT error                         0
anti spoofing                    0    local spoofing                    0
sanity error                     0    monitored spoofed                 0
QOS decision                     0    C2S violation                     0
S2C violation                    0    Loop prevention                   0
DOS Fragments                    0    DOS IP Options                    0
DOS Blacklists                   0    DOS Penalty Box                   0
DOS Rate Limiting                0    Syn Attack                        0
Reorder                          0    Expired Fragments                 0
```

Example: fwaccel stats -l

Example of the output in legacy mode (as one table):

```
Name                          Value         Name                          Value
---------------------------  ------------  ---------------------------  ------------
-                                    0     accel packets                         0
accel bytes                          0     outbound packets                      0
outbound bytes                       0     conns created                         0
conns deleted                        0     C total conns                         0
C TCP conns                          0     C non TCP conns                       0
nat conns                            0     dropped packets                       0
dropped bytes                        0     fragments received                    0
fragments transmit                   0     fragments dropped                     0
fragments expired                    0     IP options stripped                   0
IP options restored                  0     IP options dropped                    0
corrs created                        0     corrs deleted                         0
C corrections                        0     corrected packets                     0
corrected bytes                      0     C crypt conns                         0
enc bytes                            0     dec bytes                             0
ESP enc pkts                         0     ESP enc err                           0
ESP dec pkts                         0     ESP dec err                           0
ESP other err                        0     espudp enc pkts                       0
espudp enc err                       0     espudp dec pkts                       0
espudp dec err                       0     espudp other err                      0
acct update interval              3600     CPASXL packets                        0
PSLXL packets                        0     CPASXL async packets                  0
PSLXL async packets                  0     CPASXL bytes                          0
PSLXL bytes                          0     C CPASXL conns                        0
C PSLXL conns                        0     CPASXL conns created                  0
PSLXL conns created                  0     PXL FF conns                          0
PXL FF packets                       0     PXL FF bytes                          0
PXL FF acks                          0     PXL no conn drops                     0
PSL Inline packets                   0     PSL Inline bytes                      0
CPAS Inline packets                  0     CPAS Inline bytes                     0
Total QoS Conns                      0     QoS Classify Conns                    0
QoS Classify flow                    0     Reclassify QoS policy                 0
Enqueued IN packets                  0     Enqueued OUT packets                  0
Dequeued IN packets                  0     Dequeued OUT packets                  0
Enqueued IN bytes                    0     Enqueued OUT bytes                    0
Dequeued IN bytes                    0     Dequeued OUT bytes                    0
Enqueued IN packets                  0     Enqueued OUT packets                  0
Dequeued IN packets                  0     Dequeued OUT packets                  0
Enqueued IN bytes                    0     Enqueued OUT bytes                    0
Dequeued IN bytes                    0     Dequeued OUT bytes                    0
F2F packets                      35383     F2F bytes                       1801493
TCP violations                       0     F2V conn match pkts                   0
F2V packets                          0     F2V bytes                             0
gtp tunnels created                  0     gtp tunnels                           0
gtp accel pkts                       0     gtp f2f pkts                          0
gtp spoofed pkts                     0     gtp in gtp pkts                       0
gtp signaling pkts                   0     gtp tcpopt pkts                       0
gtp apn err pkts                     0     memory used                    38798784
C tcp handshake conns                0     C tcp established conns               0
C tcp closed conns                   0     C tcp pxl handshake conns             0
C tcp pxl established conns          0     C tcp pxl closed conns                0
outbound cpasxl packets              0     outbound pslxl packets                0
outbound cpasxl bytes                0     outbound pslxl bytes                  0
DNS DoR stats                        0
(*) Statistics marked with C refer to current value, others refer to total value
```

Example: fwaccel stats -m

Example of statistics for multicast traffic:

```
Name                  Value              Name                  Value
--------------------  ---------------    --------------------  ---------------
in packets                           0    out packets                          0
if restricted                        0    conns with down if                   0
f2f packets                          0    f2f bytes                            0
dropped packets                      0    dropped bytes                        0
accel packets                        0    accel bytes                          0
mcast conns                          0
```

Example: fwaccel stats -n

Example of statistics for Identity Awareness (NAC):

```
Name                  Value              Name                  Value
--------------------  ---------------    --------------------  ---------------
NAC packets                          0    NAC bytes                            0
NAC connections                      0    compliance failure                   0
```

Example: fwaccel stats -o

Example of statistics for Reorder Infrastructure:

```
Appliaction: F2V
        Statistic                       Value
----------------------------------     --------------------
                        Queued pkts                     0
                    Max queued pkts                     0
                    Timer triggered                     0
          Callback hahndling unhold                     0
 Callback hahndling unhold and drop                     0
           Callback hahndling reset                     0
              Dequeued pkts resumed                     0
                Queue ent allocated                     0
                    Queue ent freed                     0
                   Queues allocated                     0
                       Queues freed                     0
                     Ack notif sent                     0
              Ack respones handling                     0
              Dequeued pkts dropped                     0
       Reached max queued pkt limit                     0
                  Set timer failed                      0
                Error already held                      0
             Queue ent alloc failed                     0
                 Queue alloc failed                     0
                   Ack notif failed                     0
       Ack respones handling failed                     0
-------------------------------------------------

Appliaction: Route
        Statistic                       Value
----------------------------------     --------------------
                        Queued pkts                     0
                    Max queued pkts                     0
                    Timer triggered                     0
          Callback hahndling unhold                     0
 Callback hahndling unhold and drop                     0
           Callback hahndling reset                     0
              Dequeued pkts resumed                     0
                Queue ent allocated                     0
                    Queue ent freed                     0
                   Queues allocated                     0
                       Queues freed                     0
                     Ack notif sent                     0
              Ack respones handling                     0
              Dequeued pkts dropped                     0
       Reached max queued pkt limit                     0
                  Set timer failed                      0
                Error already held                      0
             Queue ent alloc failed                     0
                 Queue alloc failed                     0
                   Ack notif failed                     0
       Ack respones handling failed                     0
-------------------------------------------------

Appliaction: New connection
        Statistic                       Value
----------------------------------     --------------------
                        Queued pkts                     0
                    Max queued pkts                     0
                    Timer triggered                     0
          Callback hahndling unhold                     0
 Callback hahndling unhold and drop                     0
           Callback hahndling reset                     0
              Dequeued pkts resumed                     0
                Queue ent allocated                     0
                    Queue ent freed                     0
                   Queues allocated                     0
                       Queues freed                     0
                     Ack notif sent                     0
              Ack respones handling                     0
              Dequeued pkts dropped                     0
       Reached max queued pkt limit                     0
                  Set timer failed                      0
```

```
                Error already held                    0
             Queue ent alloc failed                   0
                 Queue alloc failed                   0
                   Ack notif failed                   0
       Ack respones handling failed                   0
-------------------------------------------------

Appliaction: F2P
        Statistic                       Value
----------------------------------     --------------------
                        Queued pkts                     0
                     Max queued pkts                    0
                     Timer triggered                    0
          Callback hahndling unhold                     0
 Callback hahndling unhold and drop                     0
           Callback hahndling reset                     0
              Dequeued pkts resumed                     0
                Queue ent allocated                     0
                    Queue ent freed                     0
                  Queues allocated                      0
                      Queues freed                      0
                    Ack notif sent                      0
              Ack respones handling                     0
              Dequeued pkts dropped                     0
       Reached max queued pkt limit                     0
                   Set timer failed                     0
                Error already held                      0
             Queue ent alloc failed                     0
                 Queue alloc failed                     0
                   Ack notif failed                     0
       Ack respones handling failed                     0
-------------------------------------------------
```

Note - Scalable Platforms do not support this parameter.

Example: fwaccel stats -p

Example of statistics for SecureXL violations (F2F packets):

```
F2F packets:
--------------
Violation             Packets            Violation             Packets
--------------------  ---------------    --------------------  ---------------
pkt has IP options                0    ICMP miss conn                    3036
TCP-SYN miss conn                 8    TCP-other miss conn              32224
UDP miss conn                  3772    other miss conn                      0
VPN returned F2F                  0    uni-directional viol                 0
possible spoof viol               0    TCP state viol                       0
out if not def/accl               0    bridge, src=dst                      0
routing decision err              0    sanity checks failed                 0
fwd to non-pivot                  0    broadcast/multicast                  0
cluster message                   0    cluster forward                      0
chain forwarding                  0    F2V conn match pkts                  0
general reason                    0    route changes                        0
```

Example: fwaccel stats -q

Example of statistics for notifications the SecureXL sent to the Firewall:

```
Notification           Packets           Notification           Packets
--------------------  --------------    ---------------------  --------------
ntSAAboutToExpire                 0    ntSAExpired                         0
ntMSPIError                       0    ntNoInboundSA                       0
ntNoOutboundSA                    0    ntDataIntegrityFailed               0
ntPossibleReplay                  0    ntReplay                            0
ntNextProtocolError               0    ntCPIError                          0
ntClearTextPacket                 0    ntFragmentation                     0
ntUpdateUdpEncTable               0    ntSASync                            0
ntReplayOutOfWindow               0    ntVPNTrafficReport                  0
ntConnDeleted                     0    ntConnUpdate                        0
ntPacketDropped                   0    ntSendLog                           0
ntRefreshGTPTunnel                0    ntMcastDrop                         0
ntAccounting                      0    ntAsyncIndex                        0
ntACkReordering                   0    ntAccelAckInfo                      0
ntMonitorPacket                   0    ntPacketCapture                     0
ntCpasPacketCapture               0    ntPSLGlueUpdateReject               0
ntSeqVerifyDrop                   0    ntPacketForwardBefore               0
ntICMPMessage                     0    ntQoSReclassifyPacket               0
ntQoSResumePacket                 0    ntVPNEncHaLinkFailure               0
ntVPNEncLsLinkFailure             0    ntVPNEncRouteChange                 0
ntVPNDecVerRouteChang             0    ntVPNDecRouteChange                 0
ntMuxSimToFw                      0    ntPSLEventLog                       0
ntSendCPHWDStats              14871    ntPacketTaggingViolat               0
ntDosNotify                      28    ntSynatkNotify                      0
ntSynatkStats                     0    ntQoSEventLog                       0
ntPrintGetParam                   0
```

Example: fwaccel stats -x

Example of statistics for PXL:

```
PXL Release Context statistics:

 Name                    Value          Name                    Value
----------------------  ------------    ----------------------  ------------
End Handler                        0    Post Sync                          0
Stop Stream                        0    kbuf fail                          0
Set field failure                  0    Notif set field fail               0
Non SYN seq fail                   0    Tmpl kbuf fail                     0
Tmpl set field fail                0    Segment Injection                  0
Init app fail                      0    Expiration                         0
Newconn set field fail             0    Newconn fail                       0
CPHWD dec                          0    No PSL policy                      0

PXL Exception statistics:

 Name                    Value          Name                    Value
----------------------  ------------    ----------------------  ------------
urgent packets                     0    invalid SYN retrans                0
SYN seq not init                   0    old pkts out win                   0
old pkts out win trunc             0    old pkts out win strip             0
new pkts out win                   0    incorrect retrans                  0
TCP pkts with bad csum             0    ACK unprocessed data               0
old ACK out win                    0    Max segments reached               0
No resources                       0    Hold timeout                       0
```

fwaccel synatk

Description

The *fwaccel synatk* and *fwaccel6 synatk* commands control the Accelerated SYN Defender on the local Security Gateway, or Cluster Member.

Important:

- See sk120476 for information about the 'SYN Attack' protection in SmartConsole.
- In a Scalable Platform, the same SecureXL command must run on all Security Group Members.
  Therefore, you must run the SecureXL commands in either Gaia gClish, or Expert mode.
  - In Gaia gClish, run the "`fwaccel ...`" and "`fwaccel6 ...`" commands.
  - In the Expert mode, run the "`g_fwaccel ...`" and "`g_fwaccel6 ...`" commands.
- In a Scalable Platform, when you add a new Security Group Member to a Security Group, the new Security Group Member pulls the "`fwaccel synatk`" configuration that you saved it in a configuration file - in the default file `$FWDIR/conf/synatk.conf`, or in the file specified with the "`fwaccel synatk -c`" command.

Syntax for IPv4

```
fwaccel synatk
      -a
      -c <options>
      -d
      -e
      -g
      -m
      -t <options>
      config
      monitor <options>
      state <options>
      whitelist <options>
```

Syntax for IPv6

```
fwaccel6 synatk
      -a
      -c <options>
      -d
      -e
      -g
      -m
      -t <options>
      config
      monitor <options>
      state <options>
      whitelist <options>
```

Parameters

Parameter	Description
No Parameters	Shows the applicable built-in usage.
`-a`	Applies the configuration from the default file. See *"fwaccel synatk -a" on page 1495*.
`-c <options>`	Applies the configuration from the specified file. See *"fwaccel synatk -c <Configuration File>" on page 1496*.
`-d`	Disables the Accelerated SYN Defender on all interfaces. See *"fwaccel synatk -d" on page 1497*.
`-e`	Enables the Accelerated SYN Defender on interfaces with topology "External". Enables the Accelerated SYN Defender in Monitor (Detect only) mode on interfaces with topology "Internal". See *"fwaccel synatk -e" on page 1498*.
`-g`	Enables the Accelerated SYN Defender on all interfaces. See *"fwaccel synatk -g" on page 1499*.
`-m`	Enables the Accelerated SYN Defender in Monitor (Detect only) mode on all interfaces. In this state, the Accelerated SYN Defender only sends a log when it recognizes a TCP SYN Flood attack. See *"fwaccel synatk -m" on page 1500*.

Parameter	Description
`-t <options>`	Configures the threshold numbers of half-opened TCP connections that trigger the Accelerated SYN Defender. See *"fwaccel synatk -t <Threshold>" on page 1501*.
`config`	Shows the current Accelerated SYN Defender configuration. See *"fwaccel synatk config" on page 1508*.
`monitor <options>`	Shows the Accelerated SYN Defender status. See *"fwaccel synatk monitor" on page 1511*.
`state <options>`	Controls the Accelerated SYN Defender states. See *"fwaccel synatk state" on page 1516*.
`whitelist <options>`	Controls the Accelerated SYN Defender whitelist. See *"fwaccel synatk allow" on page 1503*.

fwaccel synatk -a

Description

The "*fwaccel synatk -a*" and "*fwaccel6 synatk -a*" commands apply the Accelerated SYN Defender configuration from the default `$FWDIR/conf/synatk.conf` file.

Notes:

- Both IPv4 and IPv6 use the same configuration file.
- Interface specific state settings that you define in the configuration file, override the settings that you define with these commands:
  - *"fwaccel synatk -d" on page 1497*
  - *"fwaccel synatk -e" on page 1498*
  - *"fwaccel synatk -g" on page 1499*
  - *"fwaccel synatk -m" on page 1500*

Syntax for IPv4

```
fwaccel synatk -a
```

Syntax for IPv6

```
fwaccel6 synatk -a
```

fwaccel synatk -c <Configuration File>

Description

The "*fwaccel synatk -c <Configuration File>*" and "*fwaccel6 synatk -c <Configuration File>*" commands apply the Accelerated SYN Defender configuration from the specified file.

Important - If you use this parameter, then it must be the first parameter in the syntax.

Notes:

- Both IPv4 and IPv6 use the same configuration file.
- The state settings of a specific interface that you define in the configuration file, override the settings that you define with these commands:
  - *"fwaccel synatk -d" on page 1497*
  - *"fwaccel synatk -e" on page 1498*
  - *"fwaccel synatk -g" on page 1499*
  - *"fwaccel synatk -m" on page 1500*

Syntax for IPv4

```
fwaccel synatk -c <Configuration File>
```

Syntax for IPv6

```
fwaccel6 synatk -c <Configuration File>
```

Parameters

Parameter	Description
<Configuration File>	Specifies the full path and the name of the file. For reference, see the default file: `$FWDIR/conf/synatk.conf`

fwaccel synatk -d

Description

The "*fwaccel synatk -d*" and "*fwaccel6 synatk -d*" commands disable the Accelerated SYN Defender on all interfaces.

Notes:

- This command:
  1. Modifies the default configuration file `$FWDIR/conf/synatk.conf`, or the configuration file specified with the "`-c`" parameter.
  2. Loads the modified file.
  3. Does not show any output.
- Output of the *"fwaccel synatk monitor" on page 1511* command shows:
  - In the row "`Configuration`": `Disabled`
  - In the column "`Enforce`": `Disable`
  - In the column "`State (sec)`": `Disable`
- Output of the *"fwaccel synatk config" on page 1508* command shows:
  - In the row "`enabled`": `0`
  - In the row "`enforce`": `0`

Syntax for IPv4

```
fwaccel synatk -d
```

Syntax for IPv6

```
fwaccel6 synatk -d
```

fwaccel synatk -e

Description

The "*fwaccel synatk -e*" and "*fwaccel6 synatk -e*" commands:

- Enable the Accelerated SYN Defender on interfaces with topology "External".
- Enable the Accelerated SYN Defender in Monitor (Detect only) mode on interfaces with topology "Internal".

Notes:

- This command:
  1. Modifies the default configuration file `$FWDIR/conf/synatk.conf`, or the configuration file specified with the "`-c`" parameter.
  2. Loads the modified file.
- Output of the *"fwaccel synatk monitor" on page 1511* command shows for "External" interfaces:
  - Configuration: `Enforcing`
  - Enforce: `Prevent`
  - State: `Ready` (may change later depending on what the SYN Defender detects)
- Output of the *"fwaccel synatk monitor" on page 1511* command shows for "Internal" interfaces:
  - Configuration: `Enforcing`
  - Enforce: `Detect`
  - State: `Monitor`
- Output of the *"fwaccel synatk config" on page 1508* command shows:
  - `enabled 1`
  - `enforce 1`

Syntax for IPv4

```
fwaccel synatk -e
```

Syntax for IPv6

```
fwaccel6 synatk -e
```

fwaccel synatk -g

Description

The "*fwaccel synatk -g*" and "*fwaccel6 synatk -g*" commands enable the Accelerated SYN Defender on all interfaces.

Notes:

- This command:
  1. Modifies the default configuration file `$FWDIR/conf/synatk.conf`, or the configuration file specified with the "`-c`" parameter.
  2. Loads the modified file.
- Output of the *"fwaccel synatk monitor" on page 1511* command shows for "External" interfaces:
  - Configuration: `Enforcing`
  - Enforce: `Prevent`
  - State: `Ready` (may change later depending on what the SYN Defender detects)
- Output of the *"fwaccel synatk monitor" on page 1511* command shows for "Internal" interfaces:
  - Configuration: `Enforcing`
  - Enforce: `Detect`
  - State: `Monitor`
- Output of the *"fwaccel synatk config" on page 1508* command shows:
  - `enabled 1`
  - `enforce 2`

Syntax for IPv4

```
fwaccel synatk -g
```

Syntax for IPv6

```
fwaccel6 synatk -g
```

fwaccel synatk -m

Description

The "*fwaccel synatk -m*" and "*fwaccel6 synatk -m*" commands enable the Accelerated SYN Defender in Monitor (Detect only) mode on all interfaces.

In this state, the Accelerated SYN Defender only sends a log when it recognizes a TCP SYN Flood attack.

Notes:

- This command:
  1. Modifies the default configuration file `$FWDIR/conf/synatk.conf`, or the configuration file specified with the "`-c`" parameter.
  2. Loads the modified file.
- Output of the *"fwaccel synatk monitor" on page 1511* command shows:
  - Configuration: `Monitoring`
  - Enforce: `Detect`
  - State: `Monitor`
- Output of the *"fwaccel synatk config" on page 1508* command shows:
  - `enabled 1`
  - `enforce 0`

Syntax for IPv4

```
fwaccel synatk -m
```

Syntax for IPv6

```
fwaccel6 synatk -m
```

fwaccel synatk -t <Threshold>

Description

The "*fwaccel synatk -t <Threshold>*" and "*fwaccel6 synatk -t <Threshold>*" commands configure the threshold numbers of half-opened TCP connections that trigger the Accelerated SYN Defender.

Notes:

- This command:
  1. Modifies the default configuration file `$FWDIR/conf/synatk.conf`, or the configuration file specified with the "`-c`" parameter.
  2. Loads the modified file.
- Threshold values are independent for IPv4 and IPv6.

Syntax for IPv4

```
fwaccel synatk -t <Threshold>
```

Syntax for IPv6

```
fwaccel6 synatk -t <Threshold>
```

Thresholds

- The **Global high attack threshold** number is configured to the specified value *<Threshold>*.

  This is the number of half-open TCP connections on all interfaces required for the Accelerated SYN Defender to engage.

  - Valid values: 100 and greater
  - Default: 10000

- The **High attack threshold** number is configured to 1/2 of the specified value *<Threshold>*.

  This is the high number of half-open TCP connections on an interface required for the Accelerated SYN Defender to engage.

  - Valid values: (Low attack threshold) < (High attack threshold) <= (Global high attack threshold)
  - Default: 5000

- The **Low attack threshold** number is configured to 1/10 of the specified value *<Threshold>*.

  This is the low number of half-open TCP connections on an interface required for the Accelerated SYN Defender to engage.

  - Valid values: 10 and greater
  - Default: 1000

fwaccel synatk allow

Description

The "*fwaccel synatk allow*" and "*fwaccel6 synatk allow*" commands control the Accelerated SYN Defender allow-list.

Notes:

- This allow-list overrides which packet the Accelerated SYN Defender drops. Before you use a 3rd-party or automatic blacklists, add trusted networks and hosts to the allow-list to avoid outages.
- Also, see the *"fwaccel dos whitelist" on page 1428* command.

Important - In Cluster, you must configure the Rate Limiting in the same way on all the Cluster Members.

Syntax for IPv4

```
fwaccel synatk allow
      -a <IPv4 Address>[/<Subnet Prefix>]
      -d <IPv4 Address>[/<Subnet Prefix>]
      -F
      -l /<Path>/<Name of File>
      -L
      -s
```

Syntax for IPv6

```
fwaccel6 synatk allow
      -a <IPv6 Address>[/<Subnet Prefix>]
      -d <IPv6 Address>[/<Subnet Prefix>]
      -F
      -l /<Path>/<Name of File>
      -L
      -s
```

Parameters

Parameter	Description
No Parameters	Shows the applicable built-in usage.

Parameter	Description

`-a <IPv4 Address> [/<Subnet Prefix>]`	Adds the specified IPv4 address to the Accelerated SYN Defender allow-list.
	■ *<IPv4 Address>*
	Can be an IPv4 address of a network or a host.
	■ *<Subnet Prefix>*
	Must specify the length of the subnet mask in the format `/<bits>`.
	Optional for a host IPv4 address.
	Mandatory for a network IPv4 address.
	Range - from /1 to /32.
	Important - If you do not specify the subnet prefix explicitly, this command uses the subnet prefix /32.
	Examples:
	■ For a host:
	`192.168.20.30`
	`192.168.20.30/32`
	■ For a network:
	`192.168.20.0/24`

`-a <IPv6 Address> [/<Subnet Prefix>]`	Adds the specified IPv6 address to the Accelerated SYN Defender allow-list.
	■ *<IPv6 Address>*
	Can be an IPv6 address of a network or a host.
	■ *<Subnet Prefix>*
	Must specify the length of the subnet mask in the format `/<bits>`.
	Optional for a host IPv6 address.
	Mandatory for a network IPv6 address.
	Range - from /1 to /128.
	Important - If you do not specify the subnet prefix explicitly, this command uses the subnet prefix /128.
	Examples:
	■ For a host:
	`2001:0db8:85a3:0000:0000:8a2e:0370:7334`
	`2001:0db8:85a3:0000:0000:8a2e:0370:7334/128`
	■ For a network:
	`2001:cdba:9abc:5678::/64`

Parameter	Description
`-d <IPv4 Address> [/<Subnet Prefix>]`	Removes the specified IPv4 address from the Accelerated SYN Defender allow-list. ■ *<IPv4 Address>* Can be an IPv4 address of a network or a host. ■ *<Subnet Prefix>* Optional. Must specify the length of the subnet mask in the format `/<bits>`. Optional for a host IPv4 address. Mandatory for a network IPv4 address. Range - from /1 to /32. **Important** - If you do not specify the subnet prefix explicitly, this command uses the subnet prefix /32.
`-d <IPv6 Address> [/<Subnet Prefix>]`	Removes the specified IPv6 address from the Accelerated SYN Defender allow-list. ■ *<IPv6 Address>* Can be an IPv6 address of a network or a host. ■ *<Subnet Prefix>* Optional. Must specify the length of the subnet mask in the format `/<bits>`. Optional for a host IPv6 address. Mandatory for a network IPv6 address. Range - from /1 to /128. **Important** - If you do not specify the subnet prefix explicitly, this command uses the subnet prefix /128.
`-F`	Removes (flushes) all entries from the Accelerated SYN Defender allow-list.

Parameter	Description
`-l /<Path>/<Name of File>`	Loads the Accelerated SYN Defender allow-list entries from the specified plain-text file. **Note** - To replace the current allow-list with the contents of a new file, use both the `-F` and `-l` parameters on the same command line. **Important:** ■ You must manually create and configure this file with the `touch` or `vi` command. ■ You must assign at least the read permission to this file with the `chmod +x` command. ■ Each entry in this file must be on a separate line. ■ Each entry in this file must be in this format: *<IPv4 Address>*`[/`*<Subnet Prefix>*`]` ■ SecureXL ignores empty lines and lines that start with the # character in this file.
`-L`	Loads the Accelerated SYN Defender allow-list entries from the plain-text file with a predefined name: `$FWDIR/conf/synatk-allow-list-v4.conf` Security Gateway automatically runs these commands "`{fwaccel | fwaccel6} synatk allow -L`" during each boot. **Note** - To replace the current allow-list with the contents of a new file, use both the "`-F`" and "`-L`" parameters on the same command line. **Important:** ■ This file does not exist by default. ■ You must manually create and configure this file with the `touch` or `vi` command. ■ You must assign at least the read permission to this file with the `chmod +x` command.. ■ Each entry in this file must be on a separate line. ■ Each entry in this file must be in this format: *<IPv4 Address>*`[/`*<Subnet Prefix>*`]` ■ SecureXL ignores empty lines and lines that start with the # character in this file.
`-s`	Shows the current Accelerated SYN Defender allow-list entries.

Example

```
[Expert@MyGW:0]# fwaccel synatk allow -a 192.168.20.0/24
[Expert@MyGW:0]# fwaccel synatk allow -s
192.168.20.0/24
[Expert@MyGW:0]# fwaccel synatk allow -d 192.168.20.0/24
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel synatk allow -a 192.168.40.55
[Expert@MyGW:0]# fwaccel synatk allow -s
192.168.40.55/32
[Expert@MyGW:0]# fwaccel synatk allow -d 192.168.40.55
```

fwaccel synatk config

Description

The "*fwaccel synatk config*" and "*fwaccel6 synatk config*" commands show the current Accelerated SYN Defender configuration.

Syntax for IPv4

```
fwaccel synatk config
```

Syntax for IPv6

```
fwaccel6 synatk config
```

Example

```
[Expert@MyGW:0]# fwaccel synatk config
enabled 0
enforce 1
global_high_threshold 10000
periodic_updates 1
cookie_resolution_shift 6
min_frag_sz 80
high_threshold 5000
low_threshold 1000
score_alpha 100
monitor_log_interval (msec) 60000
grace_timeout (msec) 30000
min_time_in_active (msec) 60000
[Expert@MyGW:0]#
```

Description of Configuration Parameters

Parameter	Description
`enabled`	Shows if the Accelerated SYN Defender is enabled or disabled. ■ Valid values: 0 (disabled), 1 (enabled) ■ Default: 0
`enforce`	When the Accelerated SYN Defender is enabled, shows it enforces the protection. Valid values: ■ 0 - The Accelerated SYN Defender is in Monitor (Detect only) mode on all interfaces. ■ 1 - The Accelerated SYN Defender is engaged only on external interfaces when the number of half-open TCP connections exceeds the threshold. ■ 2 - The Accelerated SYN Defender is engaged on both external and internal interfaces when the number of half-open TCP connections exceeds the threshold.
`global_high_threshold`	Global high attack threshold number. See the *"fwaccel synatk -t <Threshold>" on page 1501* command.
`periodic_updates`	For internal Check Point use only. ■ Valid values: 0 (disabled), 1 (enabled) ■ Default: 1
`cookie_resolution_shift`	For internal Check Point use only. ■ Valid values: 1-7 ■ Default: 6
`min_frag_sz`	During the TCP SYN Flood attack, the Accelerated SYN Defender prevents TCP fragments smaller than this minimal size value. ■ Valid values: 80 and greater ■ Default: 80
`high_threshold`	High attack threshold number. See the *"fwaccel synatk -t <Threshold>" on page 1501* command.
`low_threshold`	Low attack threshold number. See the *"fwaccel synatk -t <Threshold>" on page 1501* command.

Parameter	Description
`score_alpha`	For internal Check Point use only. ■ Valid values: 1-127 ■ Default: 100
`monitor_log_ interval (msec)`	Interval, in milliseconds, between successive warning logs in the Monitor (Detect only) mode. ■ Valid values: 1000 and greater ■ Default: 60000
`grace_ timeout (msec)`	Maximal time, in milliseconds, to stay in the Grace state (which is a transitional state between Ready and Active). In the Grace state, the Accelerated SYN Defender stops challenging Clients for TCP SYN Cookie, but continues to validate TCP SYN Cookies it receives from Clients. ■ Valid values: 10000 and greater ■ Default: 30000
`min_time_in_ active (msec)`	Minimal time, in milliseconds, to stay in the Active mode. In the Active mode, the Accelerated SYN Defender is actively challenging TPC SYN packets with SYN Cookies. ■ Valid values: 10000 and greater ■ Default: 60000

fwaccel synatk monitor

Description

The "*fwaccel synatk monitor*" and "*fwaccel6 synatk monitor*" commands show the Accelerated SYN Defender status.

Important - To enable the Accelerated SYN Defender in Monitor (Detect only) mode on all interfaces, you must run the *"fwaccel synatk -m" on page 1500* command.

Syntax for IPv4

```
fwaccel synatk monitor
      [-p]
      [-p] -a
      [-p] -s
      [-p] -v
```

Syntax for IPv6

```
fwaccel6 synatk monitor
      [-p]
      [-p] -a
      [-p] -s
      [-p] -v
```

Parameters

Important - You can specify only one of these parameters: `-a`, `-s`, or `-v`.

Parameter	Description
`-p`	Shows the Accelerated SYN Defender status for each SecureXL instance ("`PPAK ID: 0`" is the Host Security Appliance).
`[-p] -a`	Shows the Accelerated SYN Defender statistics for all interfaces (for each SecureXL instance).
`[-p] -s`	Shows the attack state in short form (for each SecureXL instance).
`[-p] -v`	Shows the attack state in verbose form (for each SecureXL instance).

Examples

Example 1 - Default output before and after enabling the Accelerated SYN Defender

```
[Expert@MyGW:0]# fwaccel synatk monitor
+-------------------------------------------------------------------------------+
| SYN Defender status                                                           |
+-------------------------------------------------------------------------------+
| Configuration                                                        Disabled |
| Status                                                                 Normal |
| Non established connections                                                 0 |
| Global Threshold                                                        10000 |
| Interface Threshold                                                      5000 |
+-------------------------------------------------------------------------------+
| IF              | Topology | Enforce | State (sec)  | Non-established conns |
|                 |          |         |              | Peak      | Current   |
+-------------------------------------------------------------------------------+
| eth0            | External | Disable | Disable      | N/A       | N/A       |
| eth1            | Internal | Disable | Disable      | N/A       | N/A       |
+-------------------------------------------------------------------------------+
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel synatk -m
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel synatk monitor
+-------------------------------------------------------------------------------+
| SYN Defender status                                                           |
+-------------------------------------------------------------------------------+
| Configuration                                                     Monitoring |
| Status                                                                 Normal |
| Non established connections                                                 0 |
| Global Threshold                                                        10000 |
| Interface Threshold                                                      5000 |
+-------------------------------------------------------------------------------+
| IF              | Topology | Enforce | State (sec)  | Non-established conns |
|                 |          |         |              | Peak      | Current   |
+-------------------------------------------------------------------------------+
| eth0            | External | Detect  | Monitor      | 0         | 0         |
| eth1            | Internal | Detect  | Monitor      | 0         | 0         |
+-------------------------------------------------------------------------------+
[Expert@MyGW:0]#
```

Example 2 - Showing the Accelerated SYN Defender status for each SecureXL instance

```
[Expert@MyGW:0]# fwaccel synatk monitor -p
+-------------------------------------------------------------------------------+
| SYN Defender status                                                           |
+-------------------------------------------------------------------------------+
| Configuration                                                      Monitoring |
| Status                                                                 Normal |
| Non established connections                                                 0 |
| Global Threshold                                                        10000 |
| Interface Threshold                                                      5000 |
+-------------------------------------------------------------------------------+
| IF              | Topology | Enforce | State (sec)  | Non-established conns |
|                 |          |         |              | Peak      | Current   |
+-------------------------------------------------------------------------------+
| eth0            | External | Detect  | Monitor      | 0         | 0         |
| eth1            | Internal | Detect  | Monitor      | 0         | 0         |
+-------------------------------------------------------------------------------+

PPAK ID: 0
----------
+-------------------------------------------------------------------------------+
| SYN Defender status                                                           |
+-------------------------------------------------------------------------------+
| Configuration                                                      Monitoring |
| Status                                                                 Normal |
| Non established connections                                                 0 |
| Global Threshold                                                        10000 |
| Interface Threshold                                                      5000 |
+-------------------------------------------------------------------------------+
| IF              | Topology | Enforce | State (sec)  | Non-established conns |
|                 |          |         |              | Peak      | Current   |
+-------------------------------------------------------------------------------+
| eth0            | External | Detect  | Monitor      | 0         | 0         |
| eth1            | Internal | Detect  | Monitor      | 0         | 0         |
+-------------------------------------------------------------------------------+
[Expert@MyGW:0]#
```

Example 3 - Showing the Accelerated SYN Defender statistics for all interfaces and for each SecureXL instance.

```
[Expert@MyGW:0]# fwaccel synatk monitor -p -a
Global:
  status            attached
  nr_active                0

Firewall
----------
Per-interface:
                          eth0        eth1
                      ----------  ----------
topology                External    Internal
state                    Monitor     Monitor
syn ready                      0           0
syn active prev                0           0
syn active curr                0           0
active_score                   0           0
msec grace                     0           0
msec active                    0           0
sent cookies                   0           0
fail validations               0           0
succ validations               0           0
early packets                  0           0
no conn data                   0           0
bogus syn                      0           0
peak non-estab                 0           0
int sent cookies               0           0
int succ validations           0           0
msec interval                  0           0

PPAK ID: 0
----------
Per-interface:
                          eth0        eth1
                      ----------  ----------
topology                External    Internal
state                    Monitor     Monitor
syn ready                      0           0
syn active prev                0           0
syn active curr                0           0
active_score                   0           0
msec grace                     0           0
msec active                    0           0
sent cookies                   0           0
fail validations               0           0
succ validations               0           0
early packets                  0           0
no conn data                   0           0
bogus syn                      0           0
peak non-estab                 0           0
int sent cookies               0           0
int succ validations           0           0
msec interval                  0           0
[Expert@MyGW:0]#
```

Example 4 - Showing the attack state in short form (for each SecureXL instance)

```
[Expert@MyGW:0]# fwaccel synatk monitor -p -s
M,N,0,0

PPAK ID: 0
----------
M,N,0,0
[Expert@MyGW:0]#
```

Example 5 - Showing the attack state in verbose form (for each SecureXL instance)

```
[Expert@MyGW:0]# fwaccel synatk monitor -p -v
+-------------------------------------------------------------------------------+
| SYN Defender statistics                                                       |
+-------------------------------------------------------------------------------+
| Status                                                                Normal  |
| Spoofed SYN/sec                                                            0  |
+-------------------------------------------------------------------------------+
 PPAK ID: 0
----------
+-------------------------------------------------------------------------------+
| SYN Defender statistics                                                       |
+-------------------------------------------------------------------------------+
| Status                                                                Normal  |
| Spoofed SYN/sec                                                            0  |
+-------------------------------------------------------------------------------+
[Expert@MyGW:0]#
```

fwaccel synatk state

Description

The "*fwaccel synatk state*" and "*fwaccel6 synatk state*" commands control the Accelerated SYN Defender states.

The states are independent for IPv4 and IPv6.

Important - This command is **not** intended for end-user usage. Transitions between states (Ready, Grace, and Active) occur automatically. This command provides a way to force temporarily a state transition on an interface or group of interfaces.

Syntax for IPv4

```
fwaccel synatk state
      -h
      -a
      -d
      -g
      -i {all | external | internal | <Name of Interface>}
      -m
      -r
```

Syntax for IPv6

```
fwaccel6 synatk state
      -h
      -a
      -d
      -g
      -i {all | external | internal | <Name of Interface>}
      -m
      -r
```

Parameters

Important - You can specify only one of these parameters: `-a`, `-d`, `-g`, `-m`, or `-r`.

Parameter	Description
`-h`	Shows the applicable built-in usage.
`-a`	Sets the state to Active.
`-d`	Sets the state to Disabled.
`-g`	Sets the state to Grace.
`-i all`	Applies the change to all interfaces (this is the default).
`-i external`	Applies the change only to external interfaces.
`-i internal`	Applies the change only to internal interfaces.
`-i <Name of Interface>`	Applies the change to the specified interface.
`-m`	Sets the state to Monitor (Detect only) mode.
`-r`	Sets the state to Ready.

fwaccel tab

Description

The *fwaccel tab* and *fwaccel6 tab* commands show the contents of the specified SecureXL kernel table.

Notes:

- Dynamic tables, such as the `connections` table can change while this command prints their contents.
  This may cause some values to be missed or reported twice.
- For some tables, the command prints their contents on the screen.
- For some tables, the command prints their contents to the `/var/log/messages` file.
- Also, see the *"fw tab" on page 1228* command.

Syntax for IPv4

```
fwaccel tab [-f] [-m <Number of Rows>] -t <Name of Kernel Table>
fwaccel tab -s -t <Name of Kernel Table>
```

Syntax for IPv6

```
fwaccel6 tab [-f] [-m <Number of Rows>] -t <Name of Kernel Table>
fwaccel6 tab -s -t <Name of Kernel Table>
```

Parameters

Parameter	Description
No Parameters	Shows the applicable built-in usage.
`-f`	Formats the output. We recommend to always use this parameter.
`-m <Number of Rows>`	Specifies how many rows to show from the kernel table. Note - The command counts from the top of the table. Default : 1000
`-s`	Shows summary information only.

Parameter	Description
`-t <Name of Kernel Table>`	Specifies the kernel table. This command supports only these kernel tables: ■ connections ■ dos_ip_blacklists ■ dos_pbox ■ dos_pbox_violating_ips ■ dos_rate_matches ■ dos_rate_track_src ■ dos_rate_track_src_svc ■ drop_templates ■ frag_table ■ gtp_apns ■ gtp_tunnels ■ if_by_name ■ inbound_SAs ■ invalid_replay_counter ■ ipsec_mtu_icmp ■ mcast_drop_conns ■ outbound_SAs ■ PMTU_table ■ <Profile> ■ reset_table ■ vpn_link_selection ■ vpn_trusted_ifs

Examples

```
[Expert@MyGW:0]# fwaccel tab -f -m 200 -t connections
Table connections is empty
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel tab -t inbound_SAs
Table contents written to /var/log/messages.
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel tab -t outbound_SAs
Table contents written to /var/log/messages.
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel tab -t vpn_link_selection
Table contents written to /var/log/messages.
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel tab -t drop_templates
Table drop_templates is empty
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel tab -t vpn_trusted_ifs
Table contents written to /var/log/messages.
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel tab -t profile
Table contents written to /var/log/messages.
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel tab -t mcast_drop_conns
Table contents written to /var/log/messages.
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel tab -t invalid_replay_counter
Table contents written to /var/log/messages.
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel tab -t ipsec_mtu_icmp
Table contents written to /var/log/messages.
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel tab -t gtp_tunnels
Table contents written to /var/log/messages.
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel tab -t gtp_apns
Table contents written to /var/log/messages.
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel tab -t if_by_name
Table contents written to /var/log/messages.
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel tab -t PMTU_table
Table PMTU_table is empty
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel tab -t frag_table
Table frag_table is empty
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel tab -t reset_table
Table reset_table is empty
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel tab -t dos_ip_blacklists
Table dos_ip_blacklists is not active for SecureXL device 0.
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel tab -t dos_pbox
Table dos_pbox is not active for SecureXL device 0.
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel tab -t dos_rate_matches
Table dos_rate_matches is not active for SecureXL device 0.
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel tab -t dos_rate_track_src
Table dos_rate_track_src is not active for SecureXL device 0.
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel tab -t dos_rate_track_src_svc
Table dos_rate_track_src_svc is not active for SecureXL device 0.
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel tab -t dos_pbox_violating_ips
Table dos_pbox_violating_ips is not active for SecureXL device 0.
[Expert@MyGW:0]#
```

fwaccel templates

Description

The *fwaccel templates* and *fwaccel6 templates* commands show the contents of the SecureXL templates tables:

- Accept Templates
- SecureXL Drop Templates
- Firewall Drop Templates

Important:

- By default, all Drop Templates are disabled.
  To enable the SecureXL Drop Templates and Firewall Drop Templates:
  1. In SmartConsole, open the Security Gateway / Cluster object.
  2. In the left tree, click the **Optimizations** pane.
  3. Select **Enable drop optimization**.
  4. Click **OK**.
  5. Install the Access Control policy.
- To disable only the Firewall Drop Templates:
  1. Connect to the command line on the Security Gateway / each Cluster Member.
  2. Set the value of the kernel parameter `fw_drop_templates_enabled` to `0` (zero):
     ```
     fw ctl set -f int fw_drop_templates_enabled 0
     ```

  To enable the Firewall Drop Templates again, run:
  ```
  fw ctl set -f int fw_drop_templates_enabled 1
  ```

Important - Based on the number of current templates, these commands can consume memory at very high level.

Syntax for IPv4

```
fwaccel [-i <SecureXL ID>] templates
      [-h]
      [-c]
      [-d [{-R | -S}]
      [-m <Number of Rows>]
      [-r]
      [-R]
      [-s]
      [-S]
```

Syntax for IPv6

```
fwaccel6 templates
      [-h]
      [-c]
      [-d [{-R | -S}]
      [-m <Number of Rows>]
      [-r]
      [-R]
      [-s]
      [-S]
```

Parameters

Parameter	Description
`-i <SecureXL ID>`	Specifies the SecureXL instance ID (for IPv4 only).
No Parameters	Shows the contents of the SecureXL Accept Templates table (Table Name - `cphwd_tmpl`, Table ID - 8111).
`-h`	Shows the applicable built-in usage.
`-c`	Shows the contents of the Firewall Drop Templates table (connections).
`-d`	Shows the contents of the SecureXL Drop Templates table.
`-d -R`	Shows statistics for the reasons for failures to create SecureXL Drop Templates.
`-d -S`	Shows statistics for the SecureXL Drop Templates.
`-m <Number of Rows>`	Specifies how many rows to show from the templates table. Note - The command counts from the top of the table. Default : 1000
`-r`	Shows the contents of the Firewall Drop Templates table (ranges).
`-R`	Shows the reasons for failures to create SecureXL Connections Templates.
`-s`	Shows the total number of offloaded SecureXL Connections Templates.
`-S`	Shows statistics for the offloaded SecureXL Connections Templates.

Accept Templates flags

One or more of these flags appears in the output:

Flag	Description
A	Connection is accounted (SecureXL counts the number of packets and bytes).
B	Connection is created for a rule that contains an Identity Awareness object, or for a rule below that rule.
E	Connection is created for a NAT rule that contains an Identity Awareness object.
I	Identity Awareness (NAC) is enabled for this connection.
M	Connection is created for a rule that contains a Domain object, or for a rule below that rule.
N	Connection undergoes NAT.
O	Connection is created for a rule that contains a Dynamic object, or for a rule below that rule.
P	Connection is created for a rule that may match a Service with an explicitly configured Source port.
Q	QoS is enabled for this connection.
R	Connection is created for a rule that contains a Traceroute object, or for a rule below that rule.
S	PXL (combination of SecureXL and PSL (Passive Streaming Library)) is enabled for this connection.
T	Connection is created for a rule that contains a Time object, or for a rule below that rule.
U	Connection is unidirectional.
X	Connection is created for a NAT rule that contains a translated Dynamic object.
Z	Connection is created for a rule that contains a Security Zone object, or for a rule below that rule.

Drop Templates flags

One or more of these flags appears in the output:

Flag	Description
D	SecureXL Drop template exists for this connection.
L	Log and Drop action for this connection.

Firewall Drop Templates flags

One or more of these flags appears in the output:

Flag	Description
M	Connection is created for a rule that contains a Domain object, or for a rule below that rule.
O	Connection is created for a rule that contains a Dynamic object, or for a rule below that rule.
U	Connection is created for a rule that contains a Updatable object, or for a rule below that rule.

Examples

Example 1 - Default output

```
[Expert@MyGW:0]# fwaccel templates
Source          SPort Destination     DPort PR Flags         LCT  DLY C2S i/f S2C i/f
--------------- ----- --------------- ----- -- ------------  ---- --- ------- -------
192.168.10.20       * 192.168.10.50      80  6            0     0   0 eth5/eth1 eth1/eth5
[Expert@MyGW:0]#
```

Example 2 - Drop Templates

```
[Expert@MyGW:0]# fwaccel templates -d
The SecureXL drop templates table is empty
[Expert@MyGW:0]#
```

Example 3 - Summary of SecureXL Connections Templates

```
[Expert@MyGW:0]# fwaccel templates -s
Total number of templates: 1
[Expert@MyGW:0]#
```

Example 4 - Templates statistics

```
[Expert@MyGW:0]# fwaccel templates -S

Templates stats:

 Name                      Value           Name                      Value
--------------------     ------------    --------------------     ------------
C templates                          0    conns from templates                 0
nat templates                        0    conns from nat tmpl                  0
C CPASXL templates                   0    C PSLXL templates                    0
C used templates                     0    cpasxl tmpl conns                    0
pslxl tmpl conns                     0    C conns from tmpl                    0

[Expert@MyGW:0]#
```

fwaccel ver

Description

Shows this information:

- Firewall Version and Build
- Accelerator Version
- Firewall API version
- Accelerator API version

Syntax

```
fwaccel ver
```

Example

```
Expert@MyGW:0]# fwaccel ver
Firewall version: R81.20 - Build 123
Acceleration Device: Performance Pack
Accelerator Version 2.1
Firewall API version: 3.0NG (19/11/2015)
Accelerator API version: 3.0NG (19/11/2015)
[Expert@MyGW:0]#
```

fw sam_policy

Description

Manages the Suspicious Activity Policy editor that works with these types of rules:

- Suspicious Activity Monitoring (SAM) rules.

  See sk112061: How to create and view Suspicious Activity Monitoring (SAM) Rules.

- Rate Limiting rules.

  See sk112454: How to configure Rate Limiting rules for DoS Mitigation.

Also, see these commands:

- *"fw sam" on page 295*
- *"sam_alert" on page 405*

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax for IPv4

```
fw [-d] sam_policy
      add <options>
      batch
      del <options>
      get <options>
```

```
fw [-d] samp
      add <options>
      batch
      del <options>
      get <options>
```

Syntax for IPv6

```
fw6 [-d] sam_policy
      add <options>
      batch
      del <options>
      get <options>
```

```
fw6 [-d] samp
      add <options>
      batch
      del <options>
      get <options>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`add <options>`	Adds one Rate Limiting rule one at a time. See *"fw sam_policy add" on page 306*.
`batch`	Adds or deletes many Rate Limiting rules at a time. See *"fw sam_policy batch" on page 319*.
`del <options>`	Deletes one configured Rate Limiting rule one at a time. See *"fw sam_policy del" on page 321*.
`get <options>`	Shows all the configured Rate Limiting rules. See *"fw sam_policy get" on page 324*.

fw sam_policy add

Description

The "*fw sam_policy add*" and "*fw6 sam_policy add*" commands:

- Add one Suspicious Activity Monitoring (SAM) rule at a time.
- Add one Rate Limiting rule at a time.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax to configure a Suspicious Activity Monitoring (SAM) rule for IPv4

```
fw [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] ip <IP Filter Arguments>
```

Syntax to configure a Suspicious Activity Monitoring (SAM) rule for IPv6

```
fw6 [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] ip <IP Filter Arguments>
```

Syntax to configure a Rate Limiting rule for IPv4

```
fw [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] quota <Quota Filter Arguments>
```

Syntax to configure a Rate Limiting rule for IPv6

```
fw6 [-d] sam_policy add [-u] -a {d|n|b} [-l {r|a}] [-t <Timeout>]
[-f <Target>] [-n <"Rule Name">] [-c <"Rule Comment">] [-o <"Rule
Originator">] [-z "<Zone>"] quota <Quota Filter Arguments
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-u`	Optional. Specifies that the rule category is `User-defined`. Default rule category is `Auto`.
`-a {d | n | b}`	Mandatory. Specifies the rule action if the traffic matches the rule conditions: ■ `d` - Drop the connection. ■ `n` - Notify (generate a log) about the connection and let it through. ■ `b` - Bypass the connection - let it through without checking it against the policy rules. **Note** - Rules with action set to *Bypass* cannot have a log or limit specification. Bypassed packets and connections do not count towards overall number of packets and connection for limit enforcement of type ratio.
`-l {r | a}`	Optional. Specifies which type of log to generate for this rule for all traffic that matches: ■ `-r` - Generate a regular log ■ `-a` - Generate an alert log

Parameter	Description
`-t <Timeout>`	Optional. Specifies the time period (in seconds), during which the rule will be enforced. Default timeout is indefinite.
`-f <Target>`	Optional. Specifies the target Security Gateways, on which to enforce the Rate Limiting rule. `<Target>` can be one of these: ■ `all` - This is the default option. Specifies that the rule should be enforced on all managed Security Gateways. ■ Name of the Security Gateway or Cluster object - Specifies that the rule should be enforced only on this Security Gateway or Cluster object (the object name must be as defined in the SmartConsole). ■ Name of the Group object - Specifies that the rule should be enforced on all Security Gateways that are members of this Group object (the object name must be as defined in the SmartConsole).
`-n "<Rule Name>"`	Optional. Specifies the name (label) for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters. ■ Before each space or a backslash character in this string, you must write a backslash (\) character. Example: `"This\ is\ a\ rule\ name\ with\ a\ backslash\ \\"`
`-c "<Rule Comment>"`	Optional. Specifies the comment for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters. ■ Before each space or a backslash character in this string, you must write a backslash (\) character. Example: `"This\ is\ a\ comment\ with\ a\ backslash\ \\"`

Parameter	Description
`-o "<Rule Originator>"`	Optional. Specifies the name of the originator for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters. ■ Before each space or a backslash character in this string, you must write a backslash (\) character. Example: `"Created\ by\ John\ Doe"`
`-z "<Zone>"`	Optional. Specifies the name of the Security Zone for this rule. **Notes:** ■ You must enclose this string in double quotes. ■ The length of this string is limited to 128 characters.
`ip <IP Filter Arguments>`	Mandatory (use this `ip` parameter, or the `quota` parameter). Configures the *Suspicious Activity Monitoring (SAM)* rule. Specifies the IP Filter Arguments for the SAM rule (you must use at least one of these options): `[-C] [-s <Source IP>] [-m <Source Mask>] [-d <Destination IP>] [-M <Destination Mask>] [-p <Port>] [-r <Protocol>]` See the explanations below.

Parameter	Description
`quota <Quota Filter Arguments>`	Mandatory (use this `quota` parameter, or the `ip` parameter). Configures the *Rate Limiting* rule. Specifies the Quota Filter Arguments for the Rate Limiting rule (see the explanations below): ■ `[flush true]` ■ `[source-negated {true | false}] source <Source>` ■ `[destination-negated {true | false}] destination <Destination>` ■ `[service-negated {true | false}] service <Protocol and Port numbers>` ■ `[<Limit1 Name> <Limit1 Value>] [<Limit2 Name> <Limit2 Value>] ...[<LimitN Name> <LimitN Value>]` ■ `[track <Track>]` **Important:** ■ The Quota rules are not applied immediately to the Security Gateway. They are only registered in the Suspicious Activity Monitoring (SAM) policy database. To apply all the rules from the SAM policy database immediately, add "`flush true`" in the `fw samp add` command syntax. ■ Explanation: For new connections rate (and for any rate limiting in general), when a rule's limit is violated, the Security Gateway also drops all packets that match the rule. The Security Gateway computes new connection rates on a per-second basis. At the start of the 1-second timer, the Security Gateway allows all packets, including packets for existing connections. If, at some point, during that 1 second period, there are too many new connections, then the Security Gateway blocks all remaining packets for the remainder of that 1-second interval. At the start of the next 1-second interval, the counters are reset, and the process starts over - the Security Gateway allows packets to pass again up to the point, where the rule's limit is violated.

Explanation for the *IP Filter Arguments* syntax for Suspicious Activity Monitoring (SAM) rules

Argument	Description
`-C`	Specifies that open connections should be closed.
`-s <Source IP>`	Specifies the Source IP address.
`-m <Source Mask>`	Specifies the Source subnet mask (in dotted decimal format - x.y.z.w).
`-d <Destination IP>`	Specifies the Destination IP address.
`-M <Destination Mask>`	Specifies the Destination subnet mask (in dotted decimal format - x.y.z.w).
`-p <Port>`	Specifies the port number (see *IANA Service Name and Port Number Registry*).
`-r <Protocol>`	Specifies the protocol number (see *IANA Protocol Numbers*).

Explanation for the *Quota Filter Arguments* syntax for Rate Limiting rules

Argument	Description
`flush true`	Specifies to compile and load the quota rule to the SecureXL immediately.
`[source-negated {true | false}] source <Source>`	Specifies the source type and its value: ■ `any` The rule is applied to packets sent from all sources. ■ `range:<IP Address>` or `range:<IP Address Start>-<IP Address End>` The rule is applied to packets sent from: • Specified IPv4 addresses (x.y.z.w) • Specified IPv6 addresses (xxxx:yyyy:....:zzzz) ■ `cidr:<IP Address>/<Prefix>` The rule is applied to packets sent from: • IPv4 address with Prefix from 0 to 32 • IPv6 address with Prefix from 0 to 128 ■ `cc:<Country Code>` The rule matches the country code to the source IP addresses assigned to this country, based on the Geo IP database. The two-letter codes are defined in ISO 3166-1 alpha-2. ■ `asn:<Autonomous System Number>` The rule matches the AS number of the organization to the source IP addresses that are assigned to this organization, based on the Geo IP database. The valid syntax is *ASnnnn*, where *nnnn* is a number unique to the specific organization. **Notes:** ■ Default is: `source-negated false` ■ The `source-negated true` processes all source types, *except* the specified type.

Argument	Description
`[destination-negated {true | false}] destination <Destination>`	Specifies the destination type and its value: ■ `any` The rule is applied to packets sent to all destinations. ■ `range:<IP Address>` or `range:<IP Address Start>-<IP Address End>` The rule is applied to packets sent to: • Specified IPv4 addresses (x.y.z.w) • Specified IPv6 addresses (xxxx:yyyy:...:zzzz) ■ `cidr:<IP Address>/<Prefix>` The rule is applied to packets sent to: • IPv4 address with Prefix from 0 to 32 • IPv6 address with Prefix from 0 to 128 ■ `cc:<Country Code>` The rule matches the country code to the destination IP addresses assigned to this country, based on the Geo IP database. The two-letter codes are defined in ISO 3166-1 alpha-2. ■ `asn:<Autonomous System Number>` The rule matches the AS number of the organization to the destination IP addresses that are assigned to this organization, based on the Geo IP database. The valid syntax is *ASnnnn*, where *nnnn* is a number unique to the specific organization. **Notes:** ■ Default is: `destination-negated false` ■ The `destination-negated true` will process all destination types except the specified type

Argument	Description
`[service-negated {true | false}] service <Protocol and Port numbers>`	Specifies the Protocol number (see *IANA Protocol Numbers*) and Port number (see *IANA Service Name and Port Number Registry*): ■ `<Protocol>` IP protocol number in the range 1-255 ■ `<Protocol Start>-<Protocol End>` Range of IP protocol numbers ■ `<Protocol>/<Port>` IP protocol number in the range 1-255 and TCP/UDP port number in the range 1-65535 ■ `<Protocol>/<Port Start>-<Port End>` IP protocol number and range of TCP/UDP port numbers from 1 to 65535 **Notes:** ■ Default is: `service-negated false` ■ The `service-negated true` will process all traffic except the traffic with the specified protocols and ports

Argument	Description
`[<Limit 1 Name> <Limit 1 Value>] [<Limit 2 Name> <Limit 2 Value>] ... [<Limit N Name> <Limit N Value>]`	Specifies quota limits and their values. **Note** - Separate multiple quota limits with spaces. ■ `concurrent-conns <Value>` Specifies the maximal number of concurrent active connections that match this rule. ■ `concurrent-conns-ratio <Value>` Specifies the maximal ratio of the *concurrent-conns* value to the total number of active connections through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`). ■ `pkt-rate <Value>` Specifies the maximum number of packets per second that match this rule. ■ `pkt-rate-ratio <Value>` Specifies the maximal ratio of the *pkt-rate* value to the rate of all connections through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`). ■ `byte-rate <Value>` Specifies the maximal total number of bytes per second in packets that match this rule. ■ `byte-rate-ratio <Value>` Specifies the maximal ratio of the *byte-rate* value to the bytes per second rate of all connections through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`). ■ `new-conn-rate <Value>` Specifies the maximal number of connections per second that match the rule. ■ `new-conn-rate-ratio <Value>` Specifies the maximal ratio of the *new-conn-rate* value to the rate of all connections per second through the Security Gateway, expressed in parts per 65536 (formula: `N / 65536`).

Argument	Description
`[track <Track>]`	Specifies the tracking option: ■ `source` Counts connections, packets, and bytes for specific source IP address, and not cumulatively for this rule. ■ `source-service` Counts connections, packets, and bytes for specific source IP address, and for specific IP protocol and destination port, and not cumulatively for this rule.

Examples

Example 1 - Rate Limiting rule with a range

```
fw sam_policy add -a d -l r -t 3600 quota service any source range:172.16.7.11-172.16.7.13 new-conn-rate 5 flush true
```

Explanations:

- This rule drops packets for all connections (`-a d`) that exceed the quota set by this rule, including packets for existing connections.
- This rule logs packets (`-l r`) that exceed the quota set by this rule.
- This rule will expire in 3600 seconds (`-t 3600`).
- This rule limits the rate of creation of new connections to 5 connections per second (`new-conn-rate 5`) for any traffic (`service any`) from the source IP addresses in the range 172.16.7.11 - 172.16.7.13 (`source range:172.16.7.11-172.16.7.13`).

  Note - The limit of the total number of log entries per second is configured with the *fwaccel dos config set -n <rate>* command.
- This rule will be compiled and loaded on the SecureXL, together with other rules in the Suspicious Activity Monitoring (SAM) policy database immediately, because this rule includes the "`flush true`" parameter.

Example 2 - Rate Limiting rule with a service specification

```
fw sam_policy add -a n -l r quota service 1,50-51,6/443,17/53 service-negated true source cc:QQ byte-rate 0
```

Explanations:

- This rule logs and lets through all packets (`-a n`) that exceed the quota set by this rule.
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to all packets except (`service-negated true`) the packets with IP protocol number 1, 50-51, 6 port 443 and 17 port 53 (`service 1,50-51,6/443,17/53`).
- This rule applies to all packets from source IP addresses that are assigned to the country with specified country code (`cc:QQ`).
- This rule does not let any traffic through (`byte-rate 0`) except the packets with IP protocol number 1, 50-51, 6 port 443 and 17 port 53.
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

Example 3 - Rate Limiting rule with ASN

```
fw sam_policy -a d quota source asn:AS64500,cidr:[::FFFF:C0A8:1100]/120 service any pkt-rate 0
```

Explanations:

- This rule drops (`-a d`) all packets that match this rule.
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to packets from the Autonomous System number 64500 (`asn:AS64500`).
- This rule applies to packets from source IPv6 addresses FFFF:C0A8:1100/120 (`cidr:[::FFFF:C0A8:1100]/120`).
- This rule applies to all traffic (`service any`).
- This rule does not let any traffic through (`pkt-rate 0`).
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

Example 4 - Rate Limiting rule with an Allow List

```
fw sam_policy add -a b quota source range:172.16.8.17-172.16.9.121 service 6/80
```

Explanations:

- This rule bypasses (`-a b`) all packets that match this rule.

  Note - The Access Control Policy and other types of security policy rules still apply.
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to packets from the source IP addresses in the range 172.16.8.17 - 172.16.9.121 (`range:172.16.8.17-172.16.9.121`).
- This rule applies to packets sent to TCP port 80 (`service 6/80`).
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

Example 5 - Rate Limiting rule with tracking

```
fw sam_policy add -a d quota service any source-negated true source cc:QQ concurrent-conns-ratio 655 track source
```

Explanations:

- This rule drops (`-a d`) all packets that match this rule.
- This rule does not log any packets (the `-l r` parameter is not specified).
- This rule does not expire (the `timeout` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule applies to all traffic (`service any`).
- This rule applies to all sources except (`source-negated true`) the source IP addresses that are assigned to the country with specified country code (`cc:QQ`).
- This rule limits the maximal number of concurrent active connections to 655/65536=~1% (`concurrent-conns-ratio 655`) for any traffic (`service any`) except (`service-negated true`) the connections from the source IP addresses that are assigned to the country with specified country code (`cc:QQ`).
- This rule counts connections, packets, and bytes for traffic only from sources that match this rule, and not cumulatively for this rule.
- This rule will not be compiled and installed on the SecureXL immediately, because it does not include the "`flush true`" parameter.

fw sam_policy batch

Description

The "*fw sam_policy batch*" and "*fw6 sam_policy batch*" commands:

- Add and delete many Suspicious Activity Monitoring (SAM) rules at a time.
- Add and delete many Rate Limiting rules at a time.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Procedure

1. **Start the batch mode**

   - For IPv4, run:

     ```
     fw sam_policy batch << EOF
     ```

   - For IPv6, run:

     ```
     fw6 sam_policy batch << EOF
     ```

2. **Enter the applicable commands**

   - Enter one "`add`" or "`del`" command on each line, on as many lines as necessary.

     Start each line with only "`add`" or "`del`" parameter (not with "`fw samp`").
   - Use the same set of parameters and values as described in these commands:
     - `fw sam_policy add`
     - `fw sam_policy del`
   - Terminate each line with a Return (ASCII 10 - Line Feed) character (press Enter).

3. **End the batch mode**

   Type `EOF` and press Enter.

Example of a Rate Limiting rule for IPv4

```
[Expert@HostName]# fw samp batch <<EOF

add -a d -l r -t 3600 -c "Limit\ conn\ rate\ to\ 5\ conn/sec from\ these\ sources" quota service
any source range:172.16.7.13-172.16.7.13 new-conn-rate 5

del <501f6ef0,00000000,cb38a8c0,0a0afffe>

add -a b quota source range:172.16.8.17-172.16.9.121 service 6/80

EOF
[Expert@HostName]#
```

fw sam_policy del

Description

The "*fw sam_policy del*" and "*fw6 sam_policy del*" commands:

- Delete one configured Suspicious Activity Monitoring (SAM) rule at a time.
- Delete one configured Rate Limiting rule at a time.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax for IPv4

```
fw [-d] sam_policy del '<Rule UID>'
```

Syntax for IPv6

```
fw6 [-d] sam_policy del '<Rule UID>'
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`'<Rule UID>'`	Specifies the UID of the rule you wish to delete. **Important:** ■ The quote marks and angle brackets (`'<...>'`) are mandatory. ■ To see the Rule UID, run the "`fw sam_policy get`" command.

Procedure

1. **List all the existing rules in the Suspicious Activity Monitoring policy database**

   List all the existing rules in the Suspicious Activity Monitoring policy database.

   - For IPv4, run:

     ```
     fw sam_policy get
     ```

   - For IPv6, run:

     ```
     fw6 sam_policy get
     ```

   The rules show in this format:

   ```
   operation=add uid=<Value1,Value2,Value3,Value4> target=...
   timeout=... action=... log= ... name= ... comment=...
   originator= ... src_ip_addr=... req_tpe=...
   ```

   Example for IPv4:

   ```
   operation=add uid=<5ac3965f,00000000,3403a8c0,0000264a>
   target=all timeout=300 action=notify log=log name=Test\ Rule
   comment=Notify\ about\ traffic\ from\ 1.1.1.1
   originator=John\ Doe src_ip_addr=1.1.1.1 req_tpe=ip
   ```

2. **Delete a rule from the list by its UID**

   - For IPv4, run:

     ```
     fw [-d] sam_policy del '<Rule UID>'
     ```

   - For IPv6, run:

     ```
     fw6 [-d] sam_policy del '<Rule UID>'
     ```

   Example for IPv4:

   ```
   fw samp del '<5ac3965f,00000000,3403a8c0,0000264a>'
   ```

3. **Add the flush-only rule**

   - For IPv4, run:

     ```
     fw samp add -t 2 quota flush true
     ```

   - For IPv6, run:

     ```
     fw6 samp add -t 2 quota flush true
     ```

   Explanation:

   The "`fw samp del`" and "`fw6 samp del`" commands only remove a rule from the persistent database. The Security Gateway continues to enforce the deleted rule until the next time you compiled and load a policy. To force the rule deletion immediately, you must enter a flush-only rule right after the "`fw samp del`" and "`fw6 samp del`" command. This flush-only rule immediately deletes the rule you specified in the previous step, and times out in 2 seconds.

   Best Practice - Specify a short timeout period for the flush-only rules. This prevents accumulation of rules that are obsolete in the database.

fw sam_policy get

Description

The "*fw sam_policy get*" and "*fw6 sam_policy get*" commands:

- Show all the configured Suspicious Activity Monitoring (SAM) rules.
- Show all the configured Rate Limiting rules.

Notes:

- These commands are interchangeable:
  - For IPv4: "`fw sam_policy`" and "`fw samp`".
  - For IPv6: "`fw6 sam_policy`" and "`fw6 samp`".
- You can run these commands in Gaia Clish, or Expert mode.
- Security Gateway stores the SAM Policy rules in the `$FWDIR/database/sam_policy.db` file.
- Security Gateway stores the SAM Policy management settings in the `$FWDIR/database/sam_policy.mng` file.

Important:

- Configuration you make with these commands, survives reboot.
- VSX mode does **not** support Suspicious Activity Policy configured in SmartView Monitor. See sk79700.
- In VSX mode, you must go to the context of an applicable Virtual System.
  - In Gaia Clish, run: `set virtual-system <VSID>`
  - In the Expert mode, run: `vsenv <VSID>`
- In a Cluster, you must configure all the Cluster Members in the same way.

Best Practice - The SAM Policy rules consume some CPU resources on Security Gateway. Set an expiration for rules that gives you time to investigate, but does not affect performance. Keep only the required SAM Policy rules. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

Syntax for IPv4

```
fw [-d] sam_policy get [-l] [-u '<Rule UID>'] [-k '<Key>' -t
<Type> [+{-v '<Value>'}] [-n]]
```

Syntax for IPv6

```
fw6 [-d] sam_policy get [-l] [-u '<Rule UID>'] [-k '<Key>' -t
<Type> [+{-v '<Value>'}] [-n]]
```

Parameters

Note - All these parameters are optional.

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-l`	Controls how to print the rules: ■ In the default format (without "`-l`"), the output shows each rule on a separate line. ■ In the list format (with "`-l`"), the output shows each parameter of a rule on a separate line. ■ See the "`fw sam_policy add`" command.
`-u '<`*`Rule UID`*`>'`	Prints the rule specified by its Rule UID or its zero-based rule index. The quote marks and angle brackets ('<...>') are mandatory.
`-k '<`*`Key`*`>'`	Prints the rules with the specified predicate key. The quote marks are mandatory.
`-t <`*`Type`*`>`	Prints the rules with the specified predicate type. For Rate Limiting rules, you must always use "`-t in`".
`+{-v '<`*`Value`*`>'}`	Prints the rules with the specified predicate values. The quote marks are mandatory.
`-n`	Negates the condition specified by these predicate parameters: ■ `-k` ■ `-t` ■ `+-v`

Examples

Example 1 - Output in the default format

```
[Expert@HostName:0]# fw samp get

operation=add uid=<5ac3965f,00000000,3403a8c0,0000264a> target=all timeout=300 action=notify
log=log name=Test\ Rule comment=Notify\ about\ traffic\ from\ 1.1.1.1 originator=John\ Doe
src_ip_addr=1.1.1.1 req_tpe=ip
```

Example 2 - Output in the list format

```
[Expert@HostName:0]# fw samp get -l

uid
<5ac3965f,00000000,3403a8c0,0000264a>
target
all
timeout
2147483647
action
notify
log
log
name
Test\ Rule
comment
Notify\ about\ traffic\ from\ 1.1.1.1
originator
John\ Doe
src_ip_addr
1.1.1.1
req_type
ip
```

Example 3 - Printing a rule by its Rule UID

```
[Expert@HostName:0]# fw samp get -u '<5ac3965f,00000000,3403a8c0,0000264a>'
0
operation=add uid=<5ac3965f,00000000,3403a8c0,0000264a> target=all timeout=300 action=notify
log=log name=Test\ Rule comment=Notify\ about\ traffic\ from\ 1.1.1.1 originator=John\ Doe
src_ip_addr=1.1.1.1 req_tpe=ip
```

Example 4 - Printing rules that match the specified filters

```
[Expert@HostName:0]# fw samp get
no corresponding SAM policy requests
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a d -l r -t 3600 quota service any source
range:172.16.7.11-172.16.7.13 new-conn-rate 5 flush true
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a n -l r quota service 1,50-51,6/443,17/53 service-negated
true source cc:QQ byte-rate 0
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a b quota source range:172.16.8.17-172.16.9.121 service
6/80
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp add -a d quota service any source-negated true source cc:QQ
concurrent-conns-ratio 655 track source
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get
operation=add uid=<5bab3acf,00000000,3503a8c0,00003ddc> target=all timeout=indefinite
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
operation=add uid=<5bab3ac6,00000000,3503a8c0,00003dbf> target=all timeout=3586 action=drop
log=log service=any source=range:172.16.7.11-172.16.7.13 new-conn-rate=5 flush=true req_
type=quota
operation=add uid=<5bab3acc,00000000,3503a8c0,00003dd7> target=all timeout=indefinite
action=bypass source=range:172.16.8.17-172.16.9.121 service=6/80 req_type=quota
operation=add uid=<5bab3ac9,00000000,3503a8c0,00003dd5> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'service' -t in -v '6/80'
operation=add uid=<5bab3acc,00000000,3503a8c0,00003dd7> target=all timeout=indefinite
action=bypass source=range:172.16.8.17-172.16.9.121 service=6/80 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'service-negated' -t in -v 'true'
operation=add uid=<5bab3ac9,00000000,3503a8c0,00003dd5> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'source' -t in -v 'cc:QQ'
operation=add uid=<5bab3acf,00000000,3503a8c0,00003ddc> target=all timeout=indefinite
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
operation=add uid=<5bab3ac9,00000000,3503a8c0,00003dd5> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k source -t in -v 'cc:QQ' -n
operation=add uid=<5bab3ac6,00000000,3503a8c0,00003dbf> target=all timeout=3291 action=drop
log=log service=any source=range:172.16.7.11-172.16.7.13 new-conn-rate=5 flush=true req_
type=quota
operation=add uid=<5bab3acc,00000000,3503a8c0,00003dd7> target=all timeout=indefinite
action=bypass source=range:172.16.8.17-172.16.9.121 service=6/80 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'source-negated' -t in -v 'true'
operation=add uid=<5baa94e0,00000000,860318ac,00003016> target=all timeout=indefinite
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'byte-rate' -t in -v '0'
operation=add uid=<5baa9431,00000000,860318ac,00002efd> target=all timeout=indefinite
action=notify log=log service=1,50-51,6/443,17/53 service-negated=true source=cc:QQ byte-
rate=0 req_type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'flush' -t in -v 'true'
operation=add uid=<5baa9422,00000000,860318ac,00002eea> target=all timeout=2841 action=drop
log=log service=any source=range:172.16.7.11-172.16.7.13 new-conn-rate=5 flush=true req_
type=quota
[Expert@HostName:0]#
[Expert@HostName:0]# fw samp get -k 'concurrent-conns-ratio' -t in -v '655'
operation=add uid=<5baa94e0,00000000,860318ac,00003016> target=all timeout=indefinite
```

```
action=drop service=any source-negated=true source=cc:QQ concurrent-conns-ratio=655
track=source req_type=quota
[Expert@HostName:0]#
```

The /proc/ppk/ and /proc/ppk6/ entries

Description

SecureXL supports Linux **/proc** entries. The read-only entries in the **/proc/ppk/** and **/proc/ppk6/** contain various data about SecureXL.

Syntax for IPv4

```
[Expert@MyGW:0]# ls -lR /proc/ppk/
[Expert@MyGW:0]# cat /proc/ppk/<Name of File>
[Expert@MyGW:0]# cat /proc/ppk/<SecureXL Instance ID>/<Name of File>
```

Syntax for IPv6

```
[Expert@MyGW:0]# ls -lR /proc/ppk6/
[Expert@MyGW:0]# cat /proc/ppk6/<Name of File>
[Expert@MyGW:0]# cat /proc/ppk6/<SecureXL Instance ID>/<Name of File>
```

Files

File	Description
`affinity`	Contains status and the thresholds for SecureXL New Affinity mechanism. See *"/proc/ppk/affinity" on page 1556*.
`conf`	Contains the SecureXL configuration and basic statistics. See *"/proc/ppk/conf" on page 1557*.
`conns`	Contains the list of the SecureXL connections. See *"/proc/ppk/conns" on page 1558*.
`cpls`	Contains SecureXL configuration for ClusterXL Load Sharing (CPLS). See *"/proc/ppk/cpls" on page 1559*.
`cqstats`	Contains statistics for SecureXL connections queue. See *"/proc/ppk/cqstats" on page 1560*.

File	Description
`drop_ statistics`	Contains SecureXL statistics for dropped packets. See *"/proc/ppk/drop_statistics" on page 1561*.
`ifs`	Contains the list of interfaces that SecureXL uses. See *"/proc/ppk/ifs" on page 1562*.
`mcast_ statistics`	Contains SecureXL statistics for multicast traffic. See *"/proc/ppk/mcast_statistics" on page 1567*.
`nac`	Contains SecureXL statistics for Identity Awareness Network Access Control (NAC) traffic. See *"/proc/ppk/nac" on page 1568*.
`notify_ statistics`	Contains SecureXL statistics for notifications SecureXL sent to Firewall about accelerated connections. See *"/proc/ppk/notify_statistics" on page 1569*.
`profile_ cpu_stat`	Contains IDs of the CPU cores and status of Traffic Profiling See *"/proc/ppk/profile_cpu_stat" on page 1571*.
`rlc`	Contains SecureXL statistics for drops due to Rate Limiting for DoS Mitigation. See *"/proc/ppk/rlc" on page 1572*.
`statistics`	Contains SecureXL overall statistics. See *"/proc/ppk/statistics" on page 1573*.
`stats`	Contains the IRQ numbers and names of interfaces the SecureXL uses. See *"/proc/ppk/stats" on page 1575*.
`viol_ statistics`	Contains SecureXL statistics for violations - packets SecureXL forwarded (F2F) to the Firewall. See *"/proc/ppk/viol_statistics" on page 1576*.

/proc/ppk/affinity

Description

Contains the number of accelerated packets per second and rate of encrypted bytes.

Syntax for IPv4

```
[Expert@MyGW:0]# ls -lR /proc/ppk/
[Expert@MyGW:0]# cat /proc/ppk/affinity
```

Syntax for IPv6

```
[Expert@MyGW:0]# ls -lR /proc/ppk6/
[Expert@MyGW:0]# cat /proc/ppk6/affinity
```

Example for IPv4

```
[Expert@MyGW:0]# cat /proc/ppk/affinity
Current accelerated PPS        : 0
Current enc. bytes rate        : 0
[Expert@MyGW:0]#
```

/proc/ppk/conf

Description

Contains the SecureXL configuration and basic statistics.

Syntax for IPv4

```
[Expert@MyGW:0]# ls -lR /proc/ppk/
[Expert@MyGW:0]# cat /proc/ppk/conf
[Expert@MyGW:0]# cat /proc/ppk/<SecureXL Instance ID>/conf
```

Syntax for IPv6

```
[Expert@MyGW:0]# ls -lR /proc/ppk6/
[Expert@MyGW:0]# cat /proc/ppk6/conf
[Expert@MyGW:0]# cat /proc/ppk6/<SecureXL Instance ID>/conf
```

Example for IPv4

```
[Expert@MyGW:0]# cat /proc/ppk/conf
Flags                          : 0x00000592
Accounting Update Interval     : 3600
Conn Refresh Interval          : 512
SA Sync Notification Interval  : 200000
UDP Encapsulation Port         : 2746
Min TCP MSS                    : 0
TCP End Timeout                : 5
Connection Limit               : 18446744073709551615

Total Number of conns          : 0
Number of Crypt conns          : 0
Number of TCP conns            : 0
Number of Non-TCP conns        : 0
Total Number of corrs          : 0

Debug flags :
 0      : 0x1
 1      : 0x1
 2      : 0x1
 3      : 0x1
 4      : 0x1
 5      : 0x1
 6      : 0x1
 7      : 0x1
 8      : 0x100
 9      : 0x8
 10      : 0x1
 11      : 0x10
[Expert@MyGW:0]#
```

/proc/ppk/conns

Description

Contains the list of the SecureXL connections.

Important - This file is for future use. Refer to the *"fwaccel conns" on page 1408* command.

Syntax for IPv4

```
[Expert@MyGW:0]# ls -lR /proc/ppk/
[Expert@MyGW:0]# cat /proc/ppk/conns
[Expert@MyGW:0]# cat /proc/ppk/<SecureXL Instance ID>/conns
```

Syntax for IPv6

```
[Expert@MyGW:0]# ls -lR /proc/ppk6/
[Expert@MyGW:0]# cat /proc/ppk6/conns
[Expert@MyGW:0]# cat /proc/ppk6/<SecureXL Instance ID>/conns
```

/proc/ppk/cpls

Description

Contains SecureXL configuration for ClusterXL Load Sharing (CPLS).

Important - This file is for future use. Refer to the "`fwaccel cfg -h`" command (see *"fwaccel cfg" on page 1404*).

Syntax for IPv4

```
[Expert@MyGW:0]# ls -lR /proc/ppk/
[Expert@MyGW:0]# cat /proc/ppk/cpls
```

Syntax for IPv6

```
[Expert@MyGW:0]# ls -lR /proc/ppk6/
[Expert@MyGW:0]# cat /proc/ppk6/cpls
```

Example for IPv4

```
[Expert@MyGW:0]# cat /proc/ppk/cpls
fwha_conf_flags: 638
fwha_df_type: 0
fwha_member_id: 0
fwha_port: 8116
FWHAP MAC magic: 0
Forwarding MAC magic: 0
My state: ACTIVE
udp_enc_port: 0
selection table size: 0
[Expert@MyGW:0]#
```

/proc/ppk/cqstats

Description

Contains statistics for SecureXL connections queue.

Syntax for IPv4

```
[Expert@MyGW:0]# ls -lR /proc/ppk/
[Expert@MyGW:0]# cat /proc/ppk/cqstats
[Expert@MyGW:0]# cat /proc/ppk/<SecureXL Instance ID>/cqstats
```

Syntax for IPv6

```
[Expert@MyGW:0]# ls -lR /proc/ppk6/
[Expert@MyGW:0]# cat /proc/ppk6/cqstats
[Expert@MyGW:0]# cat /proc/ppk6/<SecureXL Instance ID>/cqstats
```

Example for IPv4

```
[Expert@MyGW:0]# cat /proc/ppk/cqstats
Name                   Value              Name                    Value
--------------------  ---------------    --------------------  ---------------
Queued pkts                           0    Queue fail                         0
Dequeue & f2f                         0    Dequeue & drop                     0
Dequeue & resume                      0    Async index req                    0
Err Async index req                   0    Async index cb                     0
Err Async index cb                    0    Queue alloc fail                   0
Queue empty err                       0
[Expert@MyGW:0]#
```

/proc/ppk/drop_statistics

Description

Contains SecureXL statistics for dropped packets.

Note - This is the same information that the "`fwaccel stats -d`" command shows (see *"fwaccel stats" on page 1473*).

Syntax for IPv4

```
[Expert@MyGW:0]# ls -lR /proc/ppk/
```

```
[Expert@MyGW:0]# cat /proc/ppk/drop_statistics
```

```
[Expert@MyGW:0]# cat /proc/ppk/<SecureXL Instance ID>/drop_
statistics
```

Syntax for IPv6

```
[Expert@MyGW:0]# ls -lR /proc/ppk6/
```

```
[Expert@MyGW:0]# cat /proc/ppk6/drop_statistics
```

```
[Expert@MyGW:0]# cat /proc/ppk6/<SecureXL Instance ID>/drop_
statistics
```

Example for IPv4

```
[Expert@MyGW:0]# cat /proc/ppk/drop_statistics
Reason                Packets            Reason                Packets
--------------------  ---------------    --------------------  ---------------
general reason                     0     CPASXL decision                    0
PSLXL decision                     0     clr pkt on vpn                     0
encrypt failed                     0     drop template                      0
decrypt failed                     0     interface down                     0
cluster error                      0     XMT error                          0
anti spoofing                      0     local spoofing                     0
sanity error                       0     monitored spoofed                  0
QOS decision                       0     C2S violation                      0
S2C violation                      0     Loop prevention                    0
DOS Fragments                      0     DOS IP Options                     0
DOS Blacklists                     0     DOS Penalty Box                    0
DOS Rate Limiting                  0     Syn Attack                         0
Reorder                            0     Defrag timeout                     0
[Expert@MyGW:0]#
```

/proc/ppk/ifs

Description

Contains the list of interfaces that SecureXL uses.

Syntax for IPv4

```
[Expert@MyGW:0]# ls -lR /proc/ppk/
```

```
[Expert@MyGW:0]# cat /proc/ppk/ifs
```

Syntax for IPv6

```
[Expert@MyGW:0]# ls -lR /proc/ppk6/
```

```
[Expert@MyGW:0]# cat /proc/ppk6/ifs
```

Example for IPv4

```
[Expert@MyGW:0]# cat /proc/ppk/ifs
 No | Interface | Address         | IRQ | F   | SIM F | Dev                | Output Func
| Features
-------------------------------------------------------------------------------------------------
-------------
  2 | eth0      |    192.168.3.52 |  67 |   1 |   480 | 0xffff81023e5df000 | 0x000013a0
  3 | eth1      |     10.20.30.52 |  83 |   1 |   488 | 0xffff81023dd0c000 | 0x000013a0
  4 | eth2      |     40.50.60.52 |  59 |   1 |   480 | 0xffff810237f88000 | 0x000013a0
  5 | eth3      |         0.0.0.0 |  67 |   1 |    80 | 0xffff810239b3d000 | 0x000013a0
  6 | eth4      |         0.0.0.0 |  91 |   1 |    80 | 0xffff81023841f000 | 0x000013a0
  7 | eth5      |         0.0.0.0 |  83 |   1 |   480 | 0xffff8102396fe000 | 0x000013a0
  8 | eth6      |         0.0.0.0 |  59 |   1 |   480 | 0xffff810239a4d000 | 0x000013a0
 10 | bond0     |     70.80.90.52 |   0 |   1 |   280 | 0xffff8101f1a0e000 | 0x000013a0
[Expert@MyGW:0]#
```

Example for IPv6

```
[Expert@MyGW:0]# cat /proc/ppk6/ifs
  No | Interface | Address         | IRQ | F   | SIM F | Dev                | Output Func
| Features
-------------------------------------------------------------------------------------------------------
-------------
  2 | eth0      |           fe80:0:0:0:250:56ff:fea3:1807 |  67 |   1 |   480 |
0xffff81023e5df000 | 0x000013a0
  3 | eth1      |           fe80:0:0:0:250:56ff:fea3:15a4 |  83 |   1 |   480 |
0xffff81023dd0c000 | 0x000013a0
  4 | eth2      |           fe80:0:0:0:250:56ff:fea3:2f50 |  59 |   1 |   480 |
0xffff810237f88000 | 0x000013a0
  5 | eth3      |                         0:0:0:0:0:0:0:0 |  67 |   1 |    80 |
0xffff810239b3d000 | 0x000013a0
  6 | eth4      |                         0:0:0:0:0:0:0:0 |  91 |   1 |    80 |
0xffff81023841f000 | 0x000013a0
  7 | eth5      |           fe80:0:0:0:250:56ff:fea3:75a9 |  83 |   1 |   480 |
0xffff8102396fe000 | 0x000013a0
  8 | eth6      |           fe80:0:0:0:250:56ff:fea3:5d4c |  59 |   1 |   480 |
0xffff810239a4d000 | 0x000013a0
 10 | bond0     |           fe80:0:0:0:250:56ff:fea3:287b |   0 |   1 |   280 |
0xffff8101f1a0e000 | 0x000013a0
[Expert@MyGW:0]#
```

Explanation about the configuration flags in the "F" and "SIM F" columns

The "**F**" column shows the internal configuration flags that Firewall set on these interfaces.

The "**SIM F**" column shows the internal configuration flags that SecureXL set on these interfaces.

Flag	Description
0x001	If this flag is set, the SecureXL drops the packet at the end of the inbound inspection, if the packet is a "cut-through" packet. In outbound, SecureXL forwards all the packets to the network.
0x002	If this flag is set, the SecureXL sends an applicable notification when a TCP state change occurs (connection is established or torn down).
0x004	If this flag is set, the SecureXL it sets the UDP header's checksum field correctly when the SecureXL encapsulates an encrypted packet (UDP encapsulation). If this flag is not set, SecureXL sets the UDP header's checksum field to zero. It is safe to ignore this flag, if it is set to 0 (SecureXL continues to calculate the UDP packet's checksum).
0x008	If this flag is set, the SecureXL does not create new connections that match a template, and SecureXL drops the packet that matches the template, when the number of entries in the Connections Table reaches the specified limit. If this flag is not set, the SecureXL forwards the packet to the Firewall.

Flag	Description
0x010	If this flag is set, the SecureXL forwards fragments to the Firewall.
0x020	If this flag is set, the SecureXL does not create connections from TCP templates anymore. The Firewall offloads connections to SecureXL when necessary. This flag only disables the creation of TCP templates.
0x040	If this flag is set, the SecureXL notifies the Firewall at intervals, so it refreshes the accelerated connections in the Firewall kernel tables.
0x080	If this flag is set, the SecureXL does not create connections from non-TCP templates anymore. The Firewall offloads connections to SecureXL when necessary. This flag only disables the creation of non-TCP templates.
0x100	If this flag is set, the SecureXL allows sequence verification violations for connections that did not complete the TCP 3-way handshake process. If this flag is not set, SecureXL must forward the violating packets to the Firewall.
0x200	If this flag is set, the SecureXL allows sequence verification violations for connections that completed the TCP 3-way handshake process. If this flag is not set, SecureXL must forward the violating packets to the Firewall.
0x400	If this flag is set, the SecureXL forwards TCP [RST] packets to the Firewall.
0x0001	If this flag is set, the SecureXL notifies the Firewall about HitCount data.
0x0002	If this flag is set, the VSX Virtual System works as a junction, rather than a regular Virtual System (only the local Virtual System flag is applicable).
0x0004	If this flag is set, the SecureXL disables the reply counter of inbound encrypted traffic. At a result, SecureXL kernel module works in the same way as the VPN kernel module.
0x0008	If this flag is set, the SecureXL enables the MSS Clamping. Refer to the kernel parameters "`fw_clamp_tcp_mss`" and "`fw_clamp_vpn_mss`" in sk101219.
0x0010	If this flag is set, the SecureXL disables the "No Match Ranges" (NMR) Templates (see sk117755).

Flag	Description
0x0020	If this flag is set, the SecureXL disables the "No Match Time" (NMT) Templates (see sk117755).
0x0040	If this flag is set, the SecureXL does not send Drop Templates notifications about dropped packets to the Firewall (to update the drop counters). For example, if you set the value of the kernel parameter "`activate_optimize_drops_support_now`" to 1, it disables the Drop Templates notifications.
0x0080	If this flag is set, the SecureXL enables the MultiCore support for IPSec VPN (see sk118097).
0x0100	If this flag is set, the SecureXL enables the support for CoreXL Dynamic Dispatcher (see sk105261).
0x0800	If this flag is set, the SecureXL does not enforce the Path MTU Discovery for IP multicast packets.
0x1000	If this flag is set, the SecureXL disables the SIM "drop_templates" feature.
0x2000	If this flag is set, it indicates that an administrator enabled the Link Selection Load Sharing feature.
0x4000	If this flag is set, the SecureXL disables the asynchronous notification feature.
0x8000	If this flag is set, it indicates that the capacity of the Firewall Connections Table is unlimited.

Examples:

Value	Description
0x039	Means the sum of these flags: ■ 0x001 ■ 0x008 ■ 0x010 ■ 0x020
0x00008a16	Means the sum of these flags: ■ 0x0002 ■ 0x0004 ■ 0x0010 ■ 0x0200 ■ 0x0800 ■ 0x8000
0x00009a16	Means the sum of these flags: ■ 0x0002 ■ 0x0004 ■ 0x0010 ■ 0x0200 ■ 0x0800 ■ 0x1000 ■ 0x8000

/proc/ppk/mcast_statistics

Description

Contains SecureXL statistics for multicast traffic.

Note - This is the same information that the "`fwaccel stats -m`" command shows (see *"fwaccel stats" on page 1473*).

Syntax for IPv4

```
[Expert@MyGW:0]# ls -lR /proc/ppk/
```

```
[Expert@MyGW:0]# cat /proc/ppk/mcast_statistics
```

```
[Expert@MyGW:0]# cat /proc/ppk/<SecureXL Instance ID>/mcast_
statistics
```

Syntax for IPv6

```
[Expert@MyGW:0]# ls -lR /proc/ppk6/
```

```
[Expert@MyGW:0]# cat /proc/ppk6/mcast_statistics
```

```
[Expert@MyGW:0]# cat /proc/ppk6/<SecureXL Instance ID>/mcast_
statistics
```

Example for IPv4

```
[Expert@MyGW:0]# cat /proc/ppk/mcast_statistics
Name                 Value              Name                  Value
-------------------  ---------------    --------------------  ---------------
in packets                       10100    out packets                        0
if restricted                        0    conns with down if                 0
f2f packets                          0    f2f bytes                          0
dropped packets                      0    dropped bytes                      0
accel packets                        0    accel bytes                        0
mcast conns                          0
[Expert@MyGW:0]#
```

/proc/ppk/nac

Description

Contains SecureXL statistics for Identity Awareness Network Access Control (NAC) traffic.

Note - This is the same information that the "`fwaccel stats -n`" command shows (see *"fwaccel stats" on page 1473*).

Syntax for IPv4

```
[Expert@MyGW:0]# ls -lR /proc/ppk/
[Expert@MyGW:0]# cat /proc/ppk/nac
[Expert@MyGW:0]# cat /proc/ppk/<SecureXL Instance ID>/nac
```

Syntax for IPv6

```
[Expert@MyGW:0]# ls -lR /proc/ppk6/
[Expert@MyGW:0]# cat /proc/ppk6/nac
[Expert@MyGW:0]# cat /proc/ppk6/<SecureXL Instance ID>/nac
```

Example for IPv4

```
[Expert@MyGW:0]# cat /proc/ppk/nac
Name                  Value              Name                    Value
--------------------  ---------------    --------------------  ---------------
NAC packets                          0    NAC bytes                           0
NAC connections                      0    complience failure                  0
[Expert@MyGW:0]#
```

/proc/ppk/notify_statistics

Description

Contains SecureXL statistics for notifications SecureXL sent to Firewall about accelerated connections.

Syntax for IPv4

```
[Expert@MyGW:0]# ls -lR /proc/ppk/
```

```
[Expert@MyGW:0]# cat /proc/ppk/notify_statistics
```

```
[Expert@MyGW:0]# cat /proc/ppk/<SecureXL Instance ID>/notify_
statistics
```

Syntax for IPv6

```
[Expert@MyGW:0]# ls -lR /proc/ppk6/
```

```
[Expert@MyGW:0]# cat /proc/ppk6/notify_statistics
```

```
[Expert@MyGW:0]# cat /proc/ppk6/<SecureXL Instance ID>/notify_
statistics
```

Example for IPv4

```
[Expert@MyGW:0]# cat /proc/ppk/notify_statistics
Notification           Packets           Notification           Packets
--------------------  --------------    --------------------  --------------
ntSAAboutToExpire                 0    ntSAExpired                         0
ntMSPIError                       0    ntNoInboundSA                       0
ntNoOutboundSA                    0    ntDataIntegrityFailed               0
ntPossibleReplay                  0    ntReplay                            0
ntNextProtocolError               0    ntCPIError                          0
ntClearTextPacket                 0    ntFragmentation                     0
ntUpdateUdpEncTable               0    ntSASync                            0
ntReplayOutOfWindow               0    ntVPNTrafficReport                  0
ntConnDeleted                     0    ntConnUpdate                        0
ntPacketDropped                   0    ntSendLog                           0
ntRefreshGTPTunnel                0    ntMcastDrop                         0
ntAccounting                      0    ntAsyncIndex                        0
ntACkReordering                   0    ntAccelAckInfo                      0
ntMonitorPacket                   0    ntPacketCapture                     0
ntCpasPacketCapture               0    ntPSLGlueUpdateReject               0
ntSeqVerifyDrop                   0    ntPacketForwardBefore               0
ntICMPMessage                     0    ntQoSReclassifyPacket               0
ntQoSResumePacket                 0    ntVPNEncHaLinkFailure               0
ntVPNEncLsLinkFailure             0    ntVPNEncRouteChange                 0
ntVPNDecVerRouteChang             0    ntVPNDecRouteChange                 0
ntMuxSimToFw                      0    ntPSLEventLog                       0
ntSendCPHWDStats              39375    ntPacketTaggingViolat               0
ntDosNotify                       0    ntSynatkNotify                      0
ntSynatkStats                     0    ntQoSEventLog                       0
ntPrintGetParam                   0
[Expert@MyGW:0]#
```

/proc/ppk/profile_cpu_stat

Description

This file is for Check Point use only.

Contains IDs of the CPU cores and status of Traffic Profiling:

- The first column shows the IDs of the CPU cores.
- The second column shows the status of Traffic Profiling for the applicable CPU core.

Syntax for IPv4

```
[Expert@MyGW:0]# ls -lR /proc/ppk/
```

```
[Expert@MyGW:0]# cat /proc/ppk/profile_cpu_stat
```

```
[Expert@MyGW:0]# cat /proc/ppk/<SecureXL Instance ID>/profile_cpu_
stat
```

Syntax for IPv6

```
[Expert@MyGW:0]# ls -lR /proc/ppk6/
```

```
[Expert@MyGW:0]# cat /proc/ppk6/profile_cpu_stat
```

```
[Expert@MyGW:0]# cat /proc/ppk6/<SecureXL Instance ID>/profile_
cpu_stat
```

Example for IPv4 from a Security Gateway with 4 CPU cores

```
[Expert@MyGW:0]# cat /proc/ppk/profile_cpu_stat
0 0
1 0
2 0
3 0
[Expert@MyGW:0]#
```

/proc/ppk/rlc

Description

Contains SecureXL statistics for drops due to Rate Limiting for DoS Mitigation.

Syntax for IPv4

```
[Expert@MyGW:0]# ls -lR /proc/ppk/
[Expert@MyGW:0]# cat /proc/ppk/rlc
```

Syntax for IPv6

```
[Expert@MyGW:0]# ls -lR /proc/ppk6/
[Expert@MyGW:0]# cat /proc/ppk6/rlc
```

Example for IPv4

```
[Expert@MyGW:0]# cat /proc/ppk/rlc
Total drop packets : 0
Total drop bytes : 0
[Expert@MyGW:0]#
```

/proc/ppk/statistics

Description

Contains SecureXL overall statistics.

To see these statistics in a better way, run the *"fwaccel stats" on page 1473* command.

Syntax for IPv4

```
[Expert@MyGW:0]# ls -lR /proc/ppk/
[Expert@MyGW:0]# cat /proc/ppk/statistics
[Expert@MyGW:0]# cat /proc/ppk/<SecureXL Instance ID>/statistics
```

Syntax for IPv6

```
[Expert@MyGW:0]# ls -lR /proc/ppk6/
[Expert@MyGW:0]# cat /proc/ppk6/statistics
[Expert@MyGW:0]# cat /proc/ppk6/<SecureXL Instance ID>/statistics
```

Example for IPv4

```
[Expert@MyGW:0]# cat /proc/ppk/statistics
Name                  Value             Name                  Value
--------------------  ---------------   --------------------  ---------------
accel packets                     0   accel bytes                       0
outbound packets                  0   outbound bytes                    0
conns created                     0   conns deleted                     0
current total conns               0   TCP conns                         0
non TCP conns                     0   nat conns                         0
dropped packets                 728   dropped bytes                107978
fragments received                0   fragments transmit                0
fragments dropped                 0   fragments expired                 0
IP options stripped               0   IP options restored               0
IP options dropped                0   corrs created                     0
corrs deleted                     0   C corrections                     0
corrected packets                 0   corrected bytes                   0
crypt conns                       0   enc bytes                         0
dec bytes                         0   ESP enc pkts                      0
ESP enc err                       0   ESP dec pkts                      0
ESP dec err                       0   ESP other err                     0
espudp enc pkts                   0   espudp enc err                    0
espudp dec pkts                   0   espudp dec err                    0
espudp other err                  0   acct update interval           3600
CPASXL packets                    0   PSLXL packets                     0
CPASXL async packets              0   PSLXL async packets               0
CPASXL bytes                      0   PSLXL bytes                       0
CPASXL conns                      0   PSLXL conns                       0
CPASXL conns created              0   PSLXL conns created               0
PXL FF conns                      0   PXL FF packets                    0
PXL FF bytes                      0   PXL FF acks                       0
PXL no conn drops                 0   PSL Inline packets                0
PSL Inline bytes                  0   CPAS Inline packets               0
CPAS Inline bytes                 0   Total QoS conns                   0
CLASSIFY                          0   CLASSIFY_FLOW                     0
RECLASSIFY_POLICY                 0   Enq-IN FW pkts                    0
Enq-OUT FW pkts                   0   Deq-IN FW pkts                    0
Deq-OUT FW pkts                   0   Enq-IN FW bytes                   0
Enq-OUT FW bytes                  0   Deq-IN FW bytes                   0
Deq-OUT FW bytes                  0   Enq-IN AXL pkts                   0
Enq-OUT AXL pkts                  0   Deq-IN AXL pkts                   0
Deq-OUT AXL pkts                  0   Enq-IN AXL bytes                  0
Enq-OUT AXL bytes                 0   Deq-IN AXL bytes                  0
Deq-OUT AXL bytes                 0   F2F packets                       0
F2F bytes                         0   TCP violations                    0
F2V conn match pkts               0   F2V packets                       0
F2V bytes                         0   gtp tunnels created               0
gtp tunnels                       0   gtp accel pkts                    0
gtp f2f pkts                      0   gtp spoofed pkts                  0
gtp in gtp pkts                   0   gtp signaling pkts                0
gtp tcpopt pkts                   0   gtp apn err pkts                  0
memory used                38799384   C tcp handshake conn              0
C tcp estab. conns                0   C tcp closed conns                0
C tcp pxl hnshk conn              0   C tcp pxl est. conn               0
C tcp pxl closed                  0   ob cpasxl packets                 0
ob pslxl packets                  0   ob cpasxl bytes                   0
ob pslxl bytes                    0   DNS DoR stats                     0
trimmed pkts
[Expert@MyGW:0]#
```

/proc/ppk/stats

Description

Contains the IRQ numbers and names of interfaces the SecureXL uses.

Syntax for IPv4

```
[Expert@MyGW:0]# ls -lR /proc/ppk/
```

```
[Expert@MyGW:0]# cat /proc/ppk/stats
```

Syntax for IPv6

```
[Expert@MyGW:0]# ls -lR /proc/ppk6/
```

```
[Expert@MyGW:0]# cat /proc/ppk6/stats
```

Example for IPv4

```
[Expert@MyGW:0]# cat /proc/ppk/stats
IRQ | Interface
---------------------------
 18   eth0
 16   eth1
 17   eth2
 18   eth3
 19   eth4
[Expert@MyGW:0]#
```

/proc/ppk/viol_statistics

Description

Contains SecureXL statistics for violations - packets SecureXL forwarded (F2F) to the Firewall.

Note - This is the same information that the "`fwaccel stats -p`" command shows (see *"fwaccel stats" on page 1473*).

Syntax for IPv4

```
[Expert@MyGW:0]# ls -lR /proc/ppk/
[Expert@MyGW:0]# cat /proc/ppk/viol_statistics
```

Syntax for IPv6

```
[Expert@MyGW:0]# ls -lR /proc/ppk6/
[Expert@MyGW:0]# cat /proc/ppk6/viol_statistics
```

Example for IPv4

```
[Expert@MyGW:0]# cat /proc/ppk/viol_statistics
Violation             Packets            Violation             Packets
--------------------  ---------------    --------------------  ---------------
pkt has IP options                0    ICMP miss conn                   4
TCP-SYN miss conn               356    TCP-other miss conn        1386954
UDP miss conn                943355    other miss conn                  0
VPN returned F2F                  0    uni-directional viol             0
possible spoof viol               0    TCP state viol                   0
out if not def/accl               0    bridge, src=dst                  0
routing decision err              0    sanity checks failed             0
fwd to non-pivot                  0    broadcast/multicast              0
cluster message           250859051    cluster forward                  0
chain forwarding                  0    F2V conn match pkts              0
general reason                    0    route changes                    0

[Expert@MyGW:0]#
```

SecureXL Debug

To understand how SecureXL processes the traffic, enable the SecureXL debug while the traffic passes through the Security Gateway / ClusterXL / Scalable Platform Security Group.

Warning - Debug increases the load on the CPU on the Security Gateway / Cluster Members / Security Group Members. We recommend you schedule a maintenance window to debug the SecureXL.

For the complete debug procedure, see the *R81.20 Security Gateway Guide* > Chapter "**Kernel Debug**".

fwaccel dbg

Description

The *fwaccel dbg* command controls the SecureXL debug. See *"SecureXL Debug Procedure" on page 1592*.

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms (Maestro and Chassis), you must connect to the applicable Security Group.
- If you do **not** use the complete debug procedure with the "`fw ctl kdebug`" command,
  and SecureXL works in Kernel Mode (KPPAK), then Security Gateway writes the debug outputs to these files:
  - `$FWDIR/log/fwk.elg` - Processing of traffic in the Firewall module
  - `/var/log/messages` - Additional information
- If you do **not** use the complete debug procedure with the "`fw ctl kdebug`" command,
  and SecureXL works in User Mode (UPPAK), then Security Gateway writes the debug outputs to these files:
  - `$FWDIR/log/fwk.elg` - Processing of traffic in the Firewall module
  - `/var/log/usim_x86.elg` - Processing of traffic in SecureXL
  - `/var/log/messages` - Processing of traffic in the ADP module (NVIDIA ConnectX 100G Cards)

Syntax in Gaia Clish or the Expert mode on a Security Gateway / ClusterXL:

```
fwaccel dbg
      -h
      -m <Name of SecureXL Debug Module>
      all
      + <Debug Flags>
      - <Debug Flags>
      reset
      -f {"<5-Tuple Debug Filter>" | reset}
      list
      resetall
```

Syntax in Gaia gClish on a Scalable Platform Security Group:

```
fwaccel dbg
      -h
      -m <Name of SecureXL Debug Module>
      all
      + <Debug Flags>
      - <Debug Flags>
      reset
      -f {"<5-Tuple Debug Filter>" | reset}
      list
      resetall
```

Syntax in the Expert mode on a Scalable Platform Security Group:

```
g_fwaccel dbg
      -h
      -m <Name of SecureXL Debug Module>
      all
      + <Debug Flags>
      - <Debug Flags>
      reset
      -f {"<5-Tuple Debug Filter>" | reset}
      list
      resetall
```

Parameters

Parameter	Description
`-h`	Shows the applicable built-in help.
`-m <Name of SecureXL Debug Module>`	Specifies the name of the SecureXL debug module. To see the list of available debug modules, run: `fwaccel dbg`
`all`	Enables all debug flags for the specified debug module.

Parameter	Description
`+ <Debug Flags>`	Enables the specified debug flags for the specified debug module: Syntax: `+ Flag1 [Flag2 Flag3 ... FlagN]` **Note** - You must press the space bar key after the plus (+) character.
`- <Debug Flags>`	Disables all debug flags for the specified debug module. Syntax: `- Flag1 [Flag2 Flag3 ... FlagN]` **Note** - You must press the space bar key after the minus (-) character.
`reset`	Resets all debug flags for the specified debug module to their default state.
`-f "<5-Tuple Debug Filter>"`	Configures the debug filter to show only debug messages that contain the specified connection. The filter is a string of five numbers separated with commas: `"<Source IP Address>,<Source Port>,<Destination IP Address>,<Destination Port>,<Protocol Number>"` **Notes:** ■ You can configure only one debug filter at one time. ■ You can use the asterisk "*" as a wildcard for an IP Address, Port number, or Protocol number. ■ For more information, see *IANA Service Name and Port Number Registry* and *IANA Protocol Numbers*.
`-f reset`	Resets the current debug filter.
`list`	Shows all enabled debug flags in all debug modules.
`resetall`	Reset all debug flags for all debug modules to their default state.

Enabling SecureXL debug flags during boot

From R81.20, you can configure SecureXL debug to start during boot.

Important - In a Cluster, you must configure all the Cluster Members in the same way.

Procedure

Step	Instructions
1	Connect to the command line on the Security Gateway / each Cluster Member. On Scalable Platforms (Maestro and Chassis), you must connect to the applicable Security Group.
2	Log in to the Expert mode.

3	Create the require configuration files:
	■ To collect the debug for IPv4 traffic:
	`touch $FWDIR/conf/fwaccel_dbg_flags.cfg`
	■ To collect the debug for IPv6 traffic:
	`touch $FWDIR/conf/fwaccel6_dbg_flags.cfg`

4	Edit the applicable configuration file:
	■ To collect the debug for IPv4 traffic:
	`vi $FWDIR/conf/fwaccel_dbg_flags.cfg`
	■ To collect the debug for IPv6 traffic:
	`vi $FWDIR/conf/fwaccel6_dbg_flags.cfg`

5	Configure the applicable debug modules and the debug flags (see *R81.20 Security Gateway Guide*).
	Write each debug module and its flags on a separate line:
	`<Name of Debug Module #1> <Flag1> <Flag2> <Flag3> ... <FlagN>`
	`<Name of Debug Module #2> <Flag1> <Flag2> <Flag3> ... <FlagN>`
	Example:
	`default conn nat`
	`pkt drop nat`

6	Save the changes in the file and exit the editor.

Step	Instructions

7	On the Scalable Platform Security Group, you must copy the updated file to all Security Group Members:
	`asg_cp2blades $FWDIR/conf/fwaccel_dbg_flags.cfg`
	`asg_cp2blades $FWDIR/conf/fwaccel6_dbg_flags.cfg`

8	Reboot the Security Gateway / each Cluster Member / all Security Group Members.
9	Wait for the issue to occur.
10	Connect to the command line on the Security Gateway / each Cluster Member. On Scalable Platforms (Maestro and Chassis), you must connect to the applicable Security Group.
11	Log in to the Expert mode.

12	Reset all the SecureXL debug flags in all SecureXL debug modules:
	■ On the Security Gateway / each Cluster Member:
	`fwaccel dbg resetall`
	■ On the Scalable Platform Security Group:
	`g_fwaccel dbg resetall`

13	Remove all entries from the configuration files:
	■ On the Security Gateway / each Cluster Member:
	`echo '' > $FWDIR/conf/fwaccel_dbg_flags.cfg`
	`echo '' > $FWDIR/conf/fwaccel6_dbg_flags.cfg`
	■ On the Scalable Platform Security Group:
	`echo '' > $FWDIR/conf/fwaccel_dbg_flags.cfg`
	`asg_cp2blades $FWDIR/conf/fwaccel_dbg_flags.cfg`
	`echo '' > $FWDIR/conf/fwaccel6_dbg_flags.cfg`
	`asg_cp2blades $FWDIR/conf/fwaccel6_dbg_flags.cfg`

Step	Instructions
14	Collect the output files. If SecureXL works in Kernel Mode (KPPAK): ■ `$FWDIR/log/fwk.elg` ■ `/var/log/messages` If SecureXL works in User Mode (UPPAK): ■ `$FWDIR/log/fwk.elg` ■ `/var/log/usim_x86.elg` ■ `/var/log/messages`

Examples

Example 1 - Default output

```
[Expert@MyGW:0]# fwaccel dbg
Usage: fwaccel dbg [-m <...>] [resetall | reset | list | all | +/- <flags>]
   -m <module>             - module of debugging
   -h                      - this help message
   resetall                - reset all debug flags for all modules
   reset                   - reset all debug flags for module
   all                     - set all debug flags for module
   list                    - list all debug flags for all modules
   -f reset | "<5-tuple>"  - filter debug messages
   + <flags>               - set the given debug flags
   - <flags>               - unset the given debug flags

Debug flags can be enabled at boot by adding them to
$FWDIR/conf/fwaccel_dbg_flags.cfg and $FWDIR/conf/fwaccel6_dbg_flags.cfg.
The file format is one line per module.

For example, to enable "tcp_state" and "routing" for the "pkt" module:
    echo "pkt tcp_state routing" >> $FWDIR/conf/fwaccel_dbg_flags.cfg

List of available modules and flags:

Module: default (default)
init drv tag lock cpdrv routing kdrv tcp_sv svm iter conn htab del update acct conf stat
queue ioctl corr util rngs relations ant conn_app rngs_print infra_ids offload nat

Module: db
get save del tmpl tmo init ant profile nmr nmt warning

Module: api
init add update del acct conf stat vpn notif tmpl sv pxl qos gtp infra tmpl_info upd_conf
upd_if_inf add_sa del_sa del_all_sas misc get_features get_tab get_stat reset_stat tag long_
ver del_all_tmpl get_state upd_link_sel

Module: pkt
f2f frag spoof acct notif tcp_state tcp_state_pkt sv cpls routing drop pxl qos user deliver
vlan pkt nat wrp corr caf bhm geneve sctp

Module: infras
reorder pm

Module: tmpl
dtmpl_get dtmpl_notif tmpl

Module: vpn
vpnpkt linksel routing vpn ls

Module: nac
db db_get pkt pkt_ex signature offload idnt ioctl nac

Module: cpaq
init client server exp cbuf opreg transport transport_utils broadcast

Module: synatk
init conf conn log pkt proxy state msg

Module: adp
rt nh eth heth wrp inf mbs bpl bplinf mbeinf if drop bond xmode ipsctl ac_print cpfifo qconf
qcomm filter packet mcast hw_offload hw_expn rte_api

Module: dos
fw1-cfg fw1-pkt sim-cfg sim-pkt detailed-pkt detailed-cfg drop cache

Module: gtp
pkt policy tables api drop notif general
```

```
Module: usdisp
error conn packet api msg state packet_err counter event quota ioctl lock clb uid queue
fwstats cachetab vpn temp_conns prio route dumbo

Module: dpdk_lib


Module: dpdk_pmd


Module: dpdk_other


[Expert@MyGW:0]#
```

Example 2 - Enabling and disabling of debug flags

```
[Expert@MyGW:0]# fwaccel dbg -m default + conn
Debug flags updated.
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dbg list

[Expert@MyGW:0]# fwaccel dbg list
 Module: default (400)
conn

Module: db (0)


Module: api (0)


Module: pkt (0)


Module: infras (0)


Module: tmpl (0)


Module: vpn (0)


Module: nac (0)


Module: cpaq (0)


Module: synatk (0)


Module: adp (0)


Module: dos (0)


Module: gtp (0)


Module: usdisp (0)


Module: dpdk_lib (0)


Module: dpdk_pmd (0)


Module: dpdk_other (0)


Debug filter not set.
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dbg -m default - conn
Debug flags updated.
[Expert@MyGW:0]#
```

```
[Expert@MyGW:0]# fwaccel dbg list

Module: default (0)


Module: db (0)


Module: api (0)


Module: pkt (0)


Module: infras (0)


Module: tmpl (0)


Module: vpn (0)


Module: nac (0)


Module: cpaq (0)


Module: synatk (0)


Module: adp (0)


Module: dos (0)


Module: gtp (0)


Module: usdisp (0)


Module: dpdk_lib (0)


Module: dpdk_pmd (0)


Module: dpdk_other (0)


Debug filter not set.
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dbg -m default reset
Debug flags updated.
[Expert@MyGW:0]#
```

Example 3 - Resetting all debug flags in all debug modules

```
[Expert@MyGW:0]# fwaccel dbg resetall
Debug state was reset to default.
[Expert@MyGW:0]#
```

Example 4 - Configuring debug filter for an SSH connection from 192.168.20.30 to 172.16.40.50

```
[Expert@MyGW:0]# fwaccel dbg -f 192.168.20.30,*,172.16.40.50,22,6
Debug filter was set.
[Expert@MyGW:0]#
[Expert@MyGW:0]# fwaccel dbg list

... ...

Debug filter: "<*,*,*,*,*>"
[Expert@MyGW:0]#
```

SecureXL Debug Procedure

By default, SecureXL writes the output debug information to the `/var/log/messages` file.

To collect the applicable SecureXL debug and to make its analysis easier, follow the steps below.

Note - For the complete debug procedure, see the *R81.20 Security Gateway Guide* - Chapter "**Kernel Debug**".

Important:

- We strongly recommend to schedule a full maintenance window to minimize the impact on your production traffic.
- We strongly recommend to connect over serial console to your Security Gateway / each Cluster Member / Scalable Platform Security Group Members. This is to prevent a possible issue when you cannot work with the CLI because of a high load on the CPU.
- In cluster, you must collect this debug from all Cluster Members in the same way.
- Debug the specific SecureXL instance only when you are sure that only that SecureXL instance processes the traffic.

Procedure

1. **Connect to the command line on your Security Gateway / each Cluster Member / Scalable Platform Security Group**

   Use an SSH or a console connection.

   Best Practice - Use a console connection.

   Note - On Scalable Platforms (Maestro and Chassis), you must connect to the applicable Security Group.

2. **Log in to the Expert mode**

   If the default shell is Gaia Clish, run:

   ```
   expert
   ```

3. **Reset all kernel debug flags in all kernel debug modules**

- On the Security Gateway / each Cluster Member, run:

```
fw ctl debug 0
```

- On the Scalable Platform Security Group, run:

```
g_fw ctl debug 0
```

4. **Reset all the SecureXL debug flags in all SecureXL debug modules**

   - On the Security Gateway / each Cluster Member:

```
fwaccel dbg resetall
```

   - On the Scalable Platform Security Group:

```
g_fwaccel dbg resetall
```

5. **Allocate the kernel debug buffer**

   - On the Security Gateway / each Cluster Member, run:

```
fw ctl debug -buf 8200 [-v {"<List of VSIDs>" | all}]
```

   - On the Scalable Platform Security Group, run:

```
g_fw ctl debug -buf 8200 [-v {"<List of VSIDs>" | all}]
```

   Note - The optional part "`-v {"<List of VSIDs>" | all}`" is to specify the applicable Virtual Systems on a VSX Gateway or VSX Cluster Member.

6. **Make sure the Security Gateway allocated the kernel debug buffer**

   - On the Security Gateway / each Cluster Member, run:

```
fw ctl debug | grep buffer
```

   - On the Scalable Platform Security Group, run:

```
g_fw ctl debug | grep buffer
```

7. **Configure the applicable kernel debug modules and kernel debug flags**

- On the Security Gateway / each Cluster Member, run:

```
fw ctl debug -m <Name of Kernel Debug Module> {all | +
<Kernel Debug Flags>}
```

- On the Scalable Platform Security Group, run:

```
g_fw ctl debug -m <Name of Kernel Debug Module> {all | +
<Kernel Debug Flags>}
```

8. **Configure the applicable SecureXL debug modules and SecureXL debug flags**

   - On the Security Gateway / each Cluster Member:

```
fwaccel dbg -m <Name of SecureXL Debug Module> {all | +
<SecureXL Debug Flags>}
```

   - On the Scalable Platform Security Group:

```
g_fwaccel dbg -m <Name of SecureXL Debug Module> {all |
+ <SecureXL Debug Flags>}
```

   See *"SecureXL Debug Modules and Debug Flags" on page 1598*.

9. **Examine the kernel debug configuration for kernel debug modules**

   - On the Security Gateway / each Cluster Member, run:

```
fw ctl debug
```

   - On the Scalable Platform Security Group, run:

```
g_fw ctl debug
```

10. **Examine the SecureXL debug configuration for SecureXL debug modules**

    - On the Security Gateway / each Cluster Member:

```
fwaccel dbg list
```

    - On the Scalable Platform Security Group:

```
g_fwaccel dbg list
```

11. **Remove all entries from both the Firewall Connections table and SecureXL Connections table**

Important:
- This step makes sure that you collect the debug of the real issue that is not affected by the existing connections.
- **This command deletes all existing connections. This interrupts all connections, including the SSH.**
  Run this command only if you are connected over a serial console to your Security Gateway / each Cluster Member / Scalable Platform Security Group Members.

- On the Security Gateway / each Cluster Member, run:

```
fw tab -t connections -x -y
```

- On the Scalable Platform Security Group, run:

```
g_fw tab -t connections -x -y
```

12. **Remove all entries from the Firewall Templates table**

Note - This command does **not** interrupt the existing connections. This step makes sure that you collect the debug of the real issue that is not affected by the existing connection templates.

- On the Security Gateway / each Cluster Member, run:

```
fw tab -t cphwd_tmpl -x -y
```

- On the Scalable Platform Security Group, run:

```
g_fw tab -t cphwd_tmpl -x -y
```

13. **Start the kernel debug**

In Gateway mode:

- On the Security Gateway / each Cluster Member, run:

```
fw ctl kdebug -T -f -o /var/log/kernel_debug.txt
```

- On the Scalable Platform Security Group, run:

```
g_fw ctl kdebug -T -f -o /var/log/kernel_debug.txt
```

In VSX mode - for specific Virtual Systems:

- On the VSX Gateway / each VSX Cluster Member, run:

```
fw ctl kdebug -v {"<List of VSIDs>" | all} -k -T -f -o
/var/log/kernel_debug.txt
```

- On the Scalable Platform Security Group in VSX mode, run:

```
g_fw ctl kdebug -v {"<List of VSIDs>" | all} -k -T -f -o
/var/log/kernel_debug.txt
```

14. **Replicate the issue, or wait for the issue to occur**

    Perform the steps that cause the issue to occur, or wait for it to occur.

15. **Stop the kernel debug**

    Press **CTRL+C**.

16. **Reset all kernel debug flags in all kernel debug modules**

    - On the Security Gateway / each Cluster Member, run:

```
fw ctl debug 0
```

    - On the Scalable PlatformSecurity Group, run:

```
g_fw ctl debug 0
```

17. **Reset all the SecureXL debug flags in all SecureXL debug modules**

    - On the Security Gateway / each Cluster Member:

```
fwaccel dbg resetall
```

    - On the Scalable PlatformSecurity Group:

```
g_fwaccel dbg resetall
```

18. **Examine the kernel debug configuration to make sure it returned to the default**

- On the Security Gateway / each Cluster Member, run:

```
fw ctl debug
```

- On the Scalable Platform Security Group, run:

```
g_fw ctl debug
```

19. **Examine the SecureXL debug configuration to make sure it returned to the default**

    - On the Security Gateway / each Cluster Member:

```
fwaccel dbg list
```

    - On the Scalable Platform Security Group:

```
g_fwaccel dbg list
```

20. **Analyze the debug output files**

    Transfer these files from the Security Gateway / each Cluster Member / each Security Group Member to your computer:

`/var/log/kernel_debug.txt`
`/var/log/messages*`
`$FWDIR/log/fwk.elg*`
`/var/log/usim_x86.elg*`

    Best Practice - Compress these files with the "`tar -zxvf`" command and transfer the archive from the Security Gateway / each Cluster Member / each Security Group Member to your computer. If you transfer to an FTP server, do so in the binary mode.

SecureXL Debug Modules and Debug Flags

To see the available SecureXL debug modules and their debug flags, run the *"fwaccel dbg" on page 1578* command.

Module "default"

Flag	Description
`acct`	Connection accounting information
`ant`	Anticipated connections
`conf`	Configuration of the SecureXL (for example, interfaces)
`conn`	Processing of connections
`conn_app`	Processing of connections
`corr`	Correction layer
`cpdrv`	*Currently not in use*
`del`	Deletion of connections
`drv`	Driver information
`htab`	Hash table
`infra_ids`	Allocating IDs for a given range in Identity Awareness
`init`	Initialization
`ioctl`	Changes in the configuration, which were initiated from the user space
`iter`	Connection table iterator
`kdrv`	Driver information
`lock`	Lock initializing and finalizing
`nat`	Processing of NAT connections
`offload`	Offloading of connections from the Firewall to the SecureXL
`queue`	Connections queue
`relations`	Related connections (such as FTP data connections)
`rngs`	Handling of SecureXL ranges

Flag	Description
`rngs_print`	Printing of SecureXL ranges
`routing`	Handling of SecureXL routing
`stat`	Handling of SecureXL statistics
`svm`	Registering templates or connections for System Counters in Security Gateway object in SmartConsole
`tag`	Tags that were added to the packets by the SecureXL before forwarding them to the Firewall
`tcp_sv`	Verification of sequence in TCP packets
`update`	Updates of connections
`util`	Utilization

Module "pkt" (Packet)

Flag	Description
`acct`	Connection accounting information
`bhm`	BHM Statistics for each CPU
`caf`	Mirror and Decrypt feature - Mirror only of all traffic
`corr`	Correction layer
`cpls`	ClusterXL Load Sharing
`deliver`	Packet delivery
`drop`	Packets dropped by SecureXL
`f2f`	Reason for forwarding a packet to the Firewall
`frag`	Processing of fragments
`geneve`	Processing of Generic Network Virtualization Encapsulation (Geneve) packets in GRE and VxLAN interfaces
`nat`	Processing of NAT connections
`notif`	Notifications sent to the Firewall

Flag	Description
`pkt`	Processing of packets
`pxl`	PXL (PacketXL) handling - API between the SecureXL and PSL (Packet Streaming Layer), which is a TCP Streaming engine that parses TCP streams
`qos`	QoS acceleration
`routing`	Handling of SecureXL routing
`sctp`	Handling of Stream Control Transmission Protocol (SCTP) packets
`spoof`	Handling of SecureXL Anti-Spoofing
`sv`	Validation of sequence in TCP packets
`tcp_ state`	Validation of TCP state in TCP packets
`tcp_ state_ pkt`	Validation of TCP packets
`user`	Details of a packet
`vlan`	Handling of VLAN tags
`wrp`	Handling of WRP interfaces in VSX

Module "db" (Database)

Flag	Description
`ant`	Anticipated connections
`del`	Deleting of data from the SecureXL database
`get`	Retrieving of data from the SecureXL database
`init`	Initializing and finalizing of SecureXL database
`nmr`	"No Match Ranges" templates, which allow SecureXL Accept Templates for rules that contain Dynamic objects or Domain objects (or for rules located below such rules)

Flag	Description
nmt	"No Match Time" templates, which allow SecureXL Accept Templates for rules that contain Time objects (or for rules located below such rules)
profile	Operations on profile table
save	Saving of data to the SecureXL database
tmo	Handling of timeouts for SecureXL database entries
tmpl	Handling of SecureXL templates database
warning	General failures to process a packet

Module "api" (Application Programmable Interface)

Flag	Description
acct	Connection accounting information
add	Adding of connections
add_sa	Offloading of VPN SA to SecureXL
conf	Configuration of the SecureXL (for example, interfaces)
del	Deletion of connections
del_all_sas	Deletion of all VPN SAs from SecureXL
del_all_tmpl	Deletion of the SecureXL Templates
del_sa	Deletion of VPN SA from SecureXL
get_features	Getting features buffer (in SecureXL initialization)
get_stat	Retrieving of SecureXL statistics
get_state	Getting the connection state from SecureXL
get_tab	Some extra printouts when processing SecureXL tables
gtp	Processing of GPRS Tunnelling Protocol (GTP) tunnel connections

Flag	Description
`infra`	SecureXL infrastructure
`init`	Enabling and disabling of SecureXL
`long_ver`	Prints additional verbose information about connections
`misc`	Prints additional information about SecureXL internals
`notif`	Notifications sent to the Firewall
`pxl`	PXL (PacketXL) handling - API between the SecureXL and PSL (Packet Streaming Layer), which is a TCP Streaming engine that parses TCP streams
`qos`	QoS acceleration
`reset_stat`	Prints statistics IDs that are reset
`stat`	Handling of SecureXL statistics
`sv`	Validation of sequence in TCP packets
`tag`	Tags that were added to the packets by the SecureXL before forwarding them to the Firewall
`tmpl`	Handling of SecureXL Templates
`tmpl_info`	Information about SecureXL Templates
`upd_conf`	Update of SecureXL in ClusterXL Load Sharing
`upd_if_inf`	Prints some text that shows if SecureXL updated information about interfaces
`upd_link_sel`	Updates of VPN Link Selection
`update`	Updates of connections
`vpn`	Processing of VPN connection

Module "adp" (NVIDIA ConnectX 100G Cards)

Flag	Description
`ac_print`	Prints additional information
`bond`	Information about Bond interfaces
`bpl`	Information about packet processing in the backplane
`bplinf`	Information about packet processing in the backplane
`cpfifo`	*Currently is not used*
`drop`	Information about packet drops in the backplane
`eth`	Information about ports from the NVIDIA ConnectX 100G Card's point of view
`filter`	Information about packet processing in the network interface
`heth`	Information about ports from the Host Security Appliance's point of view
`hw_expn`	Information about packet processing in the NVIDIA ConnectX 100G Card
`hw_offload`	Offloading of connections from the Host Security Appliance to the SecureXL
`if`	Information about interfaces
`inf`	Information about slots and ports
`ipsctl`	Information about slots in the Host Security Appliance
`mbeinf`	Information about packet processing in the backplane
`mbs`	Information about packet processing in the backplane
`mcast`	Handling of multicast traffic
`nh`	Handling of next hop routing
`packet`	Information about packet processing in the NVIDIA ConnectX 100G Card
`qcomm`	Information about communication queues
`qconf`	Information about packets in the communication queues
`rt`	Handling of general routing

Flag	Description
`rte_api`	Detailed information about packet processing in the NVIDIA ConnectX 100G Card
`wrp`	Handling of WRP interfaces in VSX
`xmode`	Events in the known neighbors database

Module "infras" (Identity Awareness - Identities Infrastructure)

Flag	Description
`pm`	Pattern Matcher
`reorder`	Reordering of packets in queue

Module "nac" (Identity Awareness - Network Access Control)

Flag	Description
`db`	Updating, adding, deleting of identities
`db_get`	Updating, fetching, searching of identities
`idnt`	Identity Tags
`ioctl`	Changes in the configuration, which were initiated from the user space
`nac`	Network Access Control
`offload`	Offloading of connections from the Firewall to the SecureXL
`pkt`	Forwarding of connections to Firewall (when identity is not found or revoked, or NAC packet tagging verification failed)
`pkt_ex`	NAC packet-tagging verification
`signature`	Signing of packets

Module "vpn" (VPN)

Flag	Description
`linksel`	VPN Link Selection

Flag	Description
`ls`	Forwarding of packets between Cluster Members in a ClusterXL Load Sharing mode
`routing`	VPN Encryption routing information
`vpn`	Processing of VPN connections
`vpnpkt`	Processing of VPN packets

Module "cpaq" (Internal Asynchronous Queue)

Flag	Description
`broadcast`	Processing of broadcast packets
`cbuf`	Information about queue buffers
`client`	Information about queue clients
`error`	General errors
`exp`	Information about expiration of queue items
`init`	Initializing of queue
`opreg`	*Currently not in use*
`server`	Information about queue servers
`transport`	Information about sending messages in queue
`transport_utils`	Additional information about sending messages in queue

Module "dos" (Denial of Service Defender)

Flag	Description
`cache`	*Currently not in use*
`detailed-cfg`	Detailed information about DoS Rate Limiting configuration. **Important** - This debug flag is not suitable for large traffic volumes because it prints a large number of messages. This causes high load on the CPU.

Flag	Description
`detailed-pkt`	Detailed information about DoS Rate Limiting packet flow. **Important** - This debug flag is not suitable for large traffic volumes because it prints a large number of messages. This causes high load on the CPU.
`drop`	Dropped packets
`fw1-cfg`	Information about DoS Rate Limiting configuration in the Firewall kernel module
`fw1-pkt`	Information about DoS Rate Limiting packet flow in the Firewall kernel module
`sim-cfg`	Information about DoS Rate Limiting configuration in the SecureXL kernel module
`sim-pkt`	Information about DoS Rate Limiting packet flow in the SecureXL kernel module

Module "synatk" (Accelerated SYN Defender)

Flag	Description
`conf`	Receiving and updating of Accelerated SYN Defender module's configuration
`conn`	Handling of TCP connections
`init`	Initializing of the Accelerated SYN Defender module
`log`	Prints time of the last sent monitor log and interval between the monitor logs
`msg`	Information about internal messages in the Accelerated SYN Defender module
`pkt`	Handling of TCP packets
`proxy`	*Currently not in use*
`state`	Information about states of the Accelerated SYN Defender module

Module "tmpl" (Drop Templates)

Flag	Description
`dtmpl_get`	Getting of Drop Templates
`dtmpl_notif`	Notifications about Drop Templates
`tmpl`	Information about Drop Templates

Module "gtp" (GPRS Tunnelling Protocol (GTP))

Flag	Description
`api`	Information about GTP tunnels in kernel tables
`drop`	Drops of GTP packets
`general`	General information about APN and kernel tables
`notif`	Information about notification messages
`pkt`	Processing of GTP packets
`policy`	APN information
`tables`	Operations in kernel tables

Module "usdisp" (User Space Dispatcher)

Flag	Description
`api`	*Currently not in use*
`cachetab`	*Currently not in use*
`clb`	*Currently not in use*
`conn`	Processing of connections
`counter`	*Currently not in use*
`dumbo`	*Currently not in use*
`error`	General errors
`event`	*Currently not in use*

Flag	Description
`fwstats`	*Currently not in use*
`ioctl`	IOCTL control messages (communication between kernel and user space processes)
`lock`	*Currently not in use*
`msg`	*Currently not in use*
`packet`	Processing of packets
`packet_err`	Processing of packets
`prio`	*Currently not in use*
`queue`	*Currently not in use*
`quota`	*Currently not in use*
`route`	*Currently not in use*
`state`	*Currently not in use*
`temp_conns`	Shows the selected CoreXL Firewall instance
`uid`	*Currently not in use*
`vpn`	*Currently not in use*

Module "dpdk_lib" (Data Plane Development Kit (DPDK) - Library)

Reserved for future use.

Module "dpdk_pmd" (Data Plane Development Kit (DPDK) - Poll Mode Drivers)

Reserved for future use.

Module "dpdk_other" (Data Plane Development Kit (DPDK) - Other)

Reserved for future use.

CoreXL Commands

For more information about CoreXL, see the *R81.20 Performance Tuning Administration Guide* - Chapter *CoreXL*.

cp_conf corexl

Description

Enables or disables CoreXL.

For more information, see the *R81.20 Performance Tuning Administration Guide*.

Important:

- This command is for Check Point use only.
  To configure CoreXL, use the **Check Point CoreXL** option in the *"cpconfig" on page 996* menu.
- After all changes in CoreXL configuration on the Security Gateway / Cluster Member / Security Group, you must reboot it.
- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms (Maestro and Chassis), you must connect to the applicable Security Group.

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

- To enable CoreXL with 'n' IPv4 Firewall instances and optionally 'k' IPv6 Firewall instances:

```
cp_conf corexl [-v] enable [n] [-6 k]
```

- To disable CoreXL:

```
cp_conf corexl [-v] disable
```

Syntax on a Scalable Platform Security Group in Gaia gClish

- To enable CoreXL with 'n' IPv4 Firewall instances and optionally 'k' IPv6 Firewall instances:

```
cp_conf corexl [-v] enable [n] [-6 k]
```

- To disable CoreXL:

```
cp_conf corexl [-v] disable
```

Syntax on a Scalable Platform Security Group in the Expert mode

- To enable CoreXL with 'n' IPv4 Firewall instances and optionally 'k' IPv6 Firewall instances:

```
g_all cp_conf corexl [-v] enable [n] [-6 k]
```

- To disable CoreXL:

```
g_all cp_conf corexl [-v] disable
```

The related command is: *"fwboot corexl" on page 1257*.

Parameters

Parameter	Description
-v	Leaves the high memory (vmalloc) unchanged.
n	Denotes the number of IPv4 CoreXL Firewall instances.
k	Denotes the number of IPv6 CoreXL Firewall instances.

Example

Currently, the Security Gateway runs two IP4v CoreXL Firewall instances (`KERN_INSTANCE_NUM = 2`).

We change the number of IP4v CoreXL Firewall instances to three.

```
[Expert@MyGW:0]# fw ctl multik stat
ID | Active  | CPU    | Connections | Peak
----------------------------------------------
 0 | Yes     | 2      |           7 |       28
 1 | Yes     | 1      |           0 |       11
[Expert@MyGW:0]#
[Expert@MyGW:0]# cat /etc/fw.boot/boot.conf
CTL_IPFORWARDING 1
DEFAULT_FILTER_PATH 0
KERN_INSTANCE_NUM 2
COREXL_INSTALLED 1
KERN6_INSTANCE_NUM 2
IPV6_INSTALLED 0
CORE_OVERRIDE 4
[Expert@MyGW:0]#
[Expert@MyGW:0]# cp_conf corexl -v enable 3
[Expert@MyGW:0]#
[Expert@MyGW:0]# cat /etc/fw.boot/boot.conf
CTL_IPFORWARDING 1
DEFAULT_FILTER_PATH 0
KERN_INSTANCE_NUM 3
COREXL_INSTALLED 1
KERN6_INSTANCE_NUM 2
IPV6_INSTALLED 0
CORE_OVERRIDE 4
[Expert@MyGW:0]#
[Expert@MyGW:0]# reboot
.. ... ...
[Expert@MyGW:0]# fw ctl multik stat
ID | Active  | CPU    | Connections | Peak
----------------------------------------------
 0 | Yes     | 3      |           7 |       28
 1 | Yes     | 2      |           0 |       11
 2 | Yes     | 1      |           4 |       10
[Expert@MyGW:0]#
```

dynamic_balancing

Description

On Check Point Appliances, R80.40 added the ability to change the number of CoreXL Firewall and SND instances without reboot (Dynamic Balancing).

Important:

- By default, this feature is *enabled*.
- We do **not** recommend manual configuration of CoreXL Firewall and SND instances, because such configuration *disables* the CoreXL Dynamic Balancing.
  To enable the CoreXL Dynamic Balancing again, you must disable it and enable it.
- For CoreXL Dynamic Balancing requirements, see sk164155.

The "`dynamic_balancing`" command in the Expert mode (and the command "`set dynamic-balancing state`" in Gaia Clish) controls the Dynamic Balancing of CoreXL Firewall and SND instances on the local Security Gateway, or Cluster Member.

For more information, see *R81.20 Performance Tuning Administration Guide* - Chapter *CoreXL*.

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms (Maestro and Chassis), you must connect to the applicable Security Group.

Syntax

Shell	Security Gateway (each Cluster Member)	Security Group on a Scalable Platform

Gaia Clish	`set dynamic-balancing state`
	`disable`
	`enable`
	`reset`
	`start`
	`stop`
	
	`show dynamic-balancing state`
		N / A

Gaia gClish	N / A	`set dynamic-balancing state`
		`disable`
		`enable`
		`reset`
		`start`
		`stop`
		
		`show dynamic-balancing state`

Expert mode	`dynamic_balancing`
	`-o disable`
	`-o enable`
	`-o start`
	`-o stop`
	`-p`
	`-r`
		`g_dynamic_balancing`
		`-o disable`
		`-o enable`
		`-o start`
		`-o stop`
		`-p`
		`-r`

Parameters

Parameter	Description
No Parameters	Shows the applicable built-in help.

Parameter	Description
`disable`	Disables the CoreXL Dynamic Balancing. **Important:** ■ When you disable this feature, the CoreXL configuration returns to the default. ■ After you disable this feature, the Security Gateway (Scalable Platform Security Group) **requires** a reboot. The command shows the applicable message. **Best Practice** - To keep the Scalable PlatformSecurity Group active, we recommended to reboot the Security Group Members gradually.
`enable`	Enables the CoreXL Dynamic Balancing. **Important:** ■ After you enable this feature, the Security Gateway (Scalable Platform Security Group) **requires** a reboot. The command shows the applicable message. ■ After you enable this feature for the first time, the Security Gateway (Scalable Platform Security Group) may require a reboot in these cases: • The current CoreXL configuration is not the default • More CoreXL SND instances are required for the current CPU load ■ After the boot, you can stop, start, and this feature without a reboot. **Best Practice** - To keep the Scalable PlatformSecurity Group active, we recommended to reboot the Security Group Members gradually.

`reset`
or
`-r`
	Resets the CoreXL configuration to the default and keeps the CoreXL Dynamic Balancing enabled.
	This command is equivalent to the "`disable`" command followed by the "`enable`" command.
	Important:
	■ After this feature resets, the CoreXL configuration returns to the default.
	■ This change does **not** require a reboot.

Parameter	Description
`start`	Starts the CoreXL Dynamic Balancing after it was stopped. **Important:** ■ When you start this feature, the Security Gateway (Scalable Platform Security Group) continues to change the CoreXL Balancing configuration automatically based on the CPU utilization. ■ This change does **not** require a reboot. ■ This change survives the reboot. ■ The status of the CoreXL Dynamic Balancing appears as "off".
`stop`	Stops the CoreXL Dynamic Balancing. **Important:** ■ When you stop this feature, the Security Gateway (Scalable Platform Security Group) uses the last CoreXL Balancing configuration. ■ This change does **not** require a reboot. ■ This change survives the reboot.

`show dynamic-balancing state`
or
`-p`
	Shows the current state of the CoreXL Dynamic Balancing (enabled, disabled, started, or stopped).

Example

```
[Expert@MyGW:0]# dynamic_balancing -p
Dynamic Balancing is currently On
[Expert@MyGW:0]#
```

fw ctl multik

Description

The *fw ctl multik* and *fw6 ctl multik* commands control CoreXL for IPv4 and IPv6, respectively.

Syntax for IPv4

```
fw ctl multik
      add_bypass_port <options>
      del_bypass_port <options>
      dynamic_dispatching <options>
      gconn <options>
      get_instance <options>
      print_heavy_conn
      prioq <options>
      show_bypass_ports
      stat
      start
      stop
      utilize
```

Syntax for IPv6

```
fw6 ctl multik
      add_bypass_port <options>
      del_bypass_port <options>
      dynamic_dispatching <options>
      gconn <options>
      get_instance <options>
      print_heavy_conn
      prioq <options>
      show_bypass_ports
      stat
      start
      stop
      utilize
```

Parameters

Parameter	Description
`add_bypass_port <options>`	Adds the specified TCP and UDP ports to the CoreXL Dynamic Dispatcher bypass list. See *"fw ctl multik add_bypass_port" on page 1619*.
`del_bypass_port <options>`	Removes the specified TCP and UDP ports from the CoreXL Dynamic Dispatcher bypass list. See *"fw ctl multik del_bypass_port" on page 1621*.
`dynamic_ dispatching <options>`	Shows and controls CoreXL Dynamic Dispatcher (see sk105261). See *"fw ctl multik dynamic_dispatching" on page 1623*.
`gconn <options>`	Shows statistics about CoreXL Global Connections. See *"fw ctl multik gconn" on page 1624*.
`get_instance <options>`	Shows CoreXL Firewall instance that processes the specified IPv4 connection. See *"fw ctl multik get_instance" on page 1629*.
`print_heavy_conn`	Shows the table with Heavy Connections (that consume the most CPU resources) in the CoreXL Dynamic Dispatcher. See *"fw ctl multik print_heavy_conn" on page 1631*.
`prioq <options>`	Configures the CoreXL Firewall Priority Queues (see sk105762). See *"fw ctl multik prioq" on page 1633*.
`show_bypass_ ports`	Shows the TCP and UDP ports configured in the bypass port list of the CoreXL Dynamic Dispatcher. See *"fw ctl multik show_bypass_ports" on page 1634*.
`stat`	Shows the CoreXL status. See *"fw ctl multik stat" on page 1635*.
`start`	Starts all CoreXL Firewall instances on-the-fly. See *"fw ctl multik start" on page 1637*.
`stop`	Stops all CoreXL Firewall instances temporarily. See *"fw ctl multik stop" on page 1638*.
`utilize`	Shows the CoreXL queue utilization for each CoreXL Firewall instance. See *"fw ctl multik utilize" on page 1639*.

fw ctl multik add_bypass_port

Description

Adds the specified TCP and UDP ports to the bypass port list of the CoreXL Dynamic Dispatcher.

For more information about the CoreXL Dynamic Dispatcher, see sk105261.

Important - This command saves the configuration in the `$FWDIR/conf/dispatcher_bypass.conf` file. You must **not** edit this file manually.

Syntax

```
fw ctl multik add_bypass_port <Port Number 1>,<Port Number 2>,...,<Port Number N>
```

Parameters

Parameter	Description
<Port Number>	Specifies the numbers of TCP and UDP ports to add to the list. **Important** - You can add 10 ports maximum.

Example

```
[Expert@MyGW:0]# fw ctl multik show_bypass_ports
dynamic dispatcher bypass port list:
[Expert@MyGW:0]#
[Expert@MyGW:0]# cat $FWDIR/conf/dispatcher_bypass.conf
dynamic_dispatcher_bypass_ports_number = 0
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl multik add_bypass_port 8888
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl multik show_bypass_ports
dynamic dispatcher bypass port list:
(8888)
[Expert@MyGW:0]
[Expert@MyGW:0]# cat $FWDIR/conf/dispatcher_bypass.conf
dynamic_dispatcher_bypass_ports_number = 1
dynamic_dispatcher_bypass_port_table=8888
[Expert@MyGW:0]
[Expert@MyGW:0]# fw ctl multik add_bypass_port 9999
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl multik show_bypass_ports
dynamic dispatcher bypass port list:
(8888,9999)
[Expert@MyGW:0]
[Expert@MyGW:0]# cat $FWDIR/conf/dispatcher_bypass.conf
dynamic_dispatcher_bypass_ports_number = 2
dynamic_dispatcher_bypass_port_table=8888,9999
[Expert@MyGW:0]
```

fw ctl multik del_bypass_port

Description

Removes the specified TCP and UDP ports from the bypass port list of the CoreXL Dynamic Dispatcher.

For more information about the CoreXL Dynamic Dispatcher, see sk105261.

Important - This command saves the configuration in the `$FWDIR/conf/dispatcher_bypass.conf` file. You must **not** edit this file manually.

Syntax

```
fw ctl multik del_bypass_port <Port Number 1>,<Port Number 2>,...,<Port Number N>
```

Parameters

Parameter	Description
<Port Number>	Specifies the numbers of TCP and UDP ports to remove from the list.

Example

```
[Expert@MyGW:0]# fw ctl multik show_bypass_ports
dynamic dispatcher bypass port list:
[Expert@MyGW:0]#
[Expert@MyGW:0]# cat $FWDIR/conf/dispatcher_bypass.conf
dynamic_dispatcher_bypass_ports_number = 0
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl multik add_bypass_port 8888
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl multik show_bypass_ports
dynamic dispatcher bypass port list:
(8888)
[Expert@MyGW:0]
[Expert@MyGW:0]# cat $FWDIR/conf/dispatcher_bypass.conf
dynamic_dispatcher_bypass_ports_number = 1
dynamic_dispatcher_bypass_port_table=8888
[Expert@MyGW:0]
[Expert@MyGW:0]# fw ctl multik add_bypass_port 9999
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl multik show_bypass_ports
dynamic dispatcher bypass port list:
(8888,9999)
[Expert@MyGW:0]
[Expert@MyGW:0]# cat $FWDIR/conf/dispatcher_bypass.conf
dynamic_dispatcher_bypass_ports_number = 2
dynamic_dispatcher_bypass_port_table=8888,9999
[Expert@MyGW:0]
[Expert@MyGW:0]# fw ctl multik add_bypass_port 9999
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl multik show_bypass_ports
dynamic dispatcher bypass port list:
(8888)
[Expert@MyGW:0]
[Expert@MyGW:0]# cat $FWDIR/conf/dispatcher_bypass.conf
dynamic_dispatcher_bypass_ports_number = 1
dynamic_dispatcher_bypass_port_table=8888
[Expert@MyGW:0]
```

fw ctl multik dynamic_dispatching

Description

Shows and controls the CoreXL Dynamic Dispatcher that dynamically assigns new connections to a CoreXL Firewall instances based on the utilization of CPU cores.

For more information, see sk105261.

Syntax for IPv4

```
fw ctl multik dynamic_dispatching
      get_mode
      off
      on
```

Syntax for IPv6

```
fw6 ctl multik dynamic_dispatching
      get_mode
      off
      on
```

Parameters

Parameter	Description
`get_mode`	Shows the current state of the CoreXL Dynamic Dispatcher.
`off`	Disables the CoreXL Dynamic Dispatcher.
`on`	Enables the CoreXL Dynamic Dispatcher.

Example

```
[Expert@MyGW:0]# fw ctl multik dynamic_dispatching get_mode
Current mode is Off
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl multik dynamic_dispatching on
New mode is: On
Please reboot the system
[Expert@MyGW:0]#
```

fw ctl multik gconn

Description

Shows statistics about CoreXL Global Connections that Security Gateway stores in the kernel table `fw_multik_ld_gconn_table`.

The CoreXL Global Connections table contains information about which CoreXL Firewall instance owns which connections.

Notes:

- This command does not support VSX.
- This command does not support IPv6.

Syntax

```
fw [-d] ctl multik gconn
      -h
      -p
      -sec
      -seg <Number>
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
none	Shows the interactive menu for the CoreXL Firewall Priority Queues.
`-h`	Shows the built-in help.

Parameter	Description
`-p`	Shows the additional information about each CoreXL Firewall instance, including the information about Firewall Priority Queues: ■ `I/O` (In or Out) ■ `Inst. ID` (CoreXL Firewall instance ID) ■ `Flags` ■ `Seq` (Sequence) ■ `Hold_ref` (Hold reference) ■ `Prio` (Firewall Priority Queues mode) ■ `last_enq_jiff` (Jiffies since last enqueue) ■ `queue_indx` (Queue index number) ■ `conn_tokens` (Connection Tokens)
`-s`	Shows the total number of global connections.
`-sec`	Shows the additional information about each CoreXL Firewall instance: ■ `I/O` (In or Out) ■ `Inst. ID` (CoreXL Firewall instance ID) ■ `Flags` ■ `Seq` (Sequence) ■ `Hold_ref` (Hold reference)
`-seg` *<Number>*	Shows the default information about the specified Global Connections Segment.

Example 1 - Default information

```
[Expert@MyGW:0]# fw ctl multik gconn
Default:

================================================================================================================
============================
| Segm | Src IP | S.port | Dst IP | D.port | Proto | Flags | PP |Ref Cnt(I/O)|Inst|PPAK ID|clstr
mem ID|Rec. ref|Rec. Type|

================================================================================================================
============================
|  0   | 192.168.3.52    | 18192 | 192.168.3.240   | 46082 | 6  |FP .. ..| No | 0/0 |  1   | 32 |
 0     |    0   | UNDEF |
|  0   | 192.168.3.52    | 54216 | 192.168.3.240   | 257   | 6  |FP .. ..| No | 0/0 |  1   | 32 |
 0     |    0   | UNDEF |
|  0   | 192.168.3.240   | 53925 | 192.168.3.53    | 18192 | 6  |FP .. ..| No | 0/0 |  0   | 32 |
 1     |    0   | UNDEF |
|  0   | 192.168.3.240   | 257   | 192.168.3.52    | 54216 | 6  |FP .. ..| No | 0/0 |  1   | 32 |
 0     |    0   | UNDEF |
|  0   | 192.168.3.53    | 18192 | 192.168.3.240   | 64216 | 6  |FP .. ..| No | 0/0 |  1   | 32 |
 15    |    0   | UNDEF |
|  0   | 0.0.0.0         | 8116  | 192.168.3.53    | 8116  | 17 |FP .. ..| No | 0/0 |  1   | 32 |
 1     |    0   | UNDEF |
|  0   | 0.0.0.0         | 8116  | 192.168.3.52    | 8116  | 17 |FP .. ..| No | 0/0 |  1   | 32 |
 0     |    0   | UNDEF |
|  0   | 192.168.3.240   | 64216 | 192.168.3.53    | 18192 | 6  |FP .. ..| No | 0/0 |  1   | 32 |
 15    |    0   | UNDEF |
|  0   | 192.168.3.52    | 8116  | 0.0.0.0         | 8116  | 17 |FP .. ..| No | 0/0 |  1   | 32 |
 0     |    0   | UNDEF |
|  0   | 172.20.168.16   | 63800 | 192.168.3.53    | 22    | 6  |FP .. ..| No | 0/0 |  0   | 32 |
 1     |    0   | UNDEF |
|  0   | 192.168.3.240   | 46082 | 192.168.3.52    | 18192 | 6  |FP .. ..| No | 0/0 |  1   | 32 |
 0     |    0   | UNDEF |
|  0   | 192.168.3.53    | 8116  | 0.0.0.0         | 8116  | 17 |FP .. ..| No | 0/0 |  1   | 32 |
 1     |    0   | UNDEF |
|  0   | 192.168.3.53    | 22    | 172.20.168.16   | 63800 | 6  |FP .. ..| No | 0/0 |  0   | 32 |
 1     |    0   | UNDEF |
|  0   | 192.168.3.53    | 18192 | 192.168.3.240   | 53925 | 6  |FP .. ..| No | 0/0 |  0   | 32 |
 1     |    0   | UNDEF |

================================================================================================================
============================
FP - from pool.    T - temporary connection.    PP - pending pernament.
[Expert@MyGW:0]#
```

Example 2 - Summary information only

```
[Expert@MyGW:0]# fw ctl multik gconn -s
Summary:
        Total number of global connections: 12
[Expert@MyGW:0]#
```

Example 3 - Additional information about each CoreXL Firewall instance, including the information about Firewall Priority Queues

```
[Expert@MyGW:0]# fw ctl multik gconn -p
Instance section prio info:

================================================================================================
================================================================================================
=======
| Segm | Src IP | S.port | Dst IP | D.port | Proto | Flags | PP |Ref Cnt(I/O)|Inst|PPAK ID|clstr
mem ID|Rec. ref|Rec. Type|Inst. Section: I/O|Inst. ID|Flags| Seq | Hold_ref |Prio:|last_enq_
jiff|queue_indx|conn_tokens

================================================================================================
================================================================================================
=======
|  0  | 192.168.3.52    | 18192 | 192.168.3.240   | 46082 | 6  |FP .. ..| No | 0/0 |  1  | 32 |
 0    |   0   | UNDEF |Inst. Section: Out |  1  | Perm |  0    |  0  |Prio:|  0  |  -1  |  0  |
|  0  | 192.168.3.240   | 53925 | 192.168.3.53    | 18192 | 6  |FP .. ..| No | 0/0 |  0  | 32 |
 1    |   0   | UNDEF |Inst. Section: In  |  0  | Perm |  0    |  0  |Prio:|  0  |  -1  |  0  |
|  0  | 192.168.3.240   | 257   | 192.168.3.52    | 35883 | 6  |FP .. ..| No | 0/0 |  1  | 32 |
 0    |   0   | UNDEF |Inst. Section: In  |  1  | Perm |  0    |  0  |Prio:|  0  |  -1  |  0  |
|  0  | 192.168.3.53    | 18192 | 192.168.3.240   | 64216 | 6  |FP .. ..| No | 0/0 |  1  | 32 |
 15   |   0   | UNDEF |Inst. Section: Out |  1  | Perm |  0    |  0  |Prio:|  0  |  -1  |  0  |
|  0  | 0.0.0.0         | 8116  | 192.168.3.53    | 8116  | 17 |FP .. ..| No | 0/0 |  1  | 32 |
 1    |   0   | UNDEF |Inst. Section: In  |  1  | Perm |  0    |  0  |Prio:|  0  |  -1  |  0  |
|  0  | 0.0.0.0         | 8116  | 192.168.3.52    | 8116  | 17 |FP .. ..| No | 0/0 |  1  | 32 |
 0    |   0   | UNDEF |Inst. Section: In  |  1  | Perm |  0    |  0  |Prio:|  0  |  -1  |  0  |
|  0  | 192.168.3.240   | 64216 | 192.168.3.53    | 18192 | 6  |FP .. ..| No | 0/0 |  1  | 32 |
 15   |   0   | UNDEF |Inst. Section: In  |  1  | Perm |  0    |  0  |Prio:|  0  |  -1  |  0  |
|  0  | 192.168.3.52    | 8116  | 0.0.0.0         | 8116  | 17 |FP .. ..| No | 0/0 |  1  | 32 |
 0    |   0   | UNDEF |Inst. Section: Out |  1  | Perm |  0    |  0  |Prio:|  0  |  -1  |  0  |
|  0  | 172.20.168.16   | 63800 | 192.168.3.53    | 22    | 6  |FP .. ..| No | 0/0 |  0  | 32 |
 1    |   0   | UNDEF |Inst. Section: In  |  0  | Perm |  494  |  0  |Prio:|  0  |  -1  |  0  |
|  0  | 192.168.3.240   | 46082 | 192.168.3.52    | 18192 | 6  |FP .. ..| No | 0/0 |  1  | 32 |
 0    |   0   | UNDEF |Inst. Section: In  |  1  | Perm |  0    |  0  |Prio:|  0  |  -1  |  0  |
|  0  | 192.168.3.52    | 35883 | 192.168.3.240   | 257   | 6  |FP .. ..| No | 0/0 |  1  | 32 |
 0    |   0   | UNDEF |Inst. Section: Out |  1  | Perm |  0    |  0  |Prio:|  0  |  -1  |  0  |
|  0  | 192.168.3.53    | 8116  | 0.0.0.0         | 8116  | 17 |FP .. ..| No | 0/0 |  1  | 32 |
 1    |   0   | UNDEF |Inst. Section: Out |  1  | Perm |  0    |  0  |Prio:|  0  |  -1  |  0  |
|  0  | 192.168.3.53    | 22    | 172.20.168.16   | 63800 | 6  |FP .. ..| No | 0/0 |  0  | 32 |
 1    |   0   | UNDEF |Inst. Section: Out |  0  | Perm |  280  |  0  |Prio:|  0  |  -1  |  0  |
|  0  | 192.168.3.53    | 18192 | 192.168.3.240   | 53925 | 6  |FP .. ..| No | 0/0 |  0  | 32 |
 1    |   0   | UNDEF |Inst. Section: Out |  0  | Perm |  219  |  0  |Prio:|  0  |  -1  |  0  |

================================================================================================
================================================================================================
=======
FP - from pool.    T - temporary connection.    PP - pending pernament.    In - inbound.    Out
- outbound.
[Expert@MyGW:0]#
```

Example 4 - Additional information about each CoreXL Firewall instance

```
[Expert@MyGW:0]# fw ctl multik gconn -sec
Instance section:

================================================================================================================
================================================================================
| Segm | Src IP | S.port | Dst IP | D.port | Proto | Flags | PP |Ref Cnt(I/O)|Inst|PPAK ID|clstr
mem ID|Rec. ref|Rec. Type|Inst. Section: I/O|Inst. ID|Flags| Seq | Hold_ref |

================================================================================================================
================================================================================
|  0  | 192.168.3.52    | 18192 | 192.168.3.240   | 46082 | 6  |FP .. ..| No | 0/0 |  1  | 32 |
 0    |   0   | UNDEF |Inst. Section: Out |  1  | Perm |  0    |  0  |
|  0  | 192.168.3.52    | 52864 | 192.168.3.240   | 257   | 6  |FP .. ..| No | 0/0 |  2  | 32 |
 0    |   0   | UNDEF |Inst. Section: Out |  2  | Perm |  0    |  0  |
|  0  | 192.168.3.240   | 53925 | 192.168.3.53    | 18192 | 6  |FP .. ..| No | 0/0 |  0  | 32 |
 1    |   0   | UNDEF |Inst. Section: In  |  0  | Perm |  0    |  0  |
|  0  | 192.168.3.53    | 18192 | 192.168.3.240   | 64216 | 6  |FP .. ..| No | 0/0 |  1  | 32 |
 15   |   0   | UNDEF |Inst. Section: Out |  1  | Perm |  0    |  0  |
|  0  | 192.168.3.53    | 60186 | 192.168.3.240   | 257   | 6  |FP .. ..| No | 0/0 |  1  | 32 |
 1    |   0   | UNDEF |Inst. Section: Out |  1  | Perm |  76   |  0  |
|  0  | 0.0.0.0         | 8116  | 192.168.3.53    | 8116  | 17 |FP .. ..| No | 0/0 |  1  | 32 |
 1    |   0   | UNDEF |Inst. Section: In  |  1  | Perm |  0    |  0  |
|  0  | 0.0.0.0         | 8116  | 192.168.3.52    | 8116  | 17 |FP .. ..| No | 0/0 |  1  | 32 |
 0    |   0   | UNDEF |Inst. Section: In  |  1  | Perm |  0    |  0  |
|  0  | 192.168.3.240   | 64216 | 192.168.3.53    | 18192 | 6  |FP .. ..| No | 0/0 |  1  | 32 |
 15   |   0   | UNDEF |Inst. Section: In  |  1  | Perm |  0    |  0  |
|  0  | 192.168.3.52    | 8116  | 0.0.0.0         | 8116  | 17 |FP .. ..| No | 0/0 |  1  | 32 |
 0    |   0   | UNDEF |Inst. Section: Out |  1  | Perm |  0    |  0  |
|  0  | 172.20.168.16   | 63800 | 192.168.3.53    | 22    | 6  |FP .. ..| No | 0/0 |  0  | 32 |
 1    |   0   | UNDEF |Inst. Section: In  |  0  | Perm |  479  |  0  |
|  0  | 192.168.3.240   | 46082 | 192.168.3.52    | 18192 | 6  |FP .. ..| No | 0/0 |  1  | 32 |
 0    |   0   | UNDEF |Inst. Section: In  |  1  | Perm |  0    |  0  |
|  0  | 192.168.3.53    | 8116  | 0.0.0.0         | 8116  | 17 |FP .. ..| No | 0/0 |  1  | 32 |
 1    |   0   | UNDEF |Inst. Section: Out |  1  | Perm |  0    |  0  |
|  0  | 192.168.3.240   | 257   | 192.168.3.52    | 52864 | 6  |FP .. ..| No | 0/0 |  2  | 32 |
 0    |   0   | UNDEF |Inst. Section: In  |  2  | Perm |  0    |  0  |
|  0  | 192.168.3.53    | 22    | 172.20.168.16   | 63800 | 6  |FP .. ..| No | 0/0 |  0  | 32 |
 1    |   0   | UNDEF |Inst. Section: Out |  0  | Perm |  257  |  0  |
|  0  | 192.168.3.53    | 18192 | 192.168.3.240   | 53925 | 6  |FP .. ..| No | 0/0 |  0  | 32 |
 1    |   0   | UNDEF |Inst. Section: Out |  0  | Perm |  219  |  0  |
|  0  | 192.168.3.240   | 257   | 192.168.3.53    | 60186 | 6  |FP .. ..| No | 0/0 |  1  | 32 |
 1    |   0   | UNDEF |Inst. Section: In  |  1  | Perm |  0    |  0  |

================================================================================================================
================================================================================
FP - from pool.    T - temporary connection.    PP - pending pernament.    In - inbound.    Out
- outbound.
[Expert@MyGW:0]#
```

fw ctl multik get_instance

Description

Shows CoreXL Firewall instance that processes the specified IPv4 connection.

Important - This command works only if the CoreXL Dynamic Dispatcher is disabled (see sk105261).

Syntax

- **To show the CoreXL Firewall instance that processes the specified IPv4 connection:**

```
fw ctl multik get_instance sip=<Source IPv4 Address>
dip=<Destination IPv4 Address> proto=<Protocol Number>
```

- **To show the CoreXL Firewall instance that processes the specified range of IPv4 connections:**

```
fw ctl multik get_instance sip=<Source IPv4 Address Start> -
<Source IPv4 Address End> dip=<Destination IPv4 Address Start>
- <Destination IPv4 Address End> proto=<Protocol Number>
```

Parameters

Parameter	Description
<Source IPv4 Address>	Source IPv4 address of the specified connection
<Source IPv4 Address Start>	First source IPv4 address of the specified range of IPv4 addresses
<Source IPv4 Address End>	Last source IPv4 address of the specified range of IPv4 addresses
<Destination IPv4 Address>	Destination IPv4 address of the specified connection
<Destination IPv4 Address Start>	First destination IPv4 address of the specified range of IPv4 addresses
<Destination IPv4 Address End>	Last destination IPv4 address of the specified range of IPv4 addresses
<Protocol Number>	See *IANA Protocol Numbers*. For example: ■ 1 = ICMP ■ 6 = TCP ■ 17 = UDP

Example for a specified IPv4 connection

```
[Expert@MyGW:0]# fw ctl multik get_instance sip=192.168.2.3 dip=172.30.241.66 proto=6
protocol: 6
192.168.2.3 -> 172.30.241.66 => 3
[Expert@MyGW:0]#
```

Example for a specified range of IPv4 connections

```
[Expert@MyGW:0]# fw ctl multik get_instance sip=192.168.2.3-192.168.2.8 dip=172.30.241.66
proto=6
protocol: 6
192.168.2.3 -> 172.30.241.66 => 3
192.168.2.4 -> 172.30.241.66 => 0
192.168.2.5 -> 172.30.241.66 => 3
192.168.2.6 -> 172.30.241.66 => 5
192.168.2.7 -> 172.30.241.66 => 4
192.168.2.8 -> 172.30.241.66 => 5
[Expert@MyGW:0]#
```

fw ctl multik print_heavy_conn

Description

Shows the table with Heavy Connections (that consume the most CPU resources) in the CoreXL Dynamic Dispatcher.

For more information about the CoreXL Dynamic Dispatcher, see sk105261.

CoreXL suspects that a connection is "heavy" if it meets these conditions:

- Security Gateway detected the suspected connection during the last 24 hours
- The suspected connection lasts more than 10 seconds
- CoreXL Firewall instance that processes this connection causes a CPU load of over 60%
- The suspected connection utilizes more than 50% of the total work the applicable CoreXL Firewall instance does

The output table shows this information about the Heavy Connections:

- Source IP address
- Source Port
- Destination IP address
- Destination Port
- Protocol Number
- CoreXL Firewall instance ID that processes this connection
- CoreXL Firewall instance load on the CPU
- Connection's relative load on the CoreXL Firewall instance

Notes:

- This command shows the suspected heavy connections even if they are already closed.
- In the *"cpview" on page 41* utility, go to **CPU > Top-Connections > InstancesX-Y > InstanceZ**. Refer to the **Top Connections** section.

Syntax

```
fw [-d] ctl multik print_heavy_conn
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.

Example

```
[Expert@MyGW:0]# fw ctl multik print_heavy_conn
Source: 192.168.20.31; SPort: 51006; Dest: 172.30.40.55; DPort: 80; IPP: 6; Instance 1; Instance
Load 61%; Connection instance load 100%
Source: 192.168.20.31; SPort: 50994; Dest: 172.30.40.55; DPort: 80; IPP: 6; Instance 1; Instance
Load 61%; Connection instance load 100%
Source: 192.168.20.31; SPort: 50992; Dest: 172.30.40.55; DPort: 80; IPP: 6; Instance 1; Instance
Load 61%; Connection instance load 100%
[Expert@MyGW:0]#
```

fw ctl multik prioq

Description

Configures the CoreXL Firewall Priority Queues. For more information, see sk105762.

Important - This command saves the configuration in the `$FWDIR/conf/prioq_mode.conf` file. You must **not** edit this file manually.

Syntax for IPv4

```
fw ctl multik prioq [{0 | 1 | 2}]
```

Syntax for IPv6

```
fw6 ctl multik prioq [{0 | 1 | 2}]
```

Parameters

Parameter	Description
No Parameters	Shows the interactive menu for configuration of the CoreXL Firewall Priority Queues.
0	Disables the CoreXL Firewall Priority Queues.
1	Enables the CoreXL Firewall Priority Queues in the Evaluator-only mode.
2	Enables the CoreXL Firewall Priority Queues.

Example

```
[Expert@MyGW:0]# fw ctl multik prioq
Current mode is Off

Available modes:
0.      Off
1.      Evaluator-only
2.      On

Choose the desired mode number: (or 3 to Quit)
[Expert@MyGW:0]#
```

fw ctl multik show_bypass_ports

Description

Shows the TCP and UDP ports configured in the bypass port list of the CoreXL Dynamic Dispatcher with the *"fw ctl multik add_bypass_port" on page 1619* command.

For more information about the CoreXL Dynamic Dispatcher, see sk105261.

Important - This command reads the configuration from the `$FWDIR/conf/dispatcher_bypass.conf` file. You must **not** edit this file manually.

Syntax

```
fw ctl multik show_bypass_ports
```

Example

```
[Expert@MyGW:0]# fw ctl multik show_bypass_ports
dynamic dispatcher bypass port list:
(9999,8888)
[Expert@MyGW:0]#
```

fw ctl multik stat

Description

Shows information for each CoreXL Firewall instance.

Syntax for IPv4

```
fw [-d] ctl multik stat
```

Syntax for IPv6

```
fw6 [-d] ctl multik stat
```

Information in the output

- The ID number of each CoreXL Firewall instance (numbers starts from zero).
- The state of each CoreXL Firewall instance.
- The ID number of CPU core, on which the CoreXL Firewall instance runs (numbers starts from the highest available CPU ID).
- The number of concurrent connections the CoreXL Firewall instance currently handles.
- The peak number of concurrent connections the CoreXL Firewall instance handled from the time it started.

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.

Example

```
[Expert@MyGW:0]# fw ctl multik stat
ID | Active  | CPU    | Connections | Peak
----------------------------------------------
 0 | Yes     | 7      |           5 |       21
 1 | Yes     | 6      |           3 |       23
 2 | Yes     | 5      |           5 |       25
 3 | Yes     | 4      |           4 |       21
 4 | Yes     | 3      |           5 |       21
 5 | Yes     | 2      |           5 |       20
[Expert@MyGW:0]#

[Expert@MyGW:0]# fw6 ctl multik stat
ID | Active  | CPU    | Connections | Peak
----------------------------------------------
 0 | Yes     | 7      |           0 |        4
 1 | Yes     | 6      |           0 |        4
[Expert@MyGW:0]#
```

fw ctl multik start

Description

Starts all CoreXL Firewall instances on-the-fly, if they were stopped with the *"fw ctl multik stop" on page 1638* command.

Syntax for IPv4

```
fw ctl multik start
```

Syntax for IPv6

```
fw6 ctl multik start
```

Example

```
[Expert@MyGW:0]# fw ctl multik stat
ID | Active  | CPU    | Connections | Peak
----------------------------------------------
 0 | No      | -      |           6 |       13
 1 | No      | -      |           3 |       11
 2 | No      | -      |           4 |       13
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl multik start
Instance 1 started (2 of 3 are active)
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl multik start
Instance 2 started (3 of 3 are active)
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl multik stat
ID | Active  | CPU    | Connections | Peak
----------------------------------------------
 0 | Yes     | 3      |           5 |       13
 1 | Yes     | 2      |           4 |       11
 2 | Yes     | 1      |           4 |       13
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl multik start
All instances are already active
[Expert@MyGW:0]#
```

fw ctl multik stop

Description

Stops all CoreXL Firewall instances on-the-fly.

Important - To start all CoreXL Firewall instances on-the-fly, run the *"fw ctl multik start" on page 1637* command.

Syntax for IPv4

```
fw ctl multik stop
```

Syntax for IPv6

```
fw6 ctl multik stop
```

Example

```
[Expert@MyGW:0]# fw ctl multik stat
ID | Active  | CPU    | Connections | Peak
----------------------------------------------
 0 | Yes     | 3      |           5 |       13
 1 | Yes     | 2      |           4 |       11
 2 | Yes     | 1      |           4 |       13
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl multik stop
Instance 2 stopped (2 of 3 are active)
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl multik stop
Instance 1 stopped (1 of 3 are active)
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl multik stat
ID | Active  | CPU    | Connections | Peak
----------------------------------------------
 0 | Yes     | 3      |           4 |       13
 1 | No      | -      |           3 |       11
 2 | No      | -      |           7 |       13
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl multik stop
All instances are already inactive
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl multik stat
ID | Active  | CPU    | Connections | Peak
----------------------------------------------
 0 | No      | -      |           6 |       13
 1 | No      | -      |           3 |       11
 2 | No      | -      |           4 |       13
[Expert@MyGW:0]#
```

fw ctl multik utilize

Description

Shows the CoreXL queue utilization for each CoreXL Firewall instance.

Note - This command does not support VSX.

Syntax for IPv4

```
fw ctl multik utilize
```

Syntax for IPv6

```
fw6 ctl multik utilize
```

Example

```
[Expert@MyGW:0]# fw ctl multik utilize
ID | Utilize(%)    | Queue Elements
-----------------------------------
 0 |            1 |             30
 1 |            0 |             10
 2 |            0 |             17
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw6 ctl multik utilize
ID | Utilize(%)    | Queue Elements
-----------------------------------
 0 |            0 |              0
 1 |            0 |              0
[Expert@MyGW:0]#
```

fw ctl affinity

The `fw ctl affinity` command shows and configures the CoreXL affinity settings for:

- Interfaces
- User-space processes
- CoreXL Firewall instances

In addition, see *"taskset_us_all" on page 1674*.

Running the 'fw ctl affinity -l' command in Gateway Mode

Description

The "`fw ctl affinity -l`" command shows the current CoreXL affinity settings on a Security Gateway for:

- Interfaces
- User-space processes
- CoreXL Firewall instances

Syntax

- **To see the built-in help:**

  ```
  fw ctl affinity
  ```

- **To show all the existing affinities:**

  ```
  fw ctl affinity -l [-a] [-v] [-r] [-q]
  ```

- **To show the affinity for a specified interface:**

  ```
  fw ctl affinity -l -i <Interface Name>
  ```

- **To show the affinity for a specified CoreXL Firewall instance:**

  ```
  fw ctl affinity -l -k <CoreXL Firewall instance ID>
  ```

- **To show the affinity for a specified user-space process by its PID:**

  ```
  fw ctl affinity -l -p <Process ID>
  ```

- **To show the affinity for a specified user-space process by its name:**

  ```
  fw ctl affinity -l -n <Process Name>
  ```

- **To show the number of system CPU cores allowed by the installed CoreXL license:**

  ```
  fw -d ctl affinity -corelicnum
  ```

Parameters

Parameter	Description
`-i <Interface Name>`	Shows the affinity for the specified interface.
`-k <CoreXL Firewall instance ID>`	Shows the affinity for the specified CoreXL Firewall instance.
`-p <Process ID>`	Shows the affinity for the Check Point user-space process (for example: *fwd*, *vpnd)* specified by its PID.
`-n <Process Name>`	Shows the affinity for the Check Point user-space process (for example: *fwd*, *vpnd)* specified by its name.
`all`	Shows the affinity for all CPU cores (numbers start from zero).
`<CPU ID0> ... <CPU IDn>`	Shows the affinity for the specified CPU cores (numbers start from zero).
`-a`	Shows all current CoreXL affinities.
`-v`	Shows verbose output with IRQ numbers of interfaces.
`-r`	Shows the CoreXL affinities in reverse order.
`-q`	Suppresses the errors in the output.

Example 1

```
[Expert@MyGW:0]# fw ctl affinity -l
eth0: CPU 0
eth1: CPU 0
eth2: CPU 0
eth3: CPU 0
fw_0: CPU 7
fw_1: CPU 6
fw_2: CPU 5
fw_3: CPU 4
fw_4: CPU 3
fw_5: CPU 2
fwd: CPU 2 3 4 5 6 7
fgd50: CPU 2 3 4 5 6 7
status_proxy: CPU 2 3 4 5 6 7
rad: CPU 2 3 4 5 6 7
cpstat_monitor: CPU 2 3 4 5 6 7
mpdaemon: CPU 2 3 4 5 6 7
cpsead: CPU 2 3 4 5 6 7
cserver: CPU 2 3 4 5 6 7
rtmd: CPU 2 3 4 5 6 7
fwm: CPU 2 3 4 5 6 7
cpsemd: CPU 2 3 4 5 6 7
cpca: CPU 2 3 4 5 6 7
cprid: CPU 2 3 4 5 6 7
cpd: CPU 2 3 4 5 6 7
[Expert@MyGW:0]#
```

Example 2

```
[Expert@MyGW:0]# fw ctl affinity -l -a -v
Interface eth0 (irq 67): CPU 0
Interface eth1 (irq 75): CPU 0
Interface eth2 (irq 83): CPU 0
Interface eth3 (irq 59): CPU 0
fw_0: CPU 7
fw_1: CPU 6
fw_2: CPU 5
fw_3: CPU 4
fw_4: CPU 3
fw_5: CPU 2
fwd: CPU 2 3 4 5 6 7
fgd50: CPU 2 3 4 5 6 7
status_proxy: CPU 2 3 4 5 6 7
rad: CPU 2 3 4 5 6 7
cpstat_monitor: CPU 2 3 4 5 6 7
mpdaemon: CPU 2 3 4 5 6 7
cpsead: CPU 2 3 4 5 6 7
cserver: CPU 2 3 4 5 6 7
rtmd: CPU 2 3 4 5 6 7
fwm: CPU 2 3 4 5 6 7
cpsemd: CPU 2 3 4 5 6 7
cpca: CPU 2 3 4 5 6 7
cprid: CPU 2 3 4 5 6 7
cpd: CPU 2 3 4 5 6 7
[Expert@MyGW:0]#
```

Example 3

```
[Expert@MyGW:0]# fw ctl affinity -l -a -v -r
CPU 0:  eth0 (irq 67) eth1 (irq 75) eth2 (irq 83) eth3 (irq 59)
CPU 1:
CPU 2:  fw_5
        fwd fgd50 status_proxy rad cpstat_monitor mpdaemon cpsead cserver rtmd fwm cpsemd cpca
cprid cpd
CPU 3:  fw_4
        fwd fgd50 status_proxy rad cpstat_monitor mpdaemon cpsead cserver rtmd fwm cpsemd cpca
cprid cpd
CPU 4:  fw_3
        fwd fgd50 status_proxy rad cpstat_monitor mpdaemon cpsead cserver rtmd fwm cpsemd cpca
cprid cpd
CPU 5:  fw_2
        fwd fgd50 status_proxy rad cpstat_monitor mpdaemon cpsead cserver rtmd fwm cpsemd cpca
cprid cpd
CPU 6:  fw_1
        fwd fgd50 status_proxy rad cpstat_monitor mpdaemon cpsead cserver rtmd fwm cpsemd cpca
cprid cpd
CPU 7:  fw_0
        fwd fgd50 status_proxy rad cpstat_monitor mpdaemon cpsead cserver rtmd fwm cpsemd cpca
cprid cpd
All:
[Expert@MyGW:0]#
```

Example 4

```
[Expert@MyGW:0]# fw ctl affinity -l -i eth0
eth0: CPU 0
[Expert@MyGW:0]#
```

Example 5

```
[Expert@MyGW:0]# ps -ef | grep -v grep | egrep "PID|fwd"
UID        PID  PPID  C STIME TTY          TIME CMD
admin    26641 26452  0 Mar27 ?        00:06:56 fwd
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl affinity -l -p 26641
Process 26641: CPU 2 3 4 5 6 7
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl affinity -l -n fwd
fwd: CPU 2 3 4 5 6 7
[Expert@MyGW:0]#
```

Example 6

```
[Expert@MyGW:0]# fw ctl affinity -l -k 1
fw_1: CPU 6
[Expert@MyGW:0]#
```

Example 7

```
[Expert@MyGW:0]# fw -d ctl affinity -corelicnum
[5363 4134733584]@MyGW[4 Apr 18:11:03] Number of system CPUs 8
[5363 4134733584]@MyGW[4 Apr 18:11:03] cplic_get_navailable_cpus: fw_get_allowed_cpus_num
returned invalid value (100000) - all cpus considered as allowed!!!
4
[5363 4134733584]@MyGW[4 Apr 18:11:03] cpKeyTaskManager::~cpKeyTaskManager: called.
[Expert@MyGW:0]#
```

Running the 'fw ctl affinity -l' command in VSX Mode

Description

The `fw ctl affinity -l` command shows the CoreXL affinity settings on a VSX Gateway for:

- Interfaces
- User-space processes
- CoreXL Firewall instances

Note - Before running the `fw ctl affinity -l -x` commands, you must go to the context of the applicable Virtual System or Virtual Router with the Gaia Clish command `set virtual-system <VSID>`.

Syntax

- **To show the affinities in VSX mode (you can combine the optional parameters):**

```
fw ctl affinity -l -x
      [-vsid <VSID ranges>]
      [-cpu <CPU ID ranges>]
      [-flags {e | k | t | n | h | o}]
```

- **To show the number of system CPU cores allowed by the installed CoreXL license:**

```
fw -d ctl affinity -corelicnum
```

Parameters

Parameter	Description
`-vsid <VSID ranges>`	Shows the affinity for: ■ The specified single Virtual System (for example, `-vsid 7`) ■ The specified several Virtual Systems (for example, `-vsid 0-2 4`) **Important** - If you omit the `-vsid` parameter, the command runs in the current virtual context.
`<CPU ID ranges>`	Shows the affinity for: ■ The specified single CPU (for example, `-cpu 7`) ■ The specified several CPU cores (for example, `-cpu 0-2 4`)
`-flags {e | k | t | n | h | o}`	The `-flags` parameter requires at least one of these arguments: ■ `e` - Do not print the exception processes ■ `k` - Do not print the kernel threads ■ `t` - Print all process threads ■ `n` - Print the process name instead of the `/proc/<PID>/cmdline` ■ `h` - Print the CPU mask in Hex format ■ `o` - Print the output into the file called `/tmp/affinity_list_output` **Important** - You must specify multiple arguments together. For example: `-flags tn`

Example 1

```
[Expert@VSX_GW:0]# fw ctl affinity -l -x -cpu 0
-------------------------------------------------------------------
|PID     |VSID |               CPU                    |SRC|V|KT |EXC| NAME
-------------------------------------------------------------------
|      2 |   0 |                                    0 |   | | K |   |
|      3 |   0 |                                    0 |   | | K |   |
|      4 |   0 |                                    0 |   | | K |   |
|     14 |   0 |                                    0 |   | | K |   |
|     99 |   0 |                                    0 |   | | K |   |
|    278 |   0 |                                    0 |   | | K |   |
|    382 |   0 |                                    0 |   | | K |   |
|    674 |   0 |                                    0 |   | | K |   |
|   2195 |   0 |                                    0 |   | | K |   |
|   6348 |   0 |                                    0 |   | | K |   |
|   6378 |   0 |                                    0 |   | | K |   |
-------------------------------------------------------------------
PID   - represents the pid of the process
VSID  - represents the virtual device id
CPU   - represents the CPUs assigned to the specific process
SRC   - represents the source configuration file of the process - (V)SID / (I)nstance /
(P)rocess
V     - represents validity,star means that the actual affinity is different than the configured
affinity
KT    - represents whether the process is a kernel thread
EXC   - represents whether the process belongs to the process exception list (vsaffinity_
exception.conf)
[Expert@VSX_GW:0]#
```

Example 2

```
[Expert@VSX_GW:0]# fw ctl affinity -l -x -vsid 1
-------------------------------------------------------------------
|PID     |VSID |               CPU                    |SRC|V|KT |EXC| NAME
-------------------------------------------------------------------
|   3593 |   1 |                                1 2 3 |   | |   |   | httpd
|  10997 |   1 |                                1 2 3 |   | |   |   | cvpn_rotatelogs
|  11005 |   1 |                                1 2 3 |   | |   |   | httpd
|  22294 |   1 |                                1 2 3 |   | |   |   | routed
|  22328 |   1 |                                1 2 3 |   | |   |   | fwk_wd
|  22333 |   1 |                                1 2 3 | P | |   |   | fwk
|  22488 |   1 |                                1 2 3 |   | |   |   | cpd
|  22492 |   1 |                                1 2 3 |   | |   |   | fwd
|  22504 |   1 |                                1 2 3 |   | |   |   | cpviewd
|  22525 |   1 |                                1 2 3 |   | |   |   | mpdaemon
|  22527 |   1 |                                1 2 3 |   | |   |   | ci_http_server
|  30629 |   1 |                                1 2 3 |   | |   |   | vpnd
|  30631 |   1 |                                1 2 3 |   | |   |   | pdpd
|  30632 |   1 |                                1 2 3 |   | |   |   | pepd
|  30635 |   1 |                                1 2 3 |   | |   |   | fwpushd
|  30743 |   1 |                                1 2 3 |   | |   |   | dbwriter
|  30748 |   1 |                                1 2 3 |   | |   |   | cvpnproc
|  30752 |   1 |                                1 2 3 |   | |   |   | MoveFileServer
|  30756 |   1 |                                1 2 3 |   | |   |   | CvpnUMD
|  30760 |   1 |                                1 2 3 |   | |   |   | Pinger
|  30764 |   1 |                                1 2 3 |   | |   |   | IdlePinger
|  30770 |   1 |                                1 2 3 |   | |   |   | cvpnd
-------------------------------------------------------------------
[Expert@VSX_GW:0]#
```

Running the 'fw ctl affinity -s' command in Gateway Mode

Description

The `fw ctl affinity -s` command configures the CoreXL affinity settings on a Security Gateway for:

- Interfaces
- User-space processes
- CoreXL Firewall instances

Note - The Security Gateway saves these changes in the *$FWDIR/conf/fwaffinity.conf* configuration file.

Syntax

- **To see the built-in help:**

```
fw ctl affinity
```

- **To configure the affinity for a specified interface by its name:**

```
fw ctl affinity -s -i <Interface Name>
      all
      <CPU ID0> [ <CPU ID1> ... <CPU IDn> ]
```

- **To configure the affinity for a specified CoreXL Firewall instance:**

```
fw ctl affinity -s -k <CoreXL Firewall instance ID>
      all
      <CPU ID0> [ <CPU ID1> ... <CPU IDn> ]
```

- **To configure the affinity for a specified user-space process by its PID:**

```
fw ctl affinity -s -p <Process ID>
      all
      <CPU ID0> [ <CPU ID1> ... <CPU IDn> ]
```

- **To configure the affinity for a specified user-space process by its name:**

```
fw ctl affinity -s -n <Process Name>
      all
      <CPU ID0> [ <CPU ID1> ... <CPU IDn> ]
```

Parameters

Parameter	Description
`-i <Interface Name>`	Configures the affinity for the specified interface.
`-k <CoreXL Firewall instance ID>`	Configures the affinity for the specified CoreXL Firewall instance.
`-p <Process ID>`	Configures the affinity for the Check Point user-space process (for example: *fwd*, *vpnd)* specified by its PID.
`-n <Process Name>`	Configures the affinity for the Check Point user-space process (for example: *fwd*, *vpnd)* specified by its name. **Important** - The process name is case-sensitive.
`all`	Configures the affinity for all CPU cores (numbers start from zero).
`<CPU ID0> ... <CPU IDn>`	Configures the affinity for the specified CPU cores (numbers start from zero).

Example 1 - Affine the interface eth1 to the CPU core #1

```
[Expert@MyGW:0]# fw ctl affinity -s -i eth1 1
eth1: CPU 1 - set successfully
Multi-queue affinity was not changed.  For More info, see sk113834.
[Expert@MyGW:0]#
```

Example 2 - Affine the CoreXL Firewall instance #1 to the CPU core #2

```
[Expert@MyGW:0]# fw ctl affinity -s -k 1 2
fw_1: CPU 2 - set successfully
Multi-queue affinity was not changed.  For More info, see sk113834.
[Expert@MyGW:0]#
```

Example 3 - Affine the process CPD by its PID to the CPU core #2

```
[Expert@MyGW:0]# cpwd_admin list | egrep "PID|cpd"
APP         PID    STAT  #START  START_TIME             MON  COMMAND
CPD         6080   E     1       [13:46:27] 17/9/2018   Y    cpd
[Expert@MyGW:0]#
[Expert@MyGW:0]# fw ctl affinity -s -p 6080 2
Process 6080: CPU 2 - set successfully
Multi-queue affinity was not changed.  For More info, see sk113834.
[Expert@MyGW:0]#
```

Example 4 - Affine the process CPD by its name to the CPU core #2

```
[Expert@MyGW:0]# fw ctl affinity -s -n cpd 2
cpd: CPU 2 - set successfully
Multi-queue affinity was not changed.  For More info, see sk113834.
[Expert@MyGW:0]#
```

Running the 'fw ctl affinity -s' command in VSX Mode

Description

The `fw ctl affinity -s` command configures the CoreXL affinity settings on a VSX Gateway for:

- Interfaces
- User-space processes
- CoreXL Firewall instances

Syntax

- **To see the built-in help:**

```
fw ctl affinity
```

- **To configure the affinities of Virtual Systems:**

```
fw ctl affinity -s -d [-vsid <VSID ranges> ] -cpu <CPU ID ranges>
```

- **To configure the affinities of a specified user-space process:**

```
fw ctl affinity -s -d -pname <Process Name> [-vsid <VSID ranges>]
      -cpu all
      -cpu <CPU ID ranges>
```

- **To configure the affinities of specified FWK daemon instances (user-space Firewall):**

```
fw ctl affinity -s -d -inst <Instances Ranges> -cpu <CPU ID ranges>
```

- **To configure the affinities of all FWK instances (user-space Firewalls):**

```
fw ctl affinity -s -d -fwkall <Number of CPUs>
```

- **To reset the affinities to defaults:**

```
fw ctl affinity
      -vsx_factory_defaults
      -vsx_factory_defaults_no_prompt
```

Important

- The VSX Gateway saves these changes in the *$FWDIR/conf/fwaffinity.conf* configuration file.
- When you configure affinity of an interface, it automatically configures the affinities of all other interfaces that share the same IRQ to the same CPU core.

Parameters

Parameter	Description
`-vsid <VSID ranges>`	Configures the affinity for: ■ One specified Virtual System. For example: `-vsid 7` ■ Several specified Virtual Systems. For example: `-vsid 0-2 4` **Note** - If you omit the `-vsid` parameter, the command uses the current virtual context.
`<CPU ID ranges>`	Configures the affinity to: ■ One specified CPU core. For example: `-cpu 7` ■ Several specified CPU cores. For example: `-cpu 0-2 4` **Important** - Numbers of CPU cores start from zero.
`-pname <Process Name>`	Configures the affinity for the Check Point daemon specified by its name (for example: *fwd*, *vpnd)*. **Important** - The process name is case-sensitive.
`-inst <Instances Ranges>`	Configures the affinity for: ■ One specified FWK daemon instance. For example: `-inst 7` ■ Several specified FWK daemon instances. For example: `-inst 0 2 4`

Parameter	Description
`-fwkall <Number of CPUs>`	Configures the affinity for all running FWK daemon instances to the specified number of CPU cores. If it is necessary to affine all running FWK daemon instances to all CPU cores, enter the number of all available CPU cores.
`-vsx_factory_defaults`	Deletes all existing affinity settings and creates the default affinity settings during the next reboot. **Important** - Before this operation, the command prompts the user whether to proceed. You must reboot to complete the operation.
`-vsx_factory_defaults_no_prompt`	Deletes all current affinity settings and creates the default affinity settings during the next reboot. **Important** - Before this operation, the command does **not** prompt the user whether to proceed. You must reboot to complete the operation.

Example 1 - Affine the Virtual Devices #0,1,2,4,7,8 to the CPU cores #0,1,2,4

```
[Expert@MyGW:0]# fw ctl affinity -s -d -vsid 0-2 4 6-8 -cpu 0-2 4
VDevice 0-2 4 6-8 : CPU 0 1 2 4 - set successfully
Multi-queue affinity was not changed.  For More info, see sk113834.
[Expert@MyGW:0]#
```

Example 2 - Affine the process CPD by its name for Virtual Devices #0-12 to the CPU core #7

```
[Expert@MyGW:0]# fw ctl affinity -s -d -pname cpd -vsid 0-12 -cpu 7
VDevice 0-12 : CPU 7 - set successfully
Multi-queue affinity was not changed.  For More info, see sk113834.
Warning: some of the VSIDs did not exist
[Expert@MyGW:0]#
```

Example 3 - Affine the FWK daemon instances #0,2,4 to the CPU core #5

```
[Expert@MyGW:0]# fw ctl affinity -s -d -inst 0 2 4 -cpu 5
VDevice 0 2 4: CPU 5 - set successfully
Multi-queue affinity was not changed.  For More info, see sk113834.
[Expert@MyGW:0]#
```

Example 4 - Affine all FWK daemon instances to the last two CPU cores

```
[Expert@MyGW:0]# fw ctl affinity -s -d -fwkall 2
VDevice 0-2 : CPU 2 3 - set successfully
Multi-queue affinity was not changed.  For More info, see sk113834.
[Expert@MyGW:0]#
```

Example 5 - Affine all FWK daemon instances to all CPU cores

```
[Expert@MyGW:0]# fw ctl affinity -s -d -fwkall 4
There are configured processes/FWK instances
(y) will override all currently configured affinity and erase the configuration files
(n) will set affinity only for unconfigured processes/threads
Do you want to override existing configurations (y/n) ? y
VDevice 0-2 : CPU all - set successfully
Multi-queue affinity was not changed.  For More info, see sk113834.
[Expert@MyGW:0]#
```

fw -i

Description

By default, the *"fw" on page 1068* commands apply to the entire Security Gateway.

The `fw` commands show aggregated information for all CoreXL Firewall instances.

The `fw -i` commands apply to the specified CoreXL Firewall instance.

Syntax

```
fw -i <ID of CoreXL Firewall instance> <Command>
```

Parameters

Parameter	Description
<ID of CoreXL Firewall instance>	Specifies the ID of the CoreXL Firewall instance. To see the available IDs, run the *"fw ctl multik stat" on page 1635* command.
<Command>	Only these commands support the `fw -i` syntax: ■ `fw -i <ID> conntab ...` ■ `fw -i <ID> ctl get ...` ■ `fw -i <ID> ctl leak ...` ■ `fw -i <ID> ctl pstat ...` ■ `fw -i <ID> ctl set ...` ■ `fw -i <ID> monitor ...` ■ `fw -i <ID> tab ...` For details and additional parameters for any of these commands, refer to the corresponding entry for each command.

Example 1 - Show the Connections table for CoreXL Firewall instance #1

```
fw -i 1 tab -t connections
```

Example 2 - Show various internal statistics for CoreXL Firewall instance #1

```
fw -i 1 ctl pstat
```

fwboot bootconf

Description

Configures boot security options.

Notes:

- You must run this command from the Expert mode.
- The settings are saved in the `$FWDIR/boot/boot.conf` file.

  Warning - To avoid issues, do not edit the `$FWDIR/boot/boot.conf` file manually. Edit the file only with this command.
- Refer to these related commands:
  - *"fwboot corexl" on page 1257*
  - *"control_bootsec" on page 973*

Syntax to show the current boot security options

```
[Expert@HostName:0]# $FWDIR/boot/fwboot bootconf
      get_corexl
      get_core_override
      get_def
      get_ipf
      get_ipv6
      get_kernnum
      get_kern6num
```

Syntax to configure the boot security options

```
[Expert@HostName:0]# $FWDIR/boot/fwboot bootconf
      set_corexl {0 | 1}
      set_core_override <number>
      set_def [</path/filename>]
      set_ipf {0 | 1}
      set_ipv6 {0 | 1}
      set_kernnum <number>
      set_kern6num <number>
```

Parameters

Parameter	Description
No Parameters	Shows the built-in help with available parameters.
`get_corexl`	Shows if the CoreXL is enabled or disabled: ■ 0 - disabled ■ 1 - enabled **Note** - In the `$FWDIR/boot/boot.conf` file, refer to the value of the `COREXL_INSTALLED`.
`get_core_override`	Shows the number of overriding CPU cores. The SMT (HyperThreading) feature (sk93000) uses this configuration to set the number of CPU cores after reboot. **Note** - In the `$FWDIR/boot/boot.conf` file, refer to the value of the `CORE_OVERRIDE`.
`get_def`	Shows the configured path and the name of the Default Filter policy file (default is `$FWDIR/boot/default.bin`). **Note** - In the `$FWDIR/boot/boot.conf` file, refer to the value of the `DEFAULT_FILTER_PATH`.
`get_ipf`	Shows if the IP Forwarding during boot is enabled or disabled: ■ 0 - disabled (Security Gateway does not forward traffic between its interfaces during boot) ■ 1 - enabled **Note** - In the `$FWDIR/boot/boot.conf` file, refer to the value of the `CTL_IPFORWARDING`.
`get_ipv6`	Shows if the IPv6 support is enabled or disabled: ■ 0 - disabled ■ 1 - enabled **Note** - In the `$FWDIR/boot/boot.conf` file, refer to the value of the `IPV6_INSTALLED`.
`get_kernnum`	Shows the configured number of IPv4 CoreXL Firewall instances. **Note** - In the `$FWDIR/boot/boot.conf` file, refer to the value of the `KERN_INSTANCE_NUM`.

Parameter	Description
`get_kern6num`	Shows the configured number of IPv6 CoreXL Firewall instances. **Note** - In the `$FWDIR/boot/boot.conf` file, refer to the value of the `KERN6_INSTANCE_NUM`.
`set_corexl {0 | 1}`	Enables or disables CoreXL: ■ 0 - disables ■ 1 - enables **Notes:** ■ In the `$FWDIR/boot/boot.conf` file, refer to the value of the `COREXL_INSTALLED`. ■ To configure CoreXL, use the *"cpconfig" on page 996* menu.
`set_core_ override <number>`	Configures the number of overriding CPU cores. The SMT (HyperThreading) feature (sk93000) uses this configuration to set the number of CPU cores after reboot. **Note** - In the `$FWDIR/boot/boot.conf` file, refer to the value of the `CORE_OVERRIDE`.
`set_def [< /path/filename >]`	Configures the path and the name of the Default Filter policy file (default is `$FWDIR/boot/default.bin`). **Notes:** ■ In the `$FWDIR/boot/boot.conf` file, refer to the value of the `DEFAULT_FILTER_PATH`. ■ If you do not specify the path and the name explicitly, then the value of the `DEFAULT_FILTER_PATH` is set to 0. As a result, Security Gateway does not load a Default Filter during boot. **Best Practice** - The best location for this file is the `$FWDIR/boot/` directory.
`set_ipf {0 | 1}`	Configures the IP forwarding during boot: ■ 0 - disables (forbids the Security Gateway to forward traffic between its interfaces during boot) ■ 1 - enables **Note** - In the `$FWDIR/boot/boot.conf` file, refer to the value of the `CTL_IPFORWARDING`.

Parameter	Description
`set_ipv6 {0 | 1}`	Enables or disables the IPv6 Support: ■ 0 - disables ■ 1 - enables **Notes:** ■ In the `$FWDIR/boot/boot.conf` file, refer to the value of the `IPV6_INSTALLED`. ■ Configure the IPv6 Support in Gaia Portal, or Gaia Clish. See the *R81.20 Gaia Administration Guide*.
`set_kernnum <number>`	Configures the number of IPv4 CoreXL Firewall instances. **Notes:** ■ In the `$FWDIR/boot/boot.conf` file, refer to the value of the `KERN_INSTANCE_NUM`. ■ To configure CoreXL, use the *"cpconfig" on page 996* menu.
`set_kern6num <number>`	Configures the number of IPv6 CoreXL Firewall instances. **Notes:** ■ In the `$FWDIR/boot/boot.conf` file, refer to the value of the `KERN6_INSTANCE_NUM`. ■ To configure CoreXL, use the *"cpconfig" on page 996* menu.

fwboot corexl

Description

Configures and monitors the CoreXL.

Note - The settings are saved in the `$FWDIR/boot/boot.conf` file.

Warning - To avoid issues, do not edit the `$FWDIR/boot/boot.conf` file manually. Edit the file only with this command.

Syntax to show CoreXL configuration

```
[Expert@HostName:0]# $FWDIR/boot/fwboot corexl
      core_count
      curr_instance4_count
      curr_instance6_count
      def_instance4_count
      def_instance6_count
      eligible
      installed
      max_instance4_count
      max_instances4_32bit
      max_instances4_64bit
      max_instance6_count
      max_instances_count
      max_instances_32bit
      max_instances_64bit
      min_instance_count
      unsupported_features
```

Syntax to configure CoreXL

Important:

- The configuration commands are for Check Point use only. To configure CoreXL, use the **Check Point CoreXL** option in the *"cpconfig" on page 996* menu.
- After all changes in CoreXL configuration on the Security Gateway, you must reboot it.
- In a Cluster, you must configure all the Cluster Members in the same way.

```
[Expert@HostName:0]# $FWDIR/boot/fwboot corexl
      def_by_allowed [n]
      default
      [-v] disable
      [-v] enable [n] [-6 k]
      vmalloc_recalculate
```

Parameters

Parameter	Description
No Parameters	Shows the built-in help with available parameters.

`core_count`	Returns the number of CPU cores on this server.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl core_count`
	`[Expert@MyGW:0]# echo $?`
	`4`
	`[Expert@MyGW:0]#`
	`[Expert@MyGW:0]# cat /proc/cpuinfo | grep processor`
	`processor : 0`
	`processor : 1`
	`processor : 2`
	`processor : 3`
	`[Expert@MyGW:0]#`

Parameter	Description

`curr_ instance4_ count`	Returns the current configured number of IPv4 CoreXL Firewall instances.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl curr_ instance4_count`
	`[Expert@MyGW:0]# echo $?`
	`3`
	`[Expert@MyGW:0]#`
	`[Expert@MyGW:0]# fw ctl multik stat`
	`ID | Active | CPU | Connections | Peak`
	`----------`
	` 0 | Yes | 3 | 11 | 18`
	` 1 | Yes | 2 | 12 | 18`
	` 2 | Yes | 1 | 13 | 18`
	`[Expert@MyGW:0]#`

`curr_ instance6_ count`	Returns the current configured number of IPv6 CoreXL Firewall instances.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl curr_ instance6_count`
	`[Expert@MyGW:0]# echo $?`
	`2`
	`[Expert@MyGW:0]#`
	`[Expert@MyGW:0]# fw6 ctl multik stat`
	`ID | Active | CPU | Connections | Peak`
	`----------`
	` 0 | Yes | 3 | 11 | 18`
	` 1 | Yes | 2 | 12 | 18`
	`[Expert@MyGW:0]#`

`def_by_ allowed [n]`	Sets the default configuration for CoreXL according to the specified allowed number of CPU cores.
`default`	Sets the default configuration for CoreXL.

Parameter	Description

`def_ instance4_ count`	Returns the default number of IPv4 CoreXL Firewall instances for this Security Gateway.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl def_ instance4_count`
	`[Expert@MyGW:0]# echo $?`
	`3`
	`[Expert@MyGW:0]#`

`def_ instance6_ count`	Returns the default number of IPv6 CoreXL Firewall instances for this Security Gateway.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl def_ instance6_count`
	`[Expert@MyGW:0]# echo $?`
	`2`
	`[Expert@MyGW:0]#`

`[-v] disable`	Disables CoreXL. ■ `-v` - Leaves the high memory (`vmalloc`) unchanged. See the *"cp_conf corexl" on page 983* command.

`eligible`	Returns whether CoreXL can be enabled on this Security Gateway.
	■ 0 - CoreXL cannot be enabled
	■ 1 - CoreXL can be enabled
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl eligible`
	`[Expert@MyGW:0]# echo $?`
	`1`
	`[Expert@MyGW:0]#`

Parameter	Description
`[-v] enable [n] [-6 k]`	Enables CoreXL with '`n`' IPv4 Firewall instances and optionally '`k`' IPv6 Firewall instances. ■ `-v` - Leaves the high memory (`vmalloc`) unchanged. ■ `n` - Denotes the number of IPv4 CoreXL Firewall instances. ■ `k` - Denotes the number of IPv6 CoreXL Firewall instances. See the *"cp_conf corexl" on page 983* command.

`installed`	Returns whether CoreXL is installed (enabled) on this Security Gateway.
	■ 0 - CoreXL is not enabled
	■ 1 - CoreXL is enabled
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl installed`
	`[Expert@MyGW:0]# echo $?`
	`1`
	`[Expert@MyGW:0]#`

`max_ instance4_ count`	Returns the maximal allowed number of IPv4 CoreXL Firewall instances for this Security Gateway.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl max_ instance4_count`
	`[Expert@MyGW:0]# echo $?`
	`4`
	`[Expert@MyGW:0]#`

`max_ instances 4_32bit`	Returns the maximal allowed number of IPv4 CoreXL Firewall instances for a Security Gateway that runs Gaia with 32-bit kernel.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl max_ instances4_32bit`
	`[Expert@MyGW:0]# echo $?`
	`14`
	`[Expert@MyGW:0]#`

Parameter	Description

`max_instances4_64bit`	Returns the maximal allowed number of IPv4 CoreXL Firewall instances for a Security Gateway that runs Gaia with 64-bit kernel.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl max_instances4_64bit`
	`[Expert@MyGW:0]# echo $?`
	`38`
	`[Expert@MyGW:0]#`

`max_instance6_count`	Returns the maximal allowed number of IPv6 CoreXL Firewall instances for this Security Gateway.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl max_instance6_count`
	`[Expert@MyGW:0]# echo $?`
	`3`
	`[Expert@MyGW:0]#`

`max_instances_count`	Returns the total maximal allowed number of CoreXL Firewall instances (IPv4 and IPv6) for this Security Gateway.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl max_instances_count`
	`[Expert@MyGW:0]# echo $?`
	`40`
	`[Expert@MyGW:0]#`

`max_instances_32bit`	Returns the total maximal allowed number of CoreXL Firewall instances for a Security Gateway that runs Gaia with 32-bit kernel.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl max_instances_32bit`
	`[Expert@MyGW:0]# echo $?`
	`16`
	`[Expert@MyGW:0]#`

Parameter	Description

`max_instances_64bit`	Returns the total maximal allowed number of CoreXL Firewall instances for a Security Gateway that runs Gaia with 64-bit kernel.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl max_instances_64bit`
	`[Expert@MyGW:0]# echo $?`
	`40`
	`[Expert@MyGW:0]#`

`min_instance_count`	Returns the minimal allowed number of IPv4 CoreXL Firewall instances.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl min_instance_count`
	`[Expert@MyGW:0]# echo $?`
	`2`
	`[Expert@MyGW:0]#`

`vmalloc_recalculate`	Updates the value of the `vmalloc` parameter in the `/boot/grub/grub.conf` file.

`unsupported_features`	Returns 1 if at least one feature is configured, which CoreXL does not support.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot corexl unsupported_features`
	`corexl unsupported feature: QoS is configured.`
	`[Expert@MyGW:0]# echo $?`
	`1`
	`[Expert@MyGW:0]#`

fwboot cpuid

Description

Shows the number of available CPUs and CPU cores on this Security Gateway.

Syntax

```
[Expert@HostName:0]# $FWDIR/boot/fwboot cpuid
      {-h | -help | --help}
      -c
      --full
      ht_aware
      -n
      --possible
```

Parameters

Parameter	Description

No Parameters	Shows the IDs of the available CPU cores on this Security Gateway.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot cpuid`
	`3 2 1 0`
	`[Expert@MyGW:0]#`

`-c`	Counts the number of available CPU cores on this Security Gateway. The command stores the returned number as its exit code.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot cpuid -c`
	`[Expert@MyGW:0]# echo $?`
	`4`
	`[Expert@MyGW:0]#`

Parameter	Description

`--full`	Shows a full map of the available CPUs and CPU cores on this Security Gateway.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot cpuid --full`
	`cpuid phys_id core_id thread_id`
	` 0 0 0 0`
	` 1 2 0 0`
	` 2 4 0 0`
	` 3 6 0 0`
	`[Expert@MyGW:0]#`

`ht_aware`	Shows the CPU cores in the order of their awareness of Hyper-Threading.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot cpuid ht_aware`
	`3 2 1 0`
	`[Expert@MyGW:0]#`

`-n`	Counts the number of available CPUs on this Security Gateway.
	The command stores the returned number as its exit code.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot cpuid -n`
	`[Expert@MyGW:0]# echo $?`
	`4`
	`[Expert@MyGW:0]#`

`--possible`	Counts the number of possible CPU cores.
	The command stores the returned number as its exit code.
	Example
	`[Expert@MyGW:0]# $FWDIR/boot/fwboot cpuid --possible`
	`[Expert@MyGW:0]# echo $?`
	`4`
	`[Expert@MyGW:0]#`

fwboot ht

Important - This command is obsolete and is not supported. To configure SMT (HyperThreading) feature, follow sk93000.

fwboot multik_reg

Description

Shows the internal memory address of the registration function for the specified CoreXL Firewall instance.

Important - This command is for Check Point use only.

Note - You must run this command from the Expert mode.

Syntax

```
[Expert@HostName:0]# $FWDIR/boot/fwboot multik_reg <Number of
CoreXL Firewall instance> {ipv4 | ipv6} [-d]
```

Parameters

Parameter	Description
No Parameters	Shows the built-in help with available parameters.
<Number of CoreXL Firewall instance>	Specifies the ID number of the CoreXL Firewall instance.
`ipv4`	Specifies to work with IPv4 CoreXL Firewall instances.
`ipv6`	Specifies to work with IPv6 CoreXL Firewall instances.
`-d`	Shows the decimal 64-bit address of the hook function.

Example

```
[Expert@MyGW:0]# fw ctl multik stat
ID | Active  | CPU    | Connections | Peak
----------------------------------------------
 0 | Yes     | 3      |          11 |       18
 1 | Yes     | 2      |          12 |       18
 2 | Yes     | 1      |          13 |       18
[Expert@MyGW:0]#


[Expert@MyGW:0]# $FWDIR/boot/fwboot multik_reg 0 ipv4
0
[Expert@MyGW:0]#

[Expert@MyGW:0]# $FWDIR/boot/fwboot multik_reg 1 ipv4
0xffffffff8a2a5690
[Expert@MyGW:0]#

[Expert@MyGW:0]# $FWDIR/boot/fwboot multik_reg 2 ipv4
0xffffffff8a2a5690
[Expert@MyGW:0]#
```

fwboot post_drv

Description

Loads the Firewall driver for CoreXL during boot.

Important:

- This command is for Check Point use only.
- If you run this command, Security Gateway can block all traffic. In such case, you must connect to the Security Gateway over a console and restart Check Point services with the *"cpstop" on page 1029* and *"cpstart" on page 1018* commands. Alternatively, you can reboot the Security Gateway.

Note - You must run this command from the Expert mode.

Syntax

```
[Expert@HostName:0]# $FWDIR/boot/fwboot post_drv {ipv4 | ipv6}
```

Parameters

Parameter	Description
No Parameters	Shows the built-in help with available parameters.
`ipv4`	Loads the IPv4 Firewall driver for CoreXL.
`ipv6`	Loads the IPv6 Firewall driver for CoreXL.

taskset_us_all

Description

The script `$FWDIR/bin/taskset_us_all` configures the affinity of all running User Space processes to CPU cores.

- You can enter the required CPU cores either as a list of CPU core IDs, or as a CPU bitmask.
- You can configure the affinity User Space processes to CPU cores that run as CoreXL Firewall instances, as CoreXL SND, or all CPU cores.
- You can configure a list of User Space processes that this script must ignore.
- The script creates this log file: `$FWDIR/log/taskset_us_all.elg`

Note - You must run this command from the Expert mode.

Related Information

"fw ctl affinity" on page 1640

Syntax

```
[Expert@HostName:0]# taskset_us_all
      --help}
      {-i | --instance} [<IDs of Instances>]
      {-l | --list} <IDs of CPU Cores>
            [--ignore_default]
            [--ignore_exe
"<ProcessName1>|<ProcessName2>|...|<ProcessNameN>"
      {-m | --mask} <CPU BitMask>
      {-s | --snd} [--no_zero]
```

On a Scalable Platform Security Group, you must run: `g_all taskset_us_all <parameters>`

Parameters

Parameter	Type	Description
No Parameters	N / A	Shows the syntax to call the built-in help.

Parameter	Type	Description
`--help`	Optional	Shows the built-in help with available parameters.
`{-i | --instance} [<IDs of Instances>]`	Optional	Cnfigures the CPU affinity only to CPU cores that run as CoreXL Firewall Instances. Example for the CoreXL Firewall Instances 0, 2, and 5: `--instance 0,2,5` **Notes:** ■ Mutually exclusive with the parameter '`-s | --snd`'. ■ Not supported in VSX mode.

Parameter	Type	Description
`{-l | --list} <IDs of CPU Cores> [--ignore_default] [--ignore_exe "<ProcessName1>|<ProcessName2>|...|<ProcessNameN>"]`	Mandatory	Configures the script to use the argument as a list of CPU core IDs. Examples for CPU cores from 0 to 3: ■ Comma-separated list: `--list 0,1,2,3` ■ Range of consecutive IDs: `--list 0-3` ■ Range and specific ID: `--list 0-2,3`

Parameter	Type	Description

		Notes:
		■ The optional sub-parameter '`--ignore_default`' configures the script to ignore a predefined list of Check Point executable files.
		There are specific Check Point executable files, whose CPU affinity you must **not** change.
		If you change the CPU affinity of these specific processes, the performance of the Security Gateway **decreases**.
		The predefined list of Check Point executable files to ignore:
		`fwk`, `dmd_run`, `usim_x86`, `usim_wd_agent`, `usim_launcher`
		■ The optional sub-parameter '`--ignore_exe "<ProcessName1>|<ProcessName2>|...|<ProcessNameN>"`' configures the script to ignore the specified executable files.
		Example:
		`--ignore_exe "bash|fwk|clishd"`
		To configure a constant list of ignored executable files, edit the `$FWDIR/bin/taskset_us_all` script and configure the value of the variable '`ignore_list=""`'.

Parameter	Type	Description

`{-m | --mask} <CPU BitMask>`	Mandatory	Configures the script to use the argument as a bitmask of CPU cores IDs.
		Example bitmask for CPU core IDs from 0 to 3 on a Security Gateway with 16 CPU cores:
		`0x0000000000000001 (for CPU 0) +`
		`0x0000000000000010 (for CPU 1) +`
		`0x0000000000000100 (for CPU 2) +`
		`0x0000000000001000 (for CPU 3) =`
		`----------`
		`0x0000000000001111`
		Example bitmask for CPU core IDs 5, 7, 9, and 15 on a Security Gateway with 16 CPU cores:
		`0x0000000000100000 (for CPU 5) +`
		`0x0000000010000000 (for CPU 7) +`
		`0x0000001000000000 (for CPU 9) +`
		`0x1000000000000000 (for CPU 15) =`
		`----------`
		`0x1000001010100000`

`{-s | --snd} [--no_zero]`	Optional	Configures the CPU affinity only to CPU cores that run as CoreXL SND. **Notes:** ■ Mutually exclusive with the parameter '`-i | --instance`'. ■ The optional sub-parameter '`--no_zero`' configures the script to ignore the CPU Core 0.

Multi-Queue Commands

For more information about Multi-Queue, see the *R81.20 Performance Tuning Administration Guide* - Chapter *Multi-Queue*.

mq_mng

You configure Multi-Queue on the command line in one of these shells:

- In the Expert mode
- In Gaia Clish
- In Gaia gClish on Scalable Platforms

Multi-Queue Configuration in the Expert mode

Description

The `mq_mng` utility shows and configures the Multi-Queue on supported interfaces.

Syntax

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- You must run these commands in the Expert mode.
- On Scalable Platforms, you must connect to the applicable Security Group and use the "`g_all mq_mng`" commands.
- Change in the Multi-Queue mode can cause short packet loss.

- **To see the built-in help**

```
mq_mng {-h | --help}
```

- **To show the existing Multi-Queue configuration:**

```
mq_mng {-o | --show} [{-v | -vv}] [-a]
```

- **To configure the Multi-Queue for the specified driver:**

```
mq_mng {-s | --set-mode}
      auto
      manual
            {-i | --interface} <Names of Interfaces>
            {-c | --core} <IDs of CPU Cores>
      off
            [{-i | --interface} <Names of Interfaces>]
```

- **To apply the existing Multi-Queue policy:**

```
mq_mng {-r | --reconf}
```

Parameters

Parameter	Description
`-h | --help`	Shows built-in help.

Parameter	Description
`-o	--show`	Shows the existing Multi-Queue configuration. **Notes**: ■ `Available Queues` - Shows the maximum number of queues available for the given interface. ■ `Actual Queues` - Shows the current number of queues assigned to the given interface. ■ When CoreXL Dynamic-Balancing is disabled, the values of `Available Queues` and `Actual Queues` are the same for both automatic and manual Multi-Queue modes.
`-v	-vv`	Verbose output.
`-a`	Shows all interfaces in the output.
`-s	--set-mode`	Configures the Multi-Queue mode: ■ `auto` - Automatic mode (this is the default). Multi-Queue automatically configures the affinity of all supported interfaces to CPU cores that run CoreXL SND Instances. ■ `manual` - Manual mode. Administrator configures the affinity of interfaces to CPU cores that run CoreXL SND Instances. In this mode, you can specify interfaces, CPU cores, or both. ■ `off` - Disables the Multi-Queue on all or specified supported interfaces. **Important** - Change in the Multi-Queue mode can cause short packet loss.

Parameter	Description

	Notes:
	■ To specify interfaces:
	• Use this syntax:
	`{-i | --interface} <Names of Interfaces>`
	• If you do not specify interfaces, then the configuration applies to all supported interfaces.
	• To specify a specific interface, enter its name (for example: `-i eth2`).
	• To specify several interfaces, enter their names separates with spaces (for example: `-i eth2 eth4`).
	■ To specify CPU cores:
	• Use this syntax:
	`{-c | --core} <IDs of CPU Cores that run CoreXL SND Instances>`
	• To specify a specific CPU core, enter its ID number (for example: `-c 1`).
	• To specify several nonconsecutive CPU cores, enter their ID numbers separated with spaces (for example: `-c 1 3`) or commas (for example: `-c 1,3`).
	• To specify several consecutive CPU cores, enter their first and last ID numbers separated with a hyphen (for example: `-c 3-6`).
	■ To see the current CoreXL affinity configuration, run the *"fw ctl affinity" on page 1640* command (with applicable parameters).
	■ To see the CoreXL Firewall Instances and which CPU cores they use, run the *"fw ctl multik stat" on page 1635* command.
	■ To see all available CPU cores, run:
	`cat /proc/cpuinfo | grep processor`

`-r | --reconf`	Applies the existing Multi-Queue policy.

Examples

Show the current Multi-Queue configuration on all interfaces

```
[Expert@Hostname:0]# mq_mng --show

Total 112 cores. Available for MQ 32 cores: Dynamic-Balancing enabled
i/f             driver          driver mode     state           mode (queues)   cores
                                                                actual/avail
-------------------------------------------------------------------------------------------
---
ethsBP1-01      mlx5_pci        DPDK            Up              Dynamic (10/32)
0,56,1,57,2,58,3,59,4,
                                                                                60
ethsBP1-02      mlx5_pci        DPDK            Up              Dynamic (10/32)
0,56,1,57,2,58,3,59,4,
                                                                                60
```

Show the current Multi-Queue verbose configuration on all interfaces

```
[Expert@Hostname:0]# mq_mng --show -v

Total 112 cores. Available for MQ 32 cores: Dynamic-Balancing enabled:
0,56,1,57,2,58,3,59,4,60,28,84,29,85,30,86,31,87,32,88,5,61,33,89,6,62,34,90,7,63,35,91
i/f             driver          driver mode     state           mode (queues)   cores
                                                                actual/avail
-------------------------------------------------------------------------------------------
---
ethsBP1-01      mlx5_pci        DPDK            Up              Dynamic (10/32)
0,56,1,57,2,58,3,59,4,
                                                                                60
ethsBP1-02      mlx5_pci        DPDK            Up              Dynamic (10/32)
0,56,1,57,2,58,3,59,4,
                                                                                60

core            interfaces      queue                   irq        rx packets      tx
packets
-------------------------------------------------------------------------------------------
---
0               ethsBP1-01      0                       None       18409592        388640
                ethsBP1-02      0                       None       7495723
115534704
1               ethsBP1-01      2                       None       15926139        255839
                ethsBP1-02      2                       None       6633336         975
2               ethsBP1-01      4                       None       16105770        210370
                ethsBP1-02      4                       None       6003514         1096
3               ethsBP1-01      6                       None       19906359        39
                ethsBP1-02      6                       None       7304843         0
4               ethsBP1-01      8                       None       22296468        700
                ethsBP1-02      8                       None       7920505         0
56              ethsBP1-01      1                       None       18902160        166099
                ethsBP1-02      1                       None       6603803         47917
57              ethsBP1-01      3                       None       18508951        187803
                ethsBP1-02      3                       None       7513138         776
58              ethsBP1-01      5                       None       17152508        475
                ethsBP1-02      5                       None       6001529         0
59              ethsBP1-01      7                       None       18597442        55
                ethsBP1-02      7                       None       7320374         0
60              ethsBP1-01      9                       None       21868703        86
                ethsBP1-02      9                       None       7205076         0
```

Show the current Multi-Queue verbose configuration on the interface eth2

```
[Expert@Hostname:0]# mq_mng --show -v -i ethsBP1-01

Total 112 cores. Available for MQ 32 cores: Dynamic-Balancing enabled:
0,56,1,57,2,58,3,59,4,60,28,84,29,85,30,86,31,87,32,88,5,61,33,89,6,62,34,90,7,63,35,91
i/f             driver          driver mode     state           mode (queues)   cores
                                                                actual/avail
       ------------------------------------------------------------------------------------------
----
BPEth0          mlx5_pci        Up              Dynamic (10/32) 0,56,1,57,2,58,3,59,4,
                                                                60

core            interfaces      queue                       irq         rx packets      tx
packets
------------------------------------------------------------------------------------------
---
0               BPEth0          0                           None        18414645        3887732
1               BPEth0          2                           None        15929930        255999
2               BPEth0          4                           None        16110040        210483
3               BPEth0          6                           None        19911262        39
4               BPEth0          8                           None        22302258        700
56              BPEth0          1                           None        18906274        166165
57              BPEth0          3                           None        18513354        187850
58              BPEth0          5                           None        17156988        475
59              BPEth0          7                           None        18601956        55
60              BPEth0          9                           None        21874418        86
```

Set automatic Multi-Queue mode on all interfaces

```
mq_mng --set-mode auto
```

Set manual Multi-Queue mode on the interfaces eth1 and eth2 to CPU cores 0, 1, 2, 4, 5, and 6

```
mq_mng -s manual -i eth1 eth2 -c 0-2 4-6
```

Multi-Queue Configuration in Gaia Clish / Gaia gClish

Syntax

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- You must run these commands in Gaia Clish / Gaia gClish.
- On Scalable Platforms, you must connect to the applicable Security Group.
- Change in the Multi-Queue mode can cause short packet loss.

- **To show the existing Multi-Queue configuration for the specified interface:**

```
show interface <Name of Interface> multi-queue [verbose]
```

- **To configure the Multi-Queue for the specified interface:**

```
set interface <Name of Interface> multi-queue
      auto
      manual core <IDs of CPU Cores that run CoreXL SND
Instances>
      off
```

Parameters

Parameter	Description
<Name of Interface>	Specifies the interface.
`verbose`	Verbose output that also includes: ■ IRQ numbers for traffic queues ■ Total number of RX and TX packets in traffic queues
`auto`	Configures the automatic Multi-Queue mode (this is the default). Multi-Queue automatically configures the affinity of the specified interface to CPU cores that run CoreXL SND Instances.

Parameter	Description
`manual core <IDs of CPU Cores>`	Configures the manual Multi-Queue mode. Administrator configures the affinity of the specified interface to CPU cores that run CoreXL SND Instances. **Notes:** ■ To specify a specific CPU core, enter its ID number (for example: `manual core 1`). ■ To specify several nonconsecutive CPU cores, enter their ID numbers separated with commas and without spaces (for example: `manual core 1,3`). ■ To specify several consecutive CPU cores, enter their first and last ID numbers separated with a hyphen (for example: `manual core 3-6`). ■ To see the current CoreXL affinity configuration, run the *"fw ctl affinity" on page 1640* command (with applicable parameters). ■ To see the CoreXL Firewall Instances and which CPU cores they use, run the *"fw ctl multik stat" on page 1635* command. ■ To see all available CPU cores, run: `cat /proc/cpuinfo | grep processor`
`off`	Disables the Multi-Queue on the specified interface.

Examples

Show Multi-Queue configuration on the interface eth2

```
MyGW> show interface eth2 multi-queue

Total 8 cores. Multiqueue 2 cores
i/f             type            state           config          cores
-------------------------------------------------------------------------
eth2            igb             Up              Auto            4,0

Note: The output does not include network interfaces that are currently in the down state.
MyGW>
```

Show Multi-Queue verbose configuration on the interface eth2

```
MyGW> show interface eth2 multi-queue verbose

Total 8 cores. Multiqueue 2 cores: 0,4
i/f             type            state           config          cores
-------------------------------------------------------------------------
eth2            igb             Up              Auto            4(62),0(79)

core            interfaces      queue                irq        rx packets      tx packets
-----------------------------------------------------------------------------------------
0               eth2            eth2-TxRx-1          79         212             80
4               eth2            eth2-TxRx-0          62         16232           18901
MyGW>
```

Set automatic Multi-Queue mode on the interface eth2

```
set interface eth2 multi-queue auto
```

Set manual Multi-Queue mode on the interface eth2 to CPU cores 0, 1, 2, 4, 5, and 6

```
set interface eth2 multi-queue manual core 0-2,4-6
```

Identity Awareness Commands

For more information about Identity Awareness, see the *R81.20 Identity Awareness Administration Guide*.

These terms are used in the CLI commands:

Term	Description
PDP	Identity AwarenessPolicy Decision Point. This is an Identity AwarenessSecurity Gateway, which is responsible to collect and share identities.
PEP	Identity AwarenessPolicy Enforcement Point. This is an Identity AwarenessSecurity Gateway, which is responsible to enforce network access restrictions. It makes its decisions based on identity data it collected from the **PDP**.
ADLOG	The module responsible for the acquisition of identities of entities (users or computers) from the Active Directory. The `adlog` runs on: ▪ An Identity AwarenessSecurity Gateway, for which you enabled the AD Query. The AD Query serves the Identity AwarenessSoftware Blade, which enforces the policy and logs identities. ▪ A Log Server. The `adlog` logs identities. The `adlog` is the command line process used to control and monitor the ADLOG feature. The command line tool helps control users' statuses, as well as troubleshoot and monitor the system.

The **PEP** and **PDP** processes are key components of the system. Through them, administrators control user access and network protection.

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

adlog

Description

Provides commands to control and monitor the AD Query process.

Syntax

- When the `adlog` runs on a Security Gateway, the AD Query serves the Identity Awareness Software Blade, which enforces policy and logs identities.

  In this case, the command syntax is:

  ```
  adlog a <parameter> [<option>]
  ```

- When the `adlog` runs on a Log Server, it logs identities.

  In this case, the command syntax is:

  ```
  adlog l <parameter> [<option>]
  ```

Note - Parameters for the "`adlog a`" and "`adlog l`" commands are identical.

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
No Parameters	Displays available options for this command and exits.

`a`
or
`l`
	Sets the working mode:
	■ `adlog a`- If you use the AD Query for Identity Awareness.
	■ `adlog l` - If you use a Log Server (Identity Logging).

`control <parameter> <option>`	Sends control commands to the AD Query. See *"adlog control" on page 1692*.
`dc`	Shows the status of a connection to the AD domain controller. See *"adlog dc" on page 1694*.

Parameter	Description
`debug <parameter>`	Enables and disables the `adlog` debug output. See *"adlog debug" on page 1695*.
`query <parameter> <option>`	Shows the database of identities acquired by the AD Query, according to the specified filter. See *"adlog query" on page 1696*.
`statistics`	Shows statistics about NT Event logs received by `adlog`, for each IP address and total. Also shows the number of identified IP addresses. See *"adlog statistics" on page 1697*.

adlog control

Description

Sends control commands to the AD Query.

Syntax

```
adlog {a | l} control
      muh <options>
      reconf
      srv_accounts <options>
      stop
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description

`muh <options>`	Manages the list of Multi-User Hosts.
	The available <*options*> are:
	■ Show all known Multi-User Hosts:
	`adlog {a | l} control muh show`
	■ Add an IP address as a Multi-User Host:
	`adlog {a | l} control muh mark`
	■ Removes an IP address from the list of Multi-User Hosts:
	`adlog {a | l} control muh unmark`

`reconf`	Sends a reconfiguration command to the AD Query. Resets the policy configuration to the one defined in SmartConsole.

Parameter	Description

`srv_ accounts <options>`	Manages service accounts.
	Service accounts are accounts that do not belong to actual users, rather they belong to services that run on a computer. Service accounts are suspected, if they are logged in more than a certain number of times.
	The available <*options*> are:
	■ Show all known service accounts:
	`adlog {a | l} control srv_accounts show`
	■ Clear all the accounts from the list of service accounts:
	`adlog {a | l} control srv_accounts clear`
	■ Manually update the list of service accounts:
	`adlog {a | l} control srv_accounts find`
	■ Remove an account name from the list of service accounts:
	`adlog {a | l} control srv_accounts unmark`

`stop`	Stops the AD Query. Security Gateway does not acquire new identities with the AD Query anymore.

adlog dc

Description

Shows the status of a connection to the AD domain controller.

Syntax

```
adlog a dc
```

```
adlog l dc
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

adlog debug

Description

Enables and disables the `adlog` debug output.

Feature	Output Debug File
Identity Awareness on a Security Gateway	`$FWDIR/log/pdpd.elg`
Identity Logging on a Log Server	`$FWDIR/log/fwd.elg`

Syntax

```
adlog {a | l} debug
      extended
      mode
      off
      on
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`extended`	Turns on the debug and adds extended debug topics.
`mode`	Shows the debug status ("`on`", or "`off`").
`off`	Turns off the debug.
`on`	Turns on the debug.

adlog query

Description

Shows the database of identities acquired by the AD Query, according to the specified filter.

Syntax

```
adlog {a | l} query
      all
      ip <IP Address>
      machine <Computer Name>
      string <String>
      user <Username>
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`all`	No filter. Shows the entire identity database.
`ip <IP Address>`	Filters identities that relate to the specified IP address.
`machine <Computer Name>`	Filters identity mappings based on the specified computer name.
`string <String>`	Filters identity mappings based on the specified text string.
`user <Username>`	Filters identity mappings based on the specified user.

Example - Show the entry that contains the string "jo" in the user name

```
adlog a query user jo
```

adlog statistics

Description

Shows statistics about NT Event logs received by `adlog`, for each IP address and total.

Also shows the number of identified IP addresses.

Syntax

```
adlog a statistics
```

```
adlog l statistics
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

pdp

Description

These commands control and monitor the *pdpd* process.

Syntax

```
pdp <command> [<parameter> [<option>]]
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Commands

Parameter	Description
No Parameters	Shows available options for this command and exits.
`ad <parameter> <option>`	For the AD Query, adds (or removes) an identity to the Identity Awareness database on the Security Gateway. See *"pdp ad" on page 1701*.
`auth <parameter> <option>`	Shows authentication or authorization options. See *"pdp auth" on page 1703*.
`broker <parameter> <option>`	Controls the PDP Identity Broker. See *"pdp broker" on page 1707*.
`conciliation <parameter> <option>`	Controls the session conciliation mechanism. See *"pdp conciliation" on page 1712*.
`connections <parameter>`	Shows the PDP connections with the PEP gateways, Terminal Servers, and Identity Collectors. See *"pdp connections" on page 1714*.
`control <parameter> <option>`	Controls the PDP parameters. See *"pdp control" on page 1715*.
`debug <parameter> <option>`	Controls the PDP debug. See *"pdp debug" on page 1716*.

Parameter	Description
`idc <parameter> <option>`	Operations related to Identity Collector. See *"pdp idc" on page 1719*.
`idp <parameter> <option>`	Operations related to SAML-based authentication. See *"pdp idp" on page 1723*.
`monitor <parameter> <option>`	Monitors the status of connected PDP sessions. See *"pdp monitor" on page 1724*.
`muh <parameter> <option>`	Shows Multi-User Hosts (MUHs). See *"pdp muh" on page 1726*.
`nested_groups <parameter>`	Shows LDAP Nested groups configuration. See *"pdp nested_groups" on page 1727*.
`network <parameter>`	Shows information about network related features. See *"pdp network" on page 1731*.
`radius <parameter> <option>`	Shows and configures the RADIUS accounting options. See *"pdp radius" on page 1732*.
`roles <parameter> <option>`	Shows the user role information. See *"pdp roles" on page 1735*.
`status <parameter>`	Shows PDP status information, such as start time or configuration time. See *"pdp status" on page 1738*.
`tasks_manager <parameter>`	Shows the status of the PDP tasks. See *"pdp tasks_manager" on page 1739*.
`timers <parameter>`	Shows PDP timers information for each session. See *"pdp timers" on page 1740*.
`topology_map`	Shows topology of all PDP and PEP addresses. See *"pdp topology_map" on page 1741*.
`tracker <parameter>`	Adds the TRACKER topic to the PDP logs. See *"pdp tracker" on page 1742*.
`update <parameter>`	Recalculates users and computers group membership. See *"pdp update" on page 1743*.

Parameter	Description
`vpn <parameter>`	Shows connected VPN gateways that send identity data from VPN Remote Access Clients. See *"pdp vpn" on page 1744*.

pdp ad

General Syntax

```
pdp ad
      associate <options>
      disassociate <options>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

The 'pdp ad associate' command

Description

For the AD Query, adds an identity to the Identity Awareness database on the Security Gateway.

The group data must be in the AD.

Syntax

```
pdp ad associate ip <IP Address> u <Username> d <Domain> [m
<Computer Name>] [t <Timeout>] [s]
```

Parameters

Parameter	Description
`ip <IP Address>`	Specifies the IP address for the identity.
`u <Username>`	Specifies the username for the identity.
`d <Domain>`	Specifies the Domain of the ID server.
`m <Computer Name>`	Specifies the computer that is defined for the identity.
`t <Timeout>`	Specifies the timeout for the AD Query. Default timeout is 5 hours.

Parameter	Description
`s`	Associates the "`u <Username>`" and the "`m <Computer>`" parameters sequentially. First, adds the "`<Computer>`" and then adds the "`<Username>`" to the database.

The 'pdp ad disassociate' command

Description

For the AD Query, removes the identity from the Identity Awareness database on the Security Gateway.

Identity Awareness does not authenticate a user that is removed.

Syntax

```
pdp ad disassociate ip <IP Address> {u <Username> | m <Computer
Name>} [r {override | probed | timeout}]
```

Parameters

Parameter	Description
`ip <IP Address>`	Specifies the IP address for the identity.
`u <Username>`	Specifies the username for the identity.
`m <Computer Name>`	Specifies the computer that is defined for the identity.
`r {override | probed | timeout}`	Specifies the reason to show in SmartConsole on the **Logs & Monitor** > **Logs** tab.

pdp auth

Description

Configures authentication/authorization options for PDP.

Syntax

```
pdp auth
      allow_empty_result <options>
      count_in_non_ldap_group <options>
      fetch_by_sid <options>
      force_domain <options>
      kerberos_any_domain <options>
      kerberos_encryption <options>
      reauth_agents_after_policy <options>
      recovery_interval <options>
      username_password <options>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description

`allow_empty_result <options>`	Shows the current configuration of fetching of local groups from the AD server based on SID.
	Configures that the fetching of local groups from the AD server based on SID should succeed, even if all SIDs are foreign.
	The available <*options*> are:
	■ Disable the fetching of local groups:
	`pdp auth allow_empty_result disable`
	■ Enable the fetching of local groups:
	`pdp auth allow_empty_result enable`
	■ Show the current configuration:
	`pdp auth allow_empty_result status`

Parameter	Description

`count_in_non_ldap_group <options>`	Shows and configures the identification of membership to individual users that are selected in the user picker and LDAP branch groups in SmartConsole.
	The available <*options*> are:
	■ Disable the identification of membership:
	`pdp auth count_in_non_ldap_group disable`
	■ Enable the identification of membership:
	`pdp auth count_in_non_ldap_group enable`
	■ Show the current configuration:
	`pdp auth count_in_non_ldap_group status`

`fetch_by_sid <options>`	Shows and configures the fetching of local groups from the AD server based on SID.
	The available <*options*> are:
	■ Disable the fetching of local groups:
	`pdp auth fetch_by_sid disable`
	■ Enable the fetching of local groups:
	`pdp auth fetch_by_sid enable`
	■ Show the current configuration:
	`pdp auth fetch_by_sid status`

`force_domain <options>`	Shows and configures the PDP to match the identity's source, based on the reported domain and authorization domain.
	The available <*options*> are:
	■ Disable the match the identity's source:
	`pdp auth force_domain disable`
	■ Enable the match the identity's source:
	`pdp auth force_domain enable`
	■ Show the current configuration:
	`pdp auth force_domain status`

Parameter	Description

`kerberos_any_domain <options>`	Shows and configures the use of all available Kerberos principles.
	The available <*options*> are:
	■ Disable the use of all available Kerberos principles:
	`pdp auth kerberos_any_domain disable`
	■ Enable the use of all available Kerberos principles:
	`pdp auth kerberos_any_domain enable`
	■ Show the current configuration:
	`pdp auth kerberos_any_domain status`

`kerberos_encryption <options>`	Shows and configures the Kerberos encryption type.
	Note - In SmartConsole, go to **Objects** menu > **Object Explorer** > **Servers** > open the **LDAP Account Unit** object > go to **General** tab > click **Active Directory SSO Configuration**).
	The available <*options*> are:
	■ Configure the Kerberos encryption type:
	`pdp auth kerberos_encryption set`
	■ Show the current configuration:
	`pdp auth kerberos_encryption get`

`reauth_agents_after_policy <options>`	Shows and configures the automatic reauthentication of Identity Agents after policy installation.
	The available <*options*> are:
	■ Disable the automatic reauthentication:
	`pdp auth reauth_agents_after_policy disable`
	■ Enable the automatic reauthentication:
	`pdp auth reauth_agents_after_policy enable`
	■ Show the current configuration:
	`pdp auth reauth_agents_after_policy status`

Parameter	Description

`recovery_interval <options>`	Shows and configures the frequency of attempts to connect back to the higher-priority PDP gateway.
	The available <*options*> are:
	■ Disable the reconnect attemtps:
	`pdp auth recovery_interval disable`
	■ Enable the reconnect attemtps:
	`pdp auth recovery_interval enable`
	■ Configure the frequency or reconnect attempts:
	`pdp auth recovery_interval set <Number of Seconds>`
	■ Show the current configuration:
	`pdp auth recovery_interval show`

`username_password <options>`	Shows and configures the username and password authentication.
	The available <*options*> are:
	■ Disable the username and password authentication:
	`pdp auth username_password disable`
	■ Enable the username and password authentication:
	`pdp auth username_password enable`
	■ Show the current configuration:
	`pdp auth username_password status`

pdp broker

Description

These commands control the PDP Identity Broker.

Syntax

```
pdp broker
      debug {set | unset} <options>
      discard <options>
      identity_cache_mode <options>
      reconnect <options>
      status [-e]
      sync <options>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`debug set <options>` `debug unset <options>`	Controls the debug of the PDP Identity Broker. The available <*options*> are:

	■ Print the logs related to remote Publisher PDPs:
	`pdp broker debug set pub <IP Address of Publisher PDP>`
	■ Disable the logs related to remote Publisher PDPs:
	`pdp broker debug unset pub <IP Address of Publisher PDP>`

Parameter	Description

	■ Print the extended logs related to remote Publisher PDPs:
	`pdp broker debug set pub_ext <IP Address of Publisher PDP>`
	■ Disable the extended logs related to remote Publisher PDPs:
	`pdp broker debug unset pub_ext <IP Address of Publisher PDP>`

	■ Print the logs related to communication with remote Publisher PDPs:
	`pdp broker debug set pub_transport <IP Address of Publisher PDP>`
	Enable this debug on the Subscriber PDP side to observe the Publisher PDP's JSON requests in these cases:
	• To monitor networking issues in case the message was not received.
	• To monitor the JSON requests from the Publisher PDPs and related message-parsing issues.
	• To monitor if the content of the JSON does not meet the requirements (for example: Sharing ID).
	■ Disable the logs related to communication with remote Publisher PDPs:
	`pdp broker debug unset pub_transport <IP Address of Publisher PDP>`

	■ Print the logs related to remote Subscriber PDPs:
	`pdp broker debug set sub <IP Address of Subscriber PDP>`
	■ Disable the logs related to remote Subscriber PDPs:
	`pdp broker debug unset sub <IP Address of Subscriber PDP>`

Parameter	Description

	■ Print the extended logs related to remote Subscriber PDPs:
	`pdp broker debug set sub_ext <IP Address of Subscriber PDP>`
	■ Disable the extended logs related to remote Subscriber PDPs:
	`pdp broker debug unset sub_ext <IP Address of Subscriber PDP>`

	■ Print the logs related to communication with remote Subscriber PDPs:
	`pdp broker debug set sub_transport <IP Address of Subscriber PDP>`
	■ Disable the logs related to communication with remote Subscriber PDPs:
	`pdp broker debug unset sub_transport <IP Address of Subscriber PDP>`

	Notes:
	■ For more information about the debug, see *"pdp debug" on page 1716*.
	■ To see the HTTP related issues, run this command to enable the debug on the Publisher PDP side:
	`pdp debug set HttpClient all`
	To see more information for some errors, run this command:
	`pdp broker status [-e]`

`discard <option>`	Controls the timeout for discarding sessions received from the specified Publisher PDP during a disconnection.
	The available <*options*> are:
	■ Show the current timeout:
	`pdp broker discard show_timeout <IP Address of Publisher PDP>`
	■ Configure the new timeout (in seconds):
	`pdp broker discard set_timeout <IP Address of Publisher PDP> <Timeout>`

Parameter	Description

`identity_cache_mode <option>`	**Important:**
	▪ This feature is available in the R81.20 Jumbo Hotfix Accumulator, Take 70 and higher.
	▪ This feature is **disabled** by default.
	
	Configures the Identity Cache Mode for the PDP-to-PDP sharing protocol (Identity Broker).
	The available <*options*> are:
	▪ Show the current status:
	`pdp broker identity_cache_mode status`
	▪ Enable the Identity Cache Mode:
	`pdp broker identity_cache_mode enable`
	▪ Disable the Identity Cache Mode:
	`pdp broker identity_cache_mode disable`
	▪ Configure the Identity Cache Mode timeout for the PDP-to-PDP sharing protocol (Identity Broker):
	`pdp broker identity_cache_mode set_timeout <Timeout in Seconds>`

`reconnect <IP Address of Subscriber PDP>`	Forces the reconnection to the specified Subscriber PDP immediately. If you run this command, the PDP ignores the keep-alive intervals and exponential backoff timeouts, and sends the handshake / keep-alive immediately. **Best Practice** - You can use this command when a long time passed since the PDP disconnected, and it is necessary to establish the connection again immediately.
`status [-e]`	Shows the status of remote Publisher PDPs and Subscriber PDPs. The option "`-e`" adds more information (Subscriber PDP port and the last error time and description).
`sync <option>`	Synchronizes identities with the specified Publisher PDPs or Subscriber PDPs. The available <*options*> are:

Parameter	Description

	■ Send the synchronization request (in the next broker message) to the specified remote Publisher PDP:
	`pdp broker sync pub <IP Address of Publisher PDP>`
	■ Send the synchronization request (in the next broker message) to all remote Publisher PDPs:
	`pdp broker sync pub all`

	Control the schedule for synchronization with remote Publisher PDPs:
	`pdp broker sync schedule {add <option> | remove <option>| show <option>}`
	■ To add new synchronization time:
	`pdp broker sync schedule add <IP Address of Publisher PDP> "<HH:MM>"`
	■ To remove the current schedule:
	`pdp broker sync schedule remove <IP Address of Publisher PDP> "<HH:MM>"`
	■ To show the current schedule:
	`pdp broker sync schedule show [<IP Address of Publisher PDP>]`

	■ Initiate the synchronization with the specified remote Subscriber PDP:
	`pdp broker sync sub <IP Address of Subscriber PDP>`
	■ Initiate the synchronization with all remote Subscriber PDPs:
	`pdp broker sync sub all`

pdp conciliation

Description

Controls the session conciliation mechanism.

Syntax

```
pdp conciliation
      adq_single_user <option>
      api_multiple_users <option>
      idc_multiple_users <option>
      rad_multiple_users <option>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description

`adq_single_user <option>`	Shows and controls the assumption that single AD Query user is connected on each computer.
	The available <*options*> are:
	■ Disable this behavior:
	`pdp conciliation adq_single_user disable`
	■ Enable this behavior:
	`pdp conciliation adq_single_user enable`
	■ Show the current status (enabled or disabled):
	`pdp conciliation adq_single_user stat`

Parameter	Description

`api_multiple_users <option>`	Shows and controls the assumption that multiple Web-API users are connected on each computer.
	The available <*options*> are:
	■ Disable this behavior:
	`pdp conciliation api_multiple_users disable`
	■ Enable this behavior:
	`pdp conciliation api_multiple_users enable`
	■ Show the current status (enabled or disabled):
	`pdp conciliation api_multiple_users stat`

`idc_multiple_users <option>`	Shows and controls the assumption that multiple Identity Collector users are connected on each computer.
	The available <*options*> are:
	■ Disable this behavior:
	`pdp conciliation idc_multiple_users disable`
	■ Enable this behavior:
	`pdp conciliation idc_multiple_users enable`
	■ Show the current status (enabled or disabled):
	`pdp conciliation idc_multiple_users stat`

`rad_multiple_users <option>`	Shows and controls the assumption that multiple RADIUS users are connected on each computer.
	The available <*options*> are:
	■ Disable this behavior:
	`pdp conciliation rad_multiple_users disable`
	■ Enable this behavior:
	`pdp conciliation rad_multiple_users enable`
	■ Show the current status (enabled or disabled):
	`pdp conciliation rad_multiple_users stat`

pdp connections

Description

Shows the PDP connections with PEP gateways, Terminal Servers, and Identity Collectors.

Syntax

```
pdp connections
      idc
      pep
      ts
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`idc`	Shows a list of connected Identity Collectors.
`pep`	Shows the connection status of all the PEPs, which the current PDP should update.
`ts`	Shows a list of all connected Terminal Servers.

pdp control

Description

Provides commands to control the PDP.

Syntax

```
pdp control
      revoke_ip <IP address>
      sync
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`revoke_ip <IP address>`	Logs out the session that is related to the specified IP address.
`sync`	Forces an initiated synchronization operation between the PDPs and the PEPs. When you run this command, the PDP informs its related PEPs of the up-to-date information of all connected sessions. At the end of this operation, the PDP and the PEPs contain the same and latest session information.

pdp debug

Description

Controls the debug of the PDP.

Syntax

```
pdp debug
      async1
      ccc {off | on}
      memory
      off
      on
      reset
      rotate
      set <Topic Name> <Severity>
      spaces [<0 - 5>]
      stat
      unset <Topic Name>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`async1`	Tests the `async` command line with the `echo` command for 30 seconds.
`ccc {off | on}`	Configures whether to write the CCC debug logs into the PDP log file - `$FWDIR/log/pdpd.elg` ■ `on` - Writes the CCC debug logs ■ `off` - Does not write the CCC debug logs
`memory`	Shows the memory consumption by the *pdpd* daemon.
`off`	Disables the PDP debug.

Parameter	Description
`on`	Enables the PDP debug. **Important** - After you run this command "`pdp debug on`", you must run the command "`pdp debug set ...`" to configure the required filter.
`reset`	Resets the PDP debug options for Debug Topic and Severity. **Important** - After you run this command "`pdp debug reset`", you must run the command "`pdp debug off`" to turn off the debug.
`rotate`	Rotates the PDP log files - increases the index of each log file: 1. `$FWDIR/log/pdpd.elg` becomes `$FWDIR/log/pdpd.elg.0` 2. `$FWDIR/log/pdpd.elg.0` becomes `$FWDIR/log/pdpd.elg.1` 3. And so on.
`set <Topic Name> <Severity>`	Filters which debug logs PDP writes to the log file based on the specified Debug Topics and Severity: The available Debug Topics are: ■ `all` ■ *Check Point Support* provides more specific topics, based on the reported issue The available Severities are: ■ `all` ■ `critical` ■ `events` ■ `important` ■ `surprise` **Best Practice** - We recommend to enable all Topics and all Severities. Run: `pdp debug set all all`

Parameter	Description
`spaces [<0 - 5>]`	Shows and configures the number of indentation spaces in the `$FWDIR/log/pdpd.elg` file. You can specify the number of spaces: ■ 0 (this is the default) ■ 1 ■ 2 ■ 3 ■ 4 ■ 5
`stat`	Shows the PDP current debug status.
`unset <Topic Name>`	Unsets the specified Debug Topic(s).

Important - When you enable the debug, it affects the performance of the *pdpd* daemon. Make sure to disable the debug after you complete your troubleshooting.

pdp idc

Description

Operations related to Identity Collector.

Syntax

```
pdp idc
      groups_consolidation <options>
      groups_update <options>
      muh <options>
      service_accounts <options>
      status
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description

`groups_consolidation <options>`	Shows and configures the consolidation of external groups with fetched groups.
	The available <*options*> are:
	■ Enable the consolidation (this is the default):
	`pdp idc groups_consolidation enable`
	■ Disable the consolidation:
	`pdp idc groups_consolidation disable`
	■ Show the current status:
	`pdp idc groups_consolidation status`

Parameter	Description

`groups_update <options>`	Shows and configures the automatic update of Identity Collector's LDAP Groups.
	For more information, see *Identity Awareness Clients Administration Guide* > chapter "Identity Collector" > section "Identity Collector - Automatic LDAP Group Update"
	The available <*options*> are:
	■ Perform "update all" to get the current LDAP group status:
	`pdp idc groups_update on`
	■ Disable the feature (default):
	`pdp idc groups_update off`
	■ Show the current status of the feature:
	`pdp idc groups_update status`

`muh <options>`	Shows and configures the Multi-User Host detection.
	The available <*options*> are:
	■ Mark an IP address as a Multi-User Host:
	`pdp idc muh mark <IP Address>`
	■ Show known Multi-User Host machines:
	`pdp idc muh show`
	■ Unmark an IP address as a Multi-User Host:
	`pdp idc muh unmark <IP Address>`

Parameter	Description

`service_accounts <options>`	Shows and configures the suspected Service Accounts.
	Important - This feature is enabled by default.
	For more information, see the *Identity Awareness Clients Administration Guide*.
	The available <*options*> are:
	■ Show service account statistics -the current mode, known Service Accounts, and excluded accounts:
	`pdp idc service_accounts show`
	■ Configure the number of simultaneous logins (default is 100), after which all usernames are detected as Service Accounts:
	`pdp idc service_accounts set_threshold <2-1000>`
	■ Enable (this is the default) or disable the Prevent Mode (Auto-Exclude Mode):
	`pdp idc service_accounts set_auto_prevention {enable | disable}`
	Notes:
	• If you disable the Prevent Mode, then Identity Collector works in the Detect Mode.
	• When you change the work mode from Detect to Prevent, all sessions that are marked as a Service Account are revoked.
	■ Mark specific usernames as a Service Account (if prevention is enabled, the sessions for these users are revoked):
	`pdp idc service_accounts mark <username>`
	■ Configure specific usernames **not** to be detected as Service Accounts (continue to enforce identity):
	`pdp idc service_accounts add_exception <username_1> <username_2> ... <username_N>`
	■ Configure specific usernames **to be** detected as Service Accounts, if users log in the specified number of times:
	`pdp idc service_accounts delete_exception <username_1> <username_2> ... <username_N>`
	■ Remove specific usernames from the list of Service Accounts:
	`pdp idc service_accounts unmark_service_accounts`

Parameter	Description
	Note - You must put at least one space between account names. Do not put punctuation between account names. ■ Remove all usernames from the list of Service Accounts: `pdp idc service_accounts unmark_service_accounts_all`
`status`	Shows the status of configured identity sources (Identity Collectors).

pdp idp

Description

Operations related to SAML-based authentication.

Syntax

```
pdp idp groups <options>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description

`groups <options>`	Shows and configures the consolidation of external groups with the fetched groups.
	The available <*options*> are:
	■ Configure the authorization behavior for user groups:
	`pdp idp groups set {only | prefer | union | ignore}`
	• `only` - Considers only groups the Identity Provider sends. Ignore groups received from configured User Directories.
	• `prefer` -Prefers groups the Identity Provider sends. Considers groups received from configured User Directories only if the Identity Provider sends no group. This is the default.
	• `union` - Considers both groups received from configured User Directories and groups the Identity Provider sends.
	• `ignore` - Considers only groups received from configured User Directories. Ignores groups the Identity Provider sends.
	■ Shows the configured behavior:
	`pdp idp groups status`

pdp monitor

Description

Monitors the status of connected PDP sessions.

You can run different queries with the commands below to get the output, in which you are interested.

Syntax

```
pdp monitor
      all
      client_type <Client Type>
      cv_ge <Version>
      cv_le <Version>
      groups <Group Name>
      ip <IP address>
      machine <Computer Name>
      machine_exact
      mad
      network
      s_port
      summary
      user <Username>
      user_exact
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`all`	Shows information for all connected sessions.
`client_type <Client Type>`	Shows all sessions that connect through the specified client type. Possible client types are: ■ `"AD Query"` - User was identified by the AD Query. ■ `"Identity Agent"` - User or computer was identified by an Identity Awareness Agent. ■ `portal` - User was identified by the Captive Portal. ■ `unknown` - User was identified by an unknown source.

Parameter	Description
`cv_ge <Version>`	Shows all sessions that are connected with a client version that is higher than (or equal to) the specified version.
`cv_le <Version>`	Shows all sessions that are connected through a client version that is lower than (or equal to) the specified version.
`groups <Group Name>`	Shows all sessions of users or computers that are members of the specified group.
`ip <IP address>`	Shows session information for the specified IP address.
`machine <Computer Name>`	Shows session information for the specified computer name.
`machine_exact`	Shows sessions filtered by the exact computer name.
`mad`	Shows all sessions that relate to a managed asset. For example, all sessions that successfully performed computer authentication.
`network`	Shows sessions filtered by a network wildcard. For example: `192.168.72.*`
`s_port`	Shows sessions filtered by the assigned source port (MUH sessions only).
`summary`	Shows the summary monitoring data.
`user <Username>`	Shows session information for the specified user name.
`user_exact`	Shows sessions filtered by the exact user.

Example - Show the connected user behind the IP address 192.0.2.1

```
pdp monitor ip 192.0.2.1
```

Note - The last field "`Published`" indicates whether the session information was already published to the Gateway PEPs, whose IP addresses are listed.

pdp muh

Description

Shows Multi-User Hosts (MUHs).

Syntax

```
pdp muh status
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

pdp nested_groups

Description

Configures the Security Gateway queries LDAP Nested Groups.

Shows the current configuration LDAP Nested Group queries.

Syntax

```
pdp nested_groups
      auto_tune {enable | disable}
      clear
      depth <options>
      disable
      enable
      show
      status
      __set_state <options>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`auto_tune {enable | disable}`	Enables and disables the auto-tune feature. This feature calculates and automatically selects the state of Nested Groups based on the LDAP configuration on the Security Gateway and the Management Server. **Notes:** ■ When you enable this feature, the Security Gateway automatically configures the best the state of Nested Groups it calculated. ■ When you disable this feature, the Security Gateway automatically returns to the state of Nested Groups you configured earlier with the "`__set_state`" parameter. **Best Practice** - Enable this feature on the Policy Decision Point (PDP) to increase the performance.
`clear`	Clears the list of users, for which the depth was not enough.
`depth <1 - 40>`	Configures the nested groups depth (between 1 and 40).
`disable`	Disables the nested groups.
`enable`	Enables the nested groups.
`show`	Shows a list of users, for which the depth was not enough.
`status`	Shows the configuration status of nested groups.

Parameter	Description
`__set_state {1 | 2 | 3 | 4 | 5}`	Configures the nested groups state: ■ `1` - Recursive (this is the default) • The Security Gateway queries each user to find out its group memberships, and then queries each group recursively until it determines the nested groups. • We recommend this method for environments that have few nested groups or no nested groups configured on the LDAP server. ■ `2` - Per-user • The Security Gateway sends one LDAP query. The response includes all groups for the specified user, including the nesting levels. The response includes all groups for the given user, including nesting levels. This query shows groups from any branch in the Active Directory forest. This type of query are sent to the Global Catalog ports (TCP 3268 or 3269). • We recommend this method for environments that have a policy that includes access roles with nested groups in them. • Use this state if you work with multiple branches in the account unit, or if you use group membership cross-domain trees. For example, a user belongs to the domain tree `example1.com` and belongs to the different domain tree `example2.com`. See sk134292. ■ `3` - Multi per-group • The Security Gateway sends one LDAP query. This LDAP query includes a user and a group. The response shows if the user is included in this group. • We recommend this method for environments that have all types of users and groups and have a small number of access roles with nested groups in them. ■ `4` - Per user, if there is a single branch in each Account Unit • The Security Gateway sends one LDAP query. The response includes all groups for the specified user, including the nesting levels. This query shows groups from the branch specified in the LDAP account unit. This type of query can work over all LDAP ports (TCP 3268 or 3269, TCP 389 or 636). • Use this state if you work with a single branch on each account unit. ■ `5` - One query per user • This method retrieves a user's group memberships by querying the Active Directory `tokenGroups` attribute. The `tokenGroups` attribute is a computed value that contains the Security Identifiers (SIDs) of all nested security groups to which the user belongs.

Parameter	Description
	• The query can resolve group memberships across domains in the forest and can return an unlimited number of groups. Prerequisites for State 5: • If any Active Directory distribution groups are used in access roles, convert them to security groups in Active Directory. Contact Check Point Support to obtain a script that identifies distribution groups currently selected in access roles. • Ensure that all Active Directory users, computers, and groups referenced in access roles have their SID stored in the Security Managementdatabase. • The Security Gateway recognizes Active Directory primary group memberships. This behavior can affect access role matching. Contact Check Point Support to obtain a script that identifies primary groups used in access roles. • Ensure that a Global Catalog Domain Controller exists in the Active Directory environment. Configure the LDAP Account Unit to use a Domain Controller that is accessible through LDAP port 389 or LDAPS port 636. • We recommend to configure multiple Domain Controllers with the same highest priority in the LDAP Account Unit to improve load balancing and redundancy.

pdp network

Description

Shows information about network related features.

Syntax

```
pdp network {info | registered}
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`info`	Shows a list of networks known by the PDP.
`registered`	Shows the mapping of a network address to the registered gateways (PEP module).

pdp radius

Description

Shows and configures the RADIUS accounting options.

Syntax

```
pdp radius
      ip
            reset
            set <options>
      groups
            fetch <options>
            reset
            set <options>
      parser
            reset
            set <options>
      roles
            fetch <options>
            reset
            set <options>
      status
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description

`ip <options`	Configures the secondary IP options.
	The available <*options*> are:
	■ Set the secondary IP index:
	`pdp radius ip set <attribute index> [-a <vendor specific attribute index>] [-c <vendor code>]`
	■ Reset the secondary IP settings:
	`pdp radius ip reset`

Parameter	Description

`groups <options`	Configures the options for user groups.
	The available <*options*> are:
	■ Control whether to fetch groups from RADIUS messages:
	`pdp radius groups fetch {off | on}`
	• `off` - Do not fetch.
	• `on` - Fetch.
	■ Reset user groups options:
	`pdp radius groups reset`
	■ Set group index:
	`pdp radius groups set <options>`
	• To set group index for machines:
	`pdp radius groups set -m <attribute index> [-a <vendor specific attribute index>] [-c <vendor code>] [-d <delimiter>]`
	• To set group index for users:
	`pdp radius groups set -u <attribute index> [-a <vendor specific attribute index>] [-c <vendor code>] [-d <delimiter>]`

`parser <options`	Configures the parsing options.
	The available <*options*> are:
	■ Reset parsing options:
	`pdp radius parser reset`
	■ Set parsing options for attributes:
	`pdp radius parser set <attribute index> [-c <vendor code> -a <vendor specific attribute index>] -p <prefix> -s <suffix>`

Parameter	Description

`roles <options>`	Configures how to obtain roles from RADIUS messages. The available <*options*> are:
	■ Control whether to fetch roles from RADIUS messages:
	`pdp radius roles fetch {off | on}`
	• `off` - Do not fetch.
	• `on` - Fetch.
	■ Reset role fetch options:
	`pdp radius roles reset`
	■ Set role index:
	`pdp radius roles set <options>`
	• Set role index for machines:
	`pdp radius roles set -m <attribute index> [-a <vendor specific attribute index>] [-c <vendor code>] [-d <delimiter>]`
	• Set role index for users:
	`pdp radius roles set -u <attribute index> [-a <vendor specific attribute index>] [-c <vendor code>] [-d <delimiter>]`

`status`	Shows the current status.

pdp roles

General Syntax

```
pdp roles
      extract
      fetch <options>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

The 'pdp roles extract' command

Description

Extracts and shows the roles from the file `$FWDIR/tmp/roles_command_output.txt` that was created with the "`pdp roles fetch`" command.

Syntax

```
pdp roles extract
```

The 'pdp roles fetch' command

Description

Fetches the roles that match the provided Access Role information and saves the output in the `$FWDIR/tmp/roles_command_output.txt` file.

Syntax

```
pdp roles fetch [-ip <IP Address>]
      -u "<Username>" -is "<Identity Source>"
      -ug "<User Group 1>","<User Group 2>",...
      -mg "<Machine Group 1>","<Machine Group 2>",...
```

Parameters

Parameter	Description
`-ip <IP Address>`	**Optional.** Specifies the IP address of identity, host, or session to calculate and fetch Access Roles that also contain explicitly selected objects in the **Networks** pane. Example for an Access Role object, in which a Host object with the IPv4 address 5.5.5.5 was selected in the **Networks** pane: `pdp roles fetch -i 5.5.5.5 -u "user_1" -is "AD_Query"`

`-u "<Username>" -is "<Identity Source>"`	Specifies the username and the identity source.
	The available identity sources are (case-sensitive):
	▪ `portal`
	▪ `Identity_Agent`
	▪ `Remote_Access`
	▪ `AD_Query`
	▪ `IFMAP`
	▪ `Terminal_Server_Identity_Agent`
	▪ `Radius_Accounting`
	Important - If in the Access Role object you explicitly selected objects in the **Networks** and **Users** panes, you must also use the parameter "`-ip <IP Address>`".
	Examples:
	`pdp roles fetch -u "user_1" -is "AD_Query"`
	`pdp roles fetch -i 5.5.5.5 -u "user_1" -is "AD_Query"`

`-ug "<User Group 1>","<User Group 2>",...`	Specifies the user group. Enter the comma separated list of group names. For Active Directory groups, you must enter the prefix "`ad_group_`". Example for an AD group called "LaptopUsers": `pdp roles fetch -ug "ad_group_LaptopUsers"`

Parameter	Description
`-mg "<Machine Group 1>","<Machine Group 2>", ...`	Specifies the machine group. Enter the comma separated list of group names. For Active Directory groups, you must enter the prefix "`ad_group_`". Example for an AD group called "Laptops": `pdp roles fetch -mg "ad_group_Laptops"`

pdp status

Description

Shows PDP status information, such as start time or configuration time.

Syntax

```
pdp status show
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`show`	Shows PDP information.

pdp tasks_manager

Description

Shows the status of the PDP tasks (current running, previous, and pending tasks).

Syntax

```
pdp tasks_manager status
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`status`	Shows the status of the PDP tasks.

pdp timers

Description

Shows PDP timers information for each PDP session.

Syntax

```
pdp timers show
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`show`	Shows PDP timers information for each PDP session: ■ `User Auth Timer` ■ `Machine Auth Timer` ■ `Pep Cache Timer` ■ `Compliance Timer` ■ `Keep Alive Timer` ■ `Ldap Fetch Timer`

pdp topology_map

Description

Shows topology of all PDP and PEP addresses.

Syntax

```
pdp topology_map
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

pdp tracker

Description

During the PDP debug, adds the `TRACKER` debug topic to the PDP logs (this is enabled by default).

This is very useful when you monitor the PDP-to-PEP identity sharing and other communication in distributed environments.

You can set this manually if you add the `TRACKER` topic to the PDP debug.

Syntax

```
pdp tracker {off | on}
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`off`	Disables the logging of `TRACKER` events in the PDP log.
`on`	Enables the logging of `TRACKER` events in the PDP log.

pdp update

Description

Initiates a recalculation of group membership for all users and computers.

Important - This command does **not** update deleted accounts.

Syntax

```
pdp update {all | specific}
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`all`	Recalculates group membership for all users and computers.
`specific`	Recalculates group membership for a specified user or a computer.

pdp vpn

Description

Shows the connected VPN Gateways that send identity data for VPN Remote Access Client.

Syntax

```
pdp vpn show
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`show`	Shows the connected VPN gateways.

pep

Description

Provides commands to control and monitor the *PEPD* process (see below for options).

Syntax

```
pep <command> [<parameter> [<option>]]
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Commands

Command	Description
`control <parameter> <option>`	Controls the PEP parameters. See *"pep control" on page 1746*.
`debug <parameter> <option>`	Controls the PEP debug. See *"pep debug" on page 1748*.
`show <parameter> <option>`	Shows PEP information. See *"pep show" on page 1750*.
`tracker <parameter>`	During the PEP debug, adds the `TRACKER` debug topic to the PEP logs. See *"pep tracker" on page 1753*.

pep control

Description

Provides commands to control the PEP.

Syntax

```
pep control
      extended_info_storage <options>
      identity_cache_mode <options>
      portal_dual_stack <options>
      tasks_manager status <options>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.
- In the VSNext / Legacy VSX mode, you must run the applicable commands in to the context of the applicable Virtual Gateway / Legacy Virtual System (`vsenv <VS ID>`).

Parameters

Parameter	Description
`extended_info_storage <options>`	Controls whether PEP stores the extended identities information for debug. The available <*options*> are: ▪ `disable` - PEP does not store the information. ▪ `enable` - PEP stores the information.

Parameter	Description

`identity_cache_mode <option>`	**Important:**
	■ This feature is available in the R81.20 Jumbo Hotfix Accumulator, Take 70 and higher.
	■ This feature is **disabled** by default.
	
	Configures the Identity Cache Mode for the PDP-to-PEP sharing protocol.
	The available <*options*> are:
	■ Show the current status:
	`pep control identity_cache_mode status`
	■ Enable the Identity Cache Mode:
	`pep control identity_cache_mode enable`
	■ Disable the Identity Cache Mode (this is the default):
	`pep control identity_cache_mode disable`

`portal_dual_stack <options>`	Controls the support for portal dual stack (IPv4 and IPv6). The available <*options*> are: ■ `disable` - Disables the support. ■ `enable` - Enables the support.
`tasks_manager <options>`	Shows the status of the PEP tasks (current running, previous, and pending tasks). The available <*options*> are: ■ `status` - Shows the status.

pep debug

Description

Controls the debug of the PEP.

Syntax

```
pep debug
      memory
      off
      on
      reset
      rotate
      set <options>
      spaces [<options>]
      stat
      unset <options>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`memory`	Displays the memory consumption by the *pepd* daemon.
`off`	Disables the PEP debug.
`on`	Enables the PEP debug. **Important** - After you run this command "`pep debug on`", you must run the command "`pep debug set ...`" to determine the required filter.
`reset`	Resets the PEP debug options for Debug Topics and Severities. **Important** - After you run this command "`pep debug reset ...`", you must run the command "`pep debug off`" to turn off the debug.

Parameter	Description
`rotate`	Rotates the PEP log files - increases the index of each log file: ■ `$FWDIR/log/pepd.elg` becomes `$FWDIR/log/pepd.elg.0`, ■ `$FWDIR/log/pepd.elg.0` becomes `$FWDIR/log/pepd.elg.1` ■ And so on.
`set <Topic Name> <Severity>`	Filters which debug logs PEP writes to the log file based on the specified Debug Topics and Severity. Available Debug Topics are: ■ `all` ■ Check Point Support provides more specific topics, based on the reported issue Available Severities are: ■ `all` ■ `critical` ■ `events` ■ `important` ■ `surprise` **Best Practice** - We recommend to enable all Topics and all Severities. Run: `pep debug set all all`
`spaces [0 | 1 | 2 | 3 | 4 | 5]`	Displays and sets the number of indentation spaces in the `$FWDIR/log/pepd.elg` file. The default is 0 spaces.
`stat`	Shows the PEP current debug status.
`unset <Topic Name>`	Unsets the specified Debug Topic(s).

Important - When you enable the debug, it affects the performance of the *pepd* daemon. Make sure to turn off the debug after you complete your troubleshooting.

pep show

Description

Shows information about PEP.

Syntax

```
pep show
    conciliation_clashes
        all
        clear
        ip <Session IP Address>
    network
        pdp
        registration
    pdp
        all
        id <ID of PDP>
    stat
    topology_map
    user
        all
        query
                cid <IP[,ID]>
                cmp <Compliance>
                mchn <Computer Name>
                mgrp <Group>
                pdp <IP[,ID]>
                role <Identity Role>
                ugrp <Group>
                uid <UID String>
                usr <Username>
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`conciliation_clashes <options>`	Shows session conciliation clashes. The available <*options*> are: ■ `all` - Show all conciliation clashes. ■ `clear` - Clears all session clashes. ■ `ip <Session IP Address>` - Show all conciliation clashes filtered by the specified session IP address.
`network <options>`	Shows network related information. The available <*options*> are: ■ `pdp` - Shows the Network-to-PDP mapping table. ■ `registration` - Shows the networks registration table.
`pdp <options>`	Shows the communication channel between the PEP and the PDP. Available <*options*> are: ■ `all` - Shows all connected PDPs. ■ `id` - Shows the information for the specified PDP.
`stat`	Shows the last time the *pepd* daemon was started and the last time a policy was received. **Important** - Each time the *pepd* daemon starts, it loads the policy and the two timers. The times between the *pepd* daemon start and when it fetched the policy are very close.
`topology_map`	Shows topology of all PDP and PEP addresses.

Parameter	Description
`user <options>`	Shows the status of sessions that PEP knows. You can perform various queries to get the applicable output (see below). The available <*options*> are: ■ `all` - Shows the list of all clients. ■ `query` - Queries the list of users based on the specified filters: • `cid <IP[,ID]>` - Matches entries of clients with the specified Client ID. • `cmp <Compliance>` - Matches entries with the specified compliance. • `mchn <Computer Name>` - Matches entries with the specified computer name. • `mgrp <Group>` - Matches entries with the specified machine group. • `pdp <IP[,ID]>` - Matches entries, which the specified PDP updated. • `role <Identity Role>` - Matches entries with the specified identity role. • `ugrp <Group>` - Matches entries with the specified user group. • `uid <UID String>` - Matches entries with the specified full or partial UID. • `usr <Username>` - Matches entries with the specified username. **Note** - You can use multiple query filters at the same time to create a logical *AND* correlation between them. For example, to show all users that have a sub-string of "`jo`" AND are part of the user group "`Employees`" you can use this query syntax: `# pep show user query usr jo ugrp Employees`

pep tracker

Description

During the PEP debug, adds the `TRACKER` debug topic to the PEP logs (this is enabled by default).

This is very useful when you monitor the PDP-to-PEP identity sharing and other communication in distributed environments.

You can set this manually if you add the `TRACKER` topic to the PEP debug.

Syntax

```
pep tracker {off | on}
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`off`	Disables the logging of `TRACKER` events in the PEP log.
`on`	Enables the logging of `TRACKER` events in the PEP log.

test_ad_connectivity

Description

This utility runs connectivity tests from the Security Gateway to an AD domain controller.

You can define the parameters for this utility in one of these ways:

- In the command line as specified below
- In the `$FWDIR/conf/test_ad_connectivity.conf` configuration file.

  Parameters you define in the `$FWDIR/conf/test_ad_connectivity.conf` file cannot contain white spaces and cannot be within quotation marks.

Important:

- Parameters you enter in the command line override the parameters you enter in the configuration file.
- This utility saves its output in the file you specify with the "`-o`" parameter.
  In addition, examine the `$FWDIR/log/test_ad_connectivity.elg` file.

Syntax

```
[Expert@HostName:0]# $FWDIR/bin/test_ad_connectivity -h
```

```
[Expert@HostName:0]# $FWDIR/bin/test_ad_connectivity <Parameter_1 Value_1> <Parameter Value_2> ... <Parameter_N Value_N>
 ...<Parameters And Options>
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Mandatory / Optional	Description
`-h`	Optional	Shows the built-in help.

Parameter	Mandatory / Optional	Description
`-a`	**Mandatory** Use only one of these options: ■ `-a` ■ `-c` ■ `-p`	Prompts the user for the password on the screen.
`-b <LDAP Search Base String>`	Optional	Specifies the LDAP Search Base String.
`-c <Password in Clear Text>`	**Mandatory** Use only one of these options: ■ `-a` ■ `-c` ■ `-p`	Specifies the user's password in clear text.
`-d <Domain Name>`	**Mandatory**	Specifies the domain name of the AD (for example, `ad.mycompany.com`).
`-D <User DN>`	**Mandatory**	Overrides the LDAP user DN (the utility does not try to figure out the DN automatically).
`-f <AD Fingerprint for LDAPS>`	Optional	Specifies the AD fingerprint for LDAPS.
`-i <IPv4 address of DC>`	**Mandatory**	Specifies the IPv4 address of the AD domain controller to tested.
`-I <IPv6 address of DC>`	**Mandatory**	Specifies the IPv6 address of the AD domain controller to test.
`-o <File Name>`	**Mandatory**	Specifies the name of the output file. This utility always saves the output file in the `$FWDIR/tmp/` directory.

Parameter	Mandatory / Optional	Description
`-p <Obfuscated Password>`	**Mandatory** Use only one of these options: ■ `-a` ■ `-c` ■ `-p`	Specifies the user's password in obfuscated text.
`-l`	Optional	Runs LDAP connectivity test only (no WMI test).
`-L <Timeout>`	Optional	Specifies the timeout (in milliseconds) for the LDAP test only. If this timeout expires, and the LDAP test still runs, then both LDAP connectivity and WMI connectivity tests fail.
`-M`	Optional	Run the utility in demo mode.
`-r <Port Number>`	Optional	Specifies the LDAP or LDAPS connection port number. The default ports are: ■ LDAP - 389 ■ LDAPS - 636
`-s`	Optional	Specifies that LDAP connection must be over SSL.
`-t <Timeout>`	Optional	Specifies the total timeout (in milliseconds) for both LDAP connectivity and WMI connectivity tests.
`-u <Username>`	**Mandatory**	Specifies the administrator user name on the AD.
`-v`	Optional	Prints the full path to the specified output file.
`-x <Domain Name>`	**Mandatory**	Specifies the domain name of the AD (for example, `ad.mycompany.com`). Utility prompts the user for the password.
`-w`	Optional	Runs WMI connectivity test only (no LDAP test).

Example

IPv4 of AD DC	`192.168.230.240`
Domain	`mydc.local`
Username	`Administrator`
Password	`aaaa`
Syntax	`[Expert@GW:0]# $FWDIR/bin/test_ad_connectivity -u "Administrator" -c "aaaa" -D "CN=Administrator,CN=Users,DC=mydc,DC=local" -d mydc.local -i 192.168.230.240 -b "DC=mydc,DC=local" -o test.txt` `[Expert@GW:0]#`

Output	`[Expert@GW:0]# cat $FWDIR/tmp/test.txt`
	`(`
	`  :status (SUCCESS_LDAP_WMI)`
	`  :err_msg ("WMI_SUCCESS;LDAP_SUCCESS")`
	`  :ldap_status (LDAP_SUCCESS)`
	`  :wmi_status (WMI_SUCCESS)`
	`  :timestamp ("Mon Feb 26 10:17:41 2018")`
	`)`
	`[Expert@GW:0]#`

Note - In order to know the output is authentic, pay attention that the timestamp is the same as the local time.

VPN Commands

VPN commands generate status information regarding VPN processes, or are used to stop and start specific VPN services.

All VPN commands are executed on the Security Gateway and Cluster Members.

For more information about VPN, see the:

- *R81.20 Site to Site VPN Administration Guide*.
- *R81.20 Remote Access VPN Administration Guide*.

ike debug

Background

Starting in R81.10, separate daemons handle different VPN connections.

Starting in R81.20, these are the responsibilities of the different daemons - `vpnd`, `iked`, and `cccd`:

The VPN daemon "vpnd"

Handles these VPN connections:

- All connections from non-IKE Remote Access clients (SSL Network Extender, Capsule VPN)
- Multi-Portal traffic (SSL / TLS) to a Security Gateway

The VPN daemon on a Security Gateway listens on these ports:

- Tunnel Test: 18234 (UDP)
- L2TP: 1701 (UDP)
- Check Point RDP: 259 (UDP)
- Session infrastructure manager: 9996 (TCP)

The "`vpnd`" daemon is a child of the FWD daemon (see the `$FWDIR/conf/fwauthd.conf` file on a Security Gateway).

The IKE daemon "iked"

Introduced in the R81.10 version.

Handles these VPN connections:

- All connections from IKE Remote Access clients (for example, Endpoint clients)
- All IKE Site-to-Site connections from peer Security Gateways
- Large Scale VPN (LSV) connections
- Connections from SmartLSM ROBO gateways

Listens on these ports on a Security Gateway:

- IKE: 30500 - 30563 (UDP)
- IKE NAT-T: 34500 - 34563 (UDP)
- Tunnel Test: 48234 - 48297 (UDP)
- Check Point RDP: 30259 - 30322 (UDP)
- L2TP: 31701 - 31764 (UDP)

CLI Syntax to control the IKE daemon "`iked`":

```
vpn iked {status | enable | disable | calc <Peer IP address>}
```

Starting in R81.20, there can be a maximum of 64 instances of the "iked" daemon that are calculated based on this formula:

```
Number of IKED instances = (Number of CoreXL Firewall Instances)
/ (Value of Kernel Parameter 'ike_num_instances_per_daemon')
```

Note - You can configure different values for the kernel parameter 'ike_num_instances_per_daemon'.

The CCC daemon "cccd"

Introduced in the R81.10 version.

Responsible for the Client Communication Channel (CCC) protocol, while:

- IKE for the same clients runs in the IKE daemon "iked"
- The TLS layer of the CCC protocol for the same clients runs in the VPN daemon "vpnd"

CLI Syntax to control the CCC daemon "cccd":

```
vpn cccd {status | enable | disable}
```

The "cccd" daemon is a child of the FWD daemon (see the $FWDIR/conf/fwauthd.conf file on a Security Gateway).

Enabling and Disabling the IKE daemon "iked"

By default, the IKE daemon "`iked`" is enabled on the Security Gateway.

If you disable the IKE daemon "`iked`", then in such a legacy mode the VPN daemon "`vpnd`" handles all VPN connections.

Procedure to enable the IKE daemon "iked"

Step	Instructions
1	Connect to the command line on the Security Gateway / each Cluster Member.
2	Log in to the Expert mode.
3	Examine the current status: `vpn iked status` Possible outputs: ■ `vpn: 'iked' is enabled` Means the IKE daemon `iked` is enabled (new mode available in R81.10 and higher). This is the default. There is nothing else to do. Stop this procedure. ■ `vpn: 'iked' is disabled` Means the IKE daemon `iked` is disabled (legacy mode as works in R81 and lower). Proceed to the next step.
4	Enable the IKE daemon: `vpn iked enable` **Important:** ■ This command makes the required changes in the `$FWDIR/boot/modules/fwkern.conf` file. ■ This command fetches the local policy (this may disconnect your SSH session). ■ This change survives reboot.

Procedure to disable the IKE daemon "iked"

Step	Instructions
1	Connect to the command line on the Security Gateway / each Cluster Member.
2	Log in to the Expert mode.
3	Examine the current status: `vpn iked status` Possible outputs: ■ `vpn: 'iked' is enabled` Means the IKE daemon `iked` is enabled (new mode in R81.10 and higher). This is the default. Proceed to the next step. ■ `vpn: 'iked' is disabled` Means the IKE daemon `iked` is disabled (legacy mode as works in R81 and lower). There is nothing else to do. Stop this procedure.
4	Disable the IKE daemon: `vpn iked disable` **Important** ■ This command makes the required changes in the `$FWDIR/boot/modules/fwkern.conf` file. ■ This command fetches the local policy (this may disconnect your SSH session) ■ This change survives reboot.

Enabling and Disabling the CCC Daemon "cccd"

By default, the CCC daemon "`cccd`" is disabled on the Security Gateway.

In such a legacy mode, the VPN daemon `vpnd` handles all VPN connections.

If you enable the CCC daemon "`cccd`", then this dedicated daemon handles the Client Communication Channel protocol.

Procedure to enable the CCC daemon "cccd"

Step	Instructions
1	Connect to the command line on the Security Gateway / each Cluster Member.
2	Log in to the Expert mode.
3	Examine the current status: `vpn cccd status` Possible outputs: ■ `vpn: 'cccd' is enabled` Means the CCC daemon `cccd` is enabled (new mode available in R81.10 and higher). There is nothing else to do. Stop this procedure. ■ `vpn: 'cccd' is disabled` Means the CCC daemon `cccd` is disabled (legacy mode as works in R81 and lower). This is the default. Proceed to the next step.
4	Enable the CCC daemon: `vpn cccd enable` **Important:** ■ This command makes the required changes in the `$FWDIR/boot/modules/fwkern.conf` file. ■ This command fetches the local policy (this may disconnect your SSH session) ■ This change survives reboot.

Procedure to disable the CCC daemon "cccd"

Step	Instructions
1	Connect to the command line on the Security Gateway / each Cluster Member.
2	Log in to the Expert mode.
3	Examine the current status: `vpn cccd status` Possible outputs: ■ `vpn: 'cccd' is enabled` Means the CCC daemon `cccd` is enabled (new mode available in R81.10 and higher). Proceed to the next step. ■ `vpn: 'cccd' is disabled` Means the CCC daemon `cccd` is disabled (legacy mode as works in R81 and lower). This is the default. There is nothing else to do. Stop this procedure.
4	Disable the CCC daemon: `vpn cccd disable` **Important** ■ This command makes the required changes in the `$FWDIR/boot/modules/fwkern.conf` file. ■ This command installs the local policy(this may disconnect your SSH session). ■ This change survives reboot.

Description

The "`ike debug`" command instructs the IKE daemon "`iked`" to write debug messages to these log files:

File Description	Log File for each IKED instance

Main debug output file	`$FWDIR/log/iked0.elg`
	`$FWDIR/log/iked1.elg`
	... ...
	`$FWDIR/log/iked64.elg`

IKEv1 output	`$FWDIR/log/iked0.ikev1trace`
	`$FWDIR/log/iked1.ikev1trace`
	... ...
	`$FWDIR/log/iked64.ikev1trace`

IKEv2 output	`$FWDIR/log/iked0.ikev2trace`
	`$FWDIR/log/iked1.ikev2trace`
	... ...
	`$FWDIR/log/iked64.ikev2trace`

Debugging of the IKE daemon "`iked`" is based on Debug Topics and Debug Levels:

- A Debug Topic is a specific area, on which to perform debugging.

  Check Point Support provides the specific Debug Topics when needed.

- Debug Levels range from 1 (least informative) to 5 (most informative - write all debug messages).

In addition, see *"vpn debug" on page 1780*.

How to see the index number of an IKE daemon "iked" that handles a VPN connection

1. Connect to the command line on the Security Gateway / each Cluster Member / Security Group.
2. Log in to the Expert mode.
3. Get the list of all VPN tunnels (see *"vpn tu tlist" on page 1826*):

   ```
   vpn tu tlist -z
   ```

4. Examine these items in the output:
   a. In the top section, examine the row "MSPI:".

      The number that appears after "d:" is the number of the IKE daemon "iked" instance.

   b. In the bottom section, the "Tunnel Mapping" summary shows the IKE daemon "iked" instance that handles this VPN tunnel.

Syntax

Best Practice - Use the command "vpn debug trunc ALL=5" that also enables the debug of the IKE daemon "iked" and of the CCC daemon "cccd". See sk180488.

```
ike debug
      on [<Debug_Topic>=<Debug_Level>]
      off
      ikeon [-s <Size_in_MB>]
      ikeoff
      [-i <IKED Index>] trunc [<Debug_Topic>=<Debug_Level>]
      truncon [<Debug_Topic>=<Debug_Level>]
      truncoff
      timeon [<Seconds>]
      timeoff
      ikefail [-s <Size_in_MB>]
      mon
      moff
      say ["String"]
      tunnel [<Level>]
```

Parameters

Parameter	Description
No Parameters	Shows the built-in usage.

Parameter	Description
`on`	Turns on high level IKE debug. The debug writes the information in these files: ■ `$FWDIR/log/iked<Index>.elg*` ■ `$FWDIR/log/iked<Index>.ikev1trace*` ■ `$FWDIR/log/iked<Index>.ikev2trace*`
<Debug_ Topic>=< Debug_Level>	Specifies the Debug Topic and the Debug Level. *Check Point Support* provides these. **Best Practice** - Run this command to start the debug: `ike debug trunc ALL=5`

`off`	Turns off all IKE debug.
	Best Practice - Run one of these commands to stop the IKE debug:
	`ike debug off`
	`ike debug truncoff`

`ikeon [-s <Size_in_MB>]`	Turns on the IKE trace. The debug writes the information in these files: `$FWDIR/log/iked<Index>.elg*` You can specify the size of the output file, when to perform the log rotation (close the current active file, rename it, open a new active file).
`ikeoff`	Turns off the IKE trace. Run this command to stop the IKE trace: `ike debug ikeoff`

`trunc`
or
`truncon`
	This command:
	1. Rotates the `$FWDIR/log/iked<Index>.elg` file
	2. Rotates the `$FWDIR/log/iked<Index>.ikev1trace*` file
	3. Rotates the `$FWDIR/log/iked<Index>.ikev2trace*` file
	4. Starts the IKE daemon debug
	Best Practice - Run this command to start the IKE debug:
	`ike debug trunc ALL=5`
	Note - Use the "`-i <IKED Index>`" option to start the IKE debug of a specific IKE daemon instance.

Parameter	Description

`truncoff`	Stops the IKE daemon debug.
	Run one of these commands to stop the IKE debug:
	`ike debug truncoff`
	`ike debug off`

`timeon [<Seconds>]`	Enables the timestamp in the log files. Prints one timestamp after the specified number of seconds. By default, prints the timestamp every 10 seconds.
`timeoff`	Disables the timestamp in the log files every number of seconds.
`ikefail [-s <Size_in_MB>]`	Logs failed IKE negotiations. You can specify the size of the output file, when to perform the log rotation (close the current active file, rename it, open a new active file).
`mon`	Enables the IKE Monitor. Writes the IKE packets in this file: `$FWDIR/log/ikemonitor.snoop` **Warning** - The output file may contain user X-Auth passwords. Make sure the file is protected.
`moff`	Disables the IKE Monitor.

`say "String"`	Writes the specified text string in this file:
	`$FWDIR/log/iked<Index>.elg`
	For example, run:
	`ike debug say "BEGIN TEST"`
	Notes:
	■ Run this command after you start the VPN debug (with one of these commands: "`ike debug on`", "`ike debug trunc`", or "`ike debug truncon`").
	■ The length of the string is limited to 255 characters.

Parameter	Description

`tunnel [<Debug_Level>]`	This command:
	1. Rotates the `$FWDIR/log/iked<Index>.elg` file
	2. Starts the IKE daemon debug with these two Debug Topics:
	`tunnel`
	`ikev2`
	If the `<Debug_Level>` is 2,3,4 or 5, then also enables this Debug Topic:
	`CRLCache`
	
	The debug writes the information in these files:
	■ `$FWDIR/log/iked<Index>.elg`
	■ `$FWDIR/log/iked<Index>.ikev1trace*`
	■ `$FWDIR/log/iked<Index>.ikev2trace*`

Return Values

- 0 (zero) for success
- any other value for failure (typically, -1 or 1)

vpn

Description

Configures VPN settings.

Shows VPN information.

Syntax

```
vpn
       check_ttm
       compreset
       compstat
       crl_zap
       crlview
       debug
       dll
       drv
       dump_psk
       ipafile_check
       ipafile_users_capacity
       macutil
       mep_refresh
       neo_proto
       nssm_topology
       overlap_encdom
       rim_cleanup
       rll
       set_slim_server
       set_snx_encdom_groups
       set_trac
       shell
       show_tcpt
       {tunnelutil | tu}
       ver
```

Parameters

Parameter	Description
`check_ttm`	Makes sure the specified TTM file is valid. See *"vpn check_ttm" on page 1774*.

Parameter	Description
`compreset`	Resets compression and decompression statistics counters. See *"vpn compreset" on page 1775*.
`compstat`	Shows compression and decompression statistics counters. See *"vpn compstat" on page 1776*.
`crl_zap`	Erases all Certificate Revocation Lists (CRLs) from the cache. See *"vpn crl_zap" on page 1777*.
`crlview`	Retrieves the Certificate Revocation List (CRL) from various distribution points and shows it for the user. See *"vpn crlview" on page 1778*.
`debug`	Controls the debug of `vpnd` daemon and IKE. See *"vpn debug" on page 1780*.
`dll`	Works with DNS Lookup Layer. See *"vpn dll" on page 1792*.
`drv`	Controls the VPN kernel module. See *"vpn drv" on page 1793*.
`dump_psk`	Shows hash (SHA256) of peers' pre-shared-keys. See *"vpn dump_psk" on page 1794*.
`ipafile_check`	Verifies a candidate for the `$FWDIR/conf/ipassignment.conf` file. See *"vpn ipafile_check" on page 1795*.
`ipafile_users_capacity`	Shows and configures the capacity in the `$FWDIR/conf/ipassignment.conf` file. See *"vpn ipafile_users_capacity" on page 1796*.
`macutil`	Shows a generated MAC address for each user name when you use Remote Access VPN with Office Mode. See *"vpn macutil" on page 1797*.
`mep_refresh`	Initiates MEP re-decision. See *"vpn mep_refresh" on page 1798*.
`neo_proto`	Controls the NEO client protocol. See *"vpn neo_proto" on page 1799*.

Parameter	Description
`nssm_topology`	Generates and uploads a topology in NSSM format to an NSSM server. See *"vpn nssm_toplogy" on page 1800*.
`overlap_ encdom`	Shows all overlapping VPN domains. See *"vpn overlap_encdom" on page 1801*.
`rim_cleanup`	Cleans RIM routes. See *"vpn rim_cleanup" on page 1803*.
`rll`	Works with Route Lookup Layer. See *"vpn rll" on page 1804*.
`set_slim_ server`	Deprecated. See *"vpn set_slim_server" on page 1805*.
`set_snx_ encdom_groups`	Controls the encryption domain per usergroup feature for SSL Network Extender. See *"vpn set_snx_encdom_groups" on page 1806*.
`set_trac`	Controls the TRAC server. See *"vpn set_trac" on page 1807*.
`shell`	VPN Command Line Interface. See *"vpn shell" on page 1808*.
`show_tcpt`	Shows Visitor Mode users. See *"vpn show_tcpt" on page 1815*.
`tunnelutil | tu`	Launches the `TunnelUtil` tool, which is used to control VPN tunnels. See *"vpn tu" on page 1816*.
`ver`	Shows the major version number and build number of the VPN kernel module. See *"vpn ver" on page 1837*.

vpn check_ttm

Description

Makes sure the specified TTM file contains valid syntax.

Syntax

```
vpn check_ttm <Path to TTM file>
```

Parameters

Parameter	Description
<Path to TTM file>	Specifies the full path and name of the TTM file.

Example

```
[Expert@MyGW:0]# find / -name \*.ttm -type f
find: /proc/64899: No such file or directory
/var/opt/CPsuite-R81.20/fw1/conf/fw_client_1.ttm
/var/opt/CPsuite-R81.20/fw1/conf/nemo_client_1.ttm
/var/opt/CPsuite-R81.20/fw1/conf/neo_client_1.ttm
/var/opt/CPsuite-R81.20/fw1/conf/iphone_client_1.ttm
/var/opt/CPsuite-R81.20/fw1/conf/topology_trans_tmpl.ttm
/var/opt/CPsuite-R81.20/fw1/conf/vpn_client_1.ttm
/var/opt/CPsuite-R81.20/fw1/conf/trac_client_1.ttm
... ... ...
[Expert@MyGW:0]#
[Expert@MyGW:0]# vpn check_ttm /var/opt/CPsuite-R81.20/fw1/conf/trac_client_1.ttm

 Summary for the file: trac_client_1.ttm
        result: the file passed the check without any problems

[Expert@MyGW:0]#
```

vpn compreset

Description

Resets compression and decompression statistics counters.

Syntax

```
vpn compreset
```

Example

```
[Expert@MyGW:0]# vpn compreset
Compression statistics were reset.
[Expert@MyGW:0]#
```

vpn compstat

Description

Shows compression and decompression statistics counters.

Syntax

```
vpn compstat
```

Example

```
[Expert@MyGW:0]# vpn compstat

Compression: sum of all instances :

Compression:
============
Bytes before compression         : 0
Bytes after compression          : 0
Compression overhead (bytes)     : 0
Bytes that were not compressed   : 0
Compressed packets               : 0
Packets that were not compressed : 0
Compression errors               : 0

Pure compression ratio           : 0.000000
Effective compression ratio      : 0.000000

Decompression:
==============
Bytes before decompression       : 0
Bytes after decompression        : 0
Decompression overhead (bytes)   : 0
Decompressed packets             : 0
Decompression errors             : 0
Pure decompression ratio         : 0.000000
[Expert@MyGW:0]#
```

vpn crl_zap

Description

Erases all Certificate Revocation Lists (CRLs) from the cache.

Syntax

```
vpn crl_zap
```

Return Values

- 0 (zero) for success
- any other value for failure

vpn crlview

Description

Retrieves the Certificate Revocation List (CRL) from various distribution points and shows it for the user.

Syntax

```
vpn crlview [-d]
      -obj <Network Object Name> -cert <Certificate Object Name>
      -f <Certificate File>
      -view
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`-obj <Network Object Name>`	Specifies the name of the CA network object.
`-cert <Certificate Object Name>`	Specifies the name of the certificate object.
`-f <Certificate File>`	Specifies the path and the name of the certificate file.
`-view`	Shows the CRL.

Return Values

- 0 (zero) for success
- any other value for failure

Example 1

```
vpn crlview -obj <MyCA> -cert <MyCert>
```

1. The VPN daemon contacts the Certificate Authority called **MyCA** and locates the certificate called **MyCert**.
2. The VPN daemon extracts the certificate distribution point from the certificate.
3. The VPN daemon goes to the distribution point and retrieves the CRL. The distribution point can be an LDAP or HTTP server.
4. The VPN daemon shows it to the standard output.

Example 2

```
vpn crlview -f /var/log/MyCert
```

1. The VPN daemon extracts the certificate distribution point from the certificate file called **MyCert**.
2. The VPN daemon goes to the distribution point and retrieves the CRL. The distribution point can be an LDAP or HTTP server.
3. The VPN daemon shows the CRL to the standard output.

Example 3

```
vpn crlview -view <Lastest CRL>
```

If the CRL was retrieved in the past, this command instructs the VPN daemon to show the contents to the standard output.

vpn debug

Background

Starting in R81.10, separate daemons handle different VPN connections.

Starting in R81.20, these are the responsibilities of the different daemons - `vpnd`, `iked`, and `cccd`:

The VPN daemon "vpnd"

Handles these VPN connections:

- All connections from non-IKE Remote Access clients (SSL Network Extender, Capsule VPN)
- Multi-Portal traffic (SSL / TLS) to a Security Gateway

The VPN daemon on a Security Gateway listens on these ports:

- Tunnel Test: 18234 (UDP)
- L2TP: 1701 (UDP)
- Check Point RDP: 259 (UDP)
- Session infrastructure manager: 9996 (TCP)

The "`vpnd`" daemon is a child of the FWD daemon (see the `$FWDIR/conf/fwauthd.conf` file on a Security Gateway).

The IKE daemon "iked"

Introduced in the R81.10 version.

Handles these VPN connections:

- All connections from IKE Remote Access clients (for example, Endpoint clients)
- All IKE Site-to-Site connections from peer Security Gateways
- Large Scale VPN (LSV) connections
- Connections from SmartLSM ROBO gateways

Listens on these ports on a Security Gateway:

- IKE: 30500 - 30563 (UDP)
- IKE NAT-T: 34500 - 34563 (UDP)
- Tunnel Test: 48234 - 48297 (UDP)
- Check Point RDP: 30259 - 30322 (UDP)
- L2TP: 31701 - 31764 (UDP)

CLI Syntax to control the IKE daemon "`iked`":

```
vpn iked {status | enable | disable | calc <Peer IP address>}
```

Starting in R81.20, there can be a maximum of 64 instances of the "iked" daemon that are calculated based on this formula:

```
Number of IKED instances = (Number of CoreXL Firewall Instances)
/ (Value of Kernel Parameter 'ike_num_instances_per_daemon')
```

Note - You can configure different values for the kernel parameter 'ike_num_instances_per_daemon'.

The CCC daemon "cccd"

Introduced in the R81.10 version.

Responsible for the Client Communication Channel (CCC) protocol, while:

- IKE for the same clients runs in the IKE daemon "iked"
- The TLS layer of the CCC protocol for the same clients runs in the VPN daemon "vpnd"

CLI Syntax to control the CCC daemon "cccd":

```
vpn cccd {status | enable | disable}
```

The "cccd" daemon is a child of the FWD daemon (see the $FWDIR/conf/fwauthd.conf file on a Security Gateway).

Enabling and Disabling the IKE daemon "iked"

By default, the IKE daemon "`iked`" is enabled on the Security Gateway.

If you disable the IKE daemon "`iked`", then in such a legacy mode the VPN daemon "`vpnd`" handles all VPN connections.

Procedure to enable the IKE daemon "iked"

Step	Instructions
1	Connect to the command line on the Security Gateway / each Cluster Member.
2	Log in to the Expert mode.
3	Examine the current status: `vpn iked status` Possible outputs: ■ `vpn: 'iked' is enabled` Means the IKE daemon `iked` is enabled (new mode available in R81.10 and higher). This is the default. There is nothing else to do. Stop this procedure. ■ `vpn: 'iked' is disabled` Means the IKE daemon `iked` is disabled (legacy mode as works in R81 and lower). Proceed to the next step.
4	Enable the IKE daemon: `vpn iked enable` **Important:** ■ This command makes the required changes in the `$FWDIR/boot/modules/fwkern.conf` file. ■ This command fetches the local policy (this may disconnect your SSH session). ■ This change survives reboot.

Procedure to disable the IKE daemon "iked"

Step	Instructions
1	Connect to the command line on the Security Gateway / each Cluster Member.
2	Log in to the Expert mode.
3	Examine the current status: `vpn iked status` Possible outputs: ■ `vpn: 'iked' is enabled` Means the IKE daemon `iked` is enabled (new mode in R81.10 and higher). This is the default. Proceed to the next step. ■ `vpn: 'iked' is disabled` Means the IKE daemon `iked` is disabled (legacy mode as works in R81 and lower). There is nothing else to do. Stop this procedure.
4	Disable the IKE daemon: `vpn iked disable` **Important** ■ This command makes the required changes in the `$FWDIR/boot/modules/fwkern.conf` file. ■ This command fetches the local policy (this may disconnect your SSH session) ■ This change survives reboot.

Enabling and Disabling the CCC Daemon "cccd"

By default, the CCC daemon "`cccd`" is disabled on the Security Gateway.

In such a legacy mode, the VPN daemon `vpnd` handles all VPN connections.

If you enable the CCC daemon "`cccd`", then this dedicated daemon handles the Client Communication Channel protocol.

Procedure to enable the CCC daemon "cccd"

Step	Instructions
1	Connect to the command line on the Security Gateway / each Cluster Member.
2	Log in to the Expert mode.
3	Examine the current status: `vpn cccd status` Possible outputs: ■ `vpn: 'cccd' is enabled` Means the CCC daemon `cccd` is enabled (new mode available in R81.10 and higher). There is nothing else to do. Stop this procedure. ■ `vpn: 'cccd' is disabled` Means the CCC daemon `cccd` is disabled (legacy mode as works in R81 and lower). This is the default. Proceed to the next step.
4	Enable the CCC daemon: `vpn cccd enable` **Important:** ■ This command makes the required changes in the `$FWDIR/boot/modules/fwkern.conf` file. ■ This command fetches the local policy (this may disconnect your SSH session) ■ This change survives reboot.

Procedure to disable the CCC daemon "cccd"

Step	Instructions
1	Connect to the command line on the Security Gateway / each Cluster Member.
2	Log in to the Expert mode.
3	Examine the current status: `vpn cccd status` Possible outputs: ■ `vpn: 'cccd' is enabled` Means the CCC daemon `cccd` is enabled (new mode available in R81.10 and higher). Proceed to the next step. ■ `vpn: 'cccd' is disabled` Means the CCC daemon `cccd` is disabled (legacy mode as works in R81 and lower). This is the default. There is nothing else to do. Stop this procedure.
4	Disable the CCC daemon: `vpn cccd disable` **Important** ■ This command makes the required changes in the `$FWDIR/boot/modules/fwkern.conf` file. ■ This command installs the local policy(this may disconnect your SSH session). ■ This change survives reboot.

Description

This "`vpn debug`" command instructs the VPN daemon "`vpnd`" to write debug messages to these log files:

File Description	VPND Log File	IKED Log File for Each Instance	CCCD Log File

Main debug output file	`$FWDIR/log/vpnd.elg*`	`$FWDIR/log/iked0.elg`
		`$FWDIR/log/iked1.elg`
		... ...
		`$FWDIR/log/iked64.elg`
			`$FWDIR/log/cccd.elg`

IKEv1 output	`$FWDIR/log/vpnd.ikev1trace`	`$FWDIR/log/iked0.ikev1trace`
		`$FWDIR/log/iked1.ikev1trace`
		... ...
		`$FWDIR/log/iked64.ikev1trace`
			N / A

IKEv2 output	`$FWDIR/log/vpnd.ikev2trace`	`$FWDIR/log/iked0.ikev2trace`
		`$FWDIR/log/iked1.ikev2trace`
		... ...
		`$FWDIR/log/iked64.ikev2trace`
			N / A

Debugging of the VPN daemon "`vpnd`" is based on Debug Topics and Debug Levels:

- A Debug Topic is a specific area, on which to perform debugging.

  For example, if the Debug Topic is `LDAP`, all traffic between the VPN daemon and the LDAP server is written to the log file.

  Check Point Support provides the specific Debug Topics when needed.

- Debug Levels range from 1 (least informative) to 5 (most informative - write all debug messages).

For more information, see sk180488.

In addition, see *"ike debug" on page 1759*.

Syntax

```
vpn debug
      on [<Debug_Topic>=<Debug_Level>]
      off
      ikeon [-s <Size_in_MB>]
      ikeoff
      trunc [<Debug_Topic>=<Debug_Level>]
      truncon [<Debug_Topic>=<Debug_Level>]
      truncoff
      timeon [<Seconds>]
      timeoff
      ikefail [-s <Size_in_MB>]
      mon
      moff
      say ["String"]
      tunnel [<Level>]
```

Parameters

Parameter	Description
No Parameters	Shows the built-in usage.
`on`	Turns on high level VPN debug. The debug writes the information in these files: `$FWDIR/log/vpnd.elg*` **Note** - If you disabled the IKE daemon "`iked`" to work in the legacy mode, then the debug also writes the information in these files: ■ `$FWDIR/log/iked<Index>.ikev1trace` ■ `$FWDIR/log/iked<Index>.ikev2trace`
<Debug_ Topic>=< Debug_Level>	Specifies the Debug Topic and the Debug Level. *Check Point Support* provides these. **Best Practice** - Run this command to start the VPN debug: `vpn debug trunc ALL=5`

Parameter	Description

`off`	Turns off the VPN debug (in legacy mode, also turns off the IKE debug).
	Best Practice - Run one of these commands to stop the VPN daemon debug:
	`vpn debug off`
	`vpn debug truncoff`

`ikeon [-s <Size_in_MB>]`	**Note** - Applies only if you disabled the IKE daemon "`iked`" to work in the legacy mode. Turns on the IKE trace. The debug writes the information in these files: ■ `$FWDIR/log/iked<Index>.ikev1trace` ■ `$FWDIR/log/iked<Index>.ikev2trace` You can specify the size of these files, when to perform the log rotation (close the current active file, rename it, open a new active file).
`ikeoff`	**Note** - Applies only if you disabled the IKE daemon "`iked`" to work in the legacy mode. Turns off the IKE trace. Run this command to stop the IKE trace: `vpn debug ikeoff`

`trunc`
or
`truncon`
	This command:
	1. Rotates the `$FWDIR/log/vpnd.elg` file
	2. If you disabled the IKE daemon "`iked`" to work in the legacy mode:
	a. Truncates the `$FWDIR/log/iked<Index>.ikev1trace` file
	b. Truncates the `$FWDIR/log/iked<Index>.ikev2trace` file
	3. Starts the VPN daemon "`vpnd`" debug
	4. If you disabled the IKE daemon "`iked`" to work in the legacy mode:
	a. Starts the IKE debug
	Best Practice - Run this command to start the VPN debug:
	`vpn debug trunc ALL=5`

Parameter	Description

`truncoff`	Stops the VPN daemon debug.
	Run one of these commands to stop the VPN debug:
	`vpn debug truncoff`
	`vpn debug off`

`timeon [<Seconds>]`	Enables the timestamp in the log files. Prints one timestamp after the specified number of seconds. By default, prints the timestamp every 10 seconds.
`timeoff`	Disables the timestamp in the log files every number of seconds.
`ikefail [-s <Size_in_MB>]`	**Note** - Applies only if you disabled the IKE daemon "`iked`" to work in the legacy mode. Logs failed IKE negotiations. You can specify the size of these files when to perform the log rotation (close the current active file, rename it, open a new active file): ▪ `$FWDIR/log/iked<Index>.ikev1trace` ▪ `$FWDIR/log/iked<Index>.ikev2trace`
`mon`	**Note** - Applies only if you disabled the IKE daemon "`iked`" to work in the legacy mode. Enables the IKE Monitor. Writes the IKE packets in this file: `$FWDIR/log/ikemonitor.snoop` **Warning** - The output file may contain user X-Auth passwords. Make sure the file is protected.
`moff`	**Note** - Applies only if you disabled the IKE daemon "`iked`" to work in the legacy mode. Disables the IKE Monitor.

`say "String"`	Writes the specified text string in this file:
	`$FWDIR/log/vpnd.elg`
	For example, run:
	`vpn debug say "BEGIN TEST"`
	Notes:
	▪ Run this command after you start the VPN debug (with one of these commands: "`vpn debug on`", "`vpn debug trunc`", or "`vpn debug truncon`").
	▪ The length of the string is limited to 255 characters.

Parameter	Description

`tunnel [<Debug_ Level>]`	This command:
	1. Rotates the `$FWDIR/log/vpnd.elg` file
	2. Truncates the `$FWDIR/log/iked<Index>.ikev1trace` file
	3. Truncates the `$FWDIR/log/iked<Index>.ikev2trace` file
	4. Starts the VPN daemon debug with these two Debug Topics:
	`tunnel`
	`ikev2`
	If the *<Debug_Level>* is 2,3,4 or 5, then also enables this Debug Topic:
	`CRLCache`
	5. Starts the IKE debug (if you disabled the IKE daemon "`iked`" to work in the legacy mode)

Return Values

- 0 (zero) for success
- any other value for failure (typically, -1 or 1)

vpn dll

Description

Works with VPN DNS Lookup Layer:

- Save the DNS Lookup Layer information to the specified file.
- Resolve the specified hostname.

Syntax

```
vpn dll
      dump <File>
      resolve <HostName>
```

Parameters

Parameter	Description
`dump <File>`	Saves the DNS Lookup Layer information (DNS Names and IP Addresses) to the specified file.
`resolve <HostName>`	Resolves the specified hostname. The command saves the last specified hostname in this file: `$FWDIR/tmp/vpnd_cmd.tmp`

vpn drv

Description

Controls the VPN kernel module.

Syntax

```
vpn drv {off | on | stat}
```

Parameters

Parameter	Description
`off`	Stops the VPN kernel module
`on`	Starts the VPN kernel module
`stat`	Shows the current status of the VPN kernel module

Example

```
[Expert@MyGW:0]# vpn drv stat
VPN-1 module active
[Expert@MyGW:0]#
```

vpn dump_psk

Description

Shows hash (SHA256) of peers' pre-shared-keys.

Syntax

```
vpn dump_psk
```

vpn ipafile_check

Description

Verifies a candidate for the `$FWDIR/conf/ipassignment.conf` file.

Syntax

```
vpn ipafile_check <File> [{err | warn | detail}] [verify_group_
names]
```

Parameters

Parameter	Description
<File>	Specifies the full path and name of the candidate file.
`{err | warn | detail}`	Specifies the how much information to show about the candidate file: ■ `err` - Only errors ■ `warn` - Only warnings ■ `detail` - All details
`verify_group_names`	Examines the group names.

vpn ipafile_users_capacity

Description

- Shows the current capacity in the `$FWDIR/conf/ipassignment.conf` file.
- Configures the new capacity in the `$FWDIR/conf/ipassignment.conf` file.

Syntax

```
vpn ipafile_users_capacity get
vpn ipafile_users_capacity set <128-32768>
```

Parameters

Parameter	Description
`get`	Shows the current capacity.
`set <128-32768>`	Configures the new capacity to the specified number of users. **Notes:** ■ The default is 1024 entries. ■ This command configures the amount of memory reserved to store usernames.

Example

```
[Expert@MyGW:0]# vpn ipafile_users_capacity get
The gateway can currently read 1024 users from the ipassignment.conf file
[Expert@MyGW:0]#
```

vpn macutil

Description

Shows a generated MAC address for each user name when you use Remote Access VPN with Office Mode.

This command is applicable only when allocating IP addresses through DHCP.

Remote Access VPN users in Office Mode receive an IP address, which is mapped to a hardware or MAC address.

Syntax

```
vpn macutil <username>
```

Example

```
# vpn macutil John
20-0C-EB-26-80-7D, "John"
```

vpn mep_refresh

Description

Initiates MEP re-decision.

Used in "backup stickiness" configuration to initiate MEP re-decision (fail back to primary Security Gateway, if possible).

Syntax

```
vpn mep_refresh
```

vpn neo_proto

Description

Controls the NEO client protocol.

Important - This command is for Check Point use only.

Syntax

```
vpn neo_proto {off | on}
```

Parameters

Parameter	Description
`off`	Disables the NEO client protocol.
`on`	Enables the NEO client protocol.

vpn nssm_toplogy

Description

Generates and uploads a topology in NSSM format to an NSSM server.

Syntax

```
vpn nssm_topology -url <"url"> -dn <"dn"> -name <"name"> -pass
<"password"> [-action {bypass | drop}] [-print_xml]
```

Parameters

Parameter	Description
`-url <"url">`	URL of the NSSM server.
`-dn <"dn">`	Distinguished Name of the NSSM server (needed to establish an SSL connection).
`-name <"name">`	Valid login name for the NSSM server.
`-pass <"password">`	Valid password for the NSSM server.
`-action {bypass | drop}`	Specifies the action that the Symbian client should take, if the packet is not destined for an IP address in the VPN domain. Bypass is the default.
`-print_xml`	Writes the topology to a file in XML format.

vpn overlap_encdom

Description

Shows all overlapping VPN domains.

Some IP addresses might belong to two or more VPN domains.

The command alerts for overlapping encryption domains if one or both of the following conditions exist:

- The same VPN domain is defined for both Security Gateways.
- If the Security Gateway has multiple interfaces, and one or more of the interfaces has the same IP address and netmask.

Syntax

```
vpn overlap_encdom [communities | traditional]
```

Parameters

Parameter	Description
`communities`	Shows all pairs of objects with overlapping VPN domains, only if the objects (that represent VPN sites) are included in the same VPN community. This parameter is also used, if the same destination IP can be reached through more than one VPN community.
`traditional`	Default parameter. Shows all pairs of objects with overlapping VPN domains.

Example

```
# vpn overlap_encdom communities
The objects Paris and London have overlapping encryption domains.
The overlapping domain is:
10.8.8.1 - 10.8.8.1
10.10.8.0 - 10.10.9.255
- This overlapping encryption domain generates a multiple entry points configuration in
MyIntranet and RemoteAccess communities.
- Same destination address can be reached in more than one community (Meshed, Star). This
configuration is not supported.

The objects Paris and Chicago have overlapping encryption domains. The overlapping domain is:
10.8.8.1 - 10.8.8.1
- Same destination address can be reached in more than one community (MyIntranet, NewStar). This
configuration is not supported.

The objects Washington and Tokyo have overlapping encryption domains.
The overlapping domain is:
10.12.10.68 - 10.12.10.68
10.12.12.0 - 10.12.12.127
10.12.14.0 - 10.12.14.255
- This overlapping encryption domain generates a multiple entry points configuration in Meshed,
Star and NewStar communities.
```

vpn rim_cleanup

Description

Cleans RIM routes.

Syntax

```
vpn rim_cleanup
```

vpn rll

Description

Controls the VPN Route Lookup Layer:

- Saves the Route Lookup Layer information to the specified file.
- Synchronizes the routing table.

Syntax

```
vpn rll
      dump <File>
      sync
```

Parameters

Parameter	Description
`dump <File>`	Saves the Route Lookup Layer information to the specified file: ■ ISP Redundancy Default Routes (Next Hop, Interface, Metric) ■ Route Shadow (Interface and Metric, IP/Mask, Next Hop) ■ Monitored IP Addresses (Data, IP/Mask)
`sync`	Synchronizes the routing table.

vpn set_slim_server

Description

This command is deprecated.

Delete the `$FWDIR/conf/slim.conf` file and use the Management Server to configure SSL Network Extender.

As long as the `$FWDIR/conf/slim.conf` file exists, it **overrides** the settings you configure on the Management Server.

vpn set_snx_encdom_groups

Description

Controls the encryption domain per usergroup feature for SSL Network Extender.

Syntax

```
vpn set_snx_encdom_groups
      off
      on
```

Parameters

Parameter	Description
`off`	Disables the encryption domain per usergroup feature.
`on`	Enables the encryption domain per usergroup feature.

vpn set_trac

Description

Controls the TRAC server.

Syntax

```
vpn set_trac
      disable
      enable
```

Parameters

Parameter	Description
`disable`	Disables the TRAC server.
`enable`	Enables the TRAC server.

Example

```
[Expert@MyGW:0]# vpn set_trac enable
 Trac client enabled, Install Policy for this change to take effect
[Expert@MyGW:0]#

[Expert@MyGW:0]# vpn set_trac disable
 Trac client disabled, Install Policy for this change to take effect
[Expert@MyGW:0]#
```

vpn shell

Description

VPN Command Line Interface.

Syntax for IPv4

```
vpn shell
```

Syntax for IPv6

```
vpn6 shell
```

Menu Options

```
[Expert@MyGW:0]# vpn shell
 ?              - This help
 ..             - Go up one level
 quit           - Quit
[interface    ] - Manipulate tunnel interfaces
[show         ] - Show internal data
[tunnels      ] - Manipulate tunnel data
[license      ] - Display SCM licenses
VPN shell:[/] >
```

Menu Sub-Options

```
interface
      add
      modify
      delete
      show
show
      interface
      tunnels
            IKE
                  all
                  peer <Internal Peer IP>
            IPsec
                  all
                  peer <Internal Peer IP>
tunnels
      show
            IKE
                  all
                  peer <Internal Peer IP>
            IPsec
                  all
                  peer <Internal Peer IP>
      delete
            IKE
                  peer <Security Gateway>
                  user <Username>
                  all
            IPsec
                  peer <Security Gateway>
                  user <Username>
                  all
            all
                  IKE
                  IPsec
license
      scm
            status
            list
```

Description of Options and Sub-Options

Option	Description
`?`	Shows the available advanced commands in the current menu level.
`..`	Goes up one level in the menu.
`quit`	Quits the VPN shell (available only in the main level).
`interface`	These commands are deprecated on Gaia OS. Use the applicable options in Gaia Portal or the applicable commands in Gaia Clish. See the *R81.20 Gaia Administration Guide*.
`show`	Shows internal data. The available options are: ■ Show and configure tunnel interfaces: `show > interface` These commands are deprecated on Gaia OS. Use the applicable options in Gaia Portal or the applicable commands in Gaia Clish. See the *R81.20 Gaia Administration Guide*.

Option	Description

	■ Show Security Associations (SAs):
	`show > tunnels`
	The available sub-options are:
	• Show all IKE SAs
	`show > tunnels > IKE > all`
	Note - This sub-option is the same as:
	◦ In the main *"vpn tu" on page 1816* menu, the option **(3) List all IKE SAs for a given peer (GW)**.
	◦ The "`vpn tu [-w] list ike`" command (see *"vpn tu list" on page 1823*).
	• Show all IKE SAs for a specified VPN peer:
	`show > tunnels > IKE > peer <Internal Peer IP>`
	Note - This sub-option is the same as:
	◦ In the main *"vpn tu" on page 1816* menu, the option **(1) List all IKE SAs**.
	◦ The "`vpn tu [-w] list peer_ike <IP Address>`" command (see *"vpn tu list" on page 1823*).
	• Show all IPsec SAs
	`show > tunnels > IPsec > all`
	Note - This sub-option is the same as:
	◦ In the main *"vpn tu" on page 1816* menu, the option **(2) List all IPsec SAs**.
	◦ The "`vpn tu [-w] list ipsec`" command (see *"vpn tu list" on page 1823*).
	• Show all IPsec SAs for a specified VPN peer:
	`show > tunnels > IPsec > peer <Internal Peer IP>`
	Note - This sub-option is the same as:
	◦ In the main *"vpn tu" on page 1816* menu, the option **(4) List all IPsec SAs for a given peer (GW)**.
	◦ The "`vpn tu [-w] list peer_ipsec <IP Address>`" command (see *"vpn tu list" on page 1823*).

Option	Description

`tunnels`	Shows and deletes Security Associations (SAs).
	The available options are:
	■ Show Security Associations (SAs):
	`tunnels > show`
	The available sub-options are:
	• Show all IKE SAs:
	`tunnels > show > IKE > all`
	Note - This sub-option is the same as:
	◦ In the main *"vpn tu" on page 1816* menu, the option **(1) List all IKE SAs**.
	◦ The "`vpn tu [-w] list ike`" command (see *"vpn tu list" on page 1823*).
	• Show all IKE SAs for a specified VPN peer:
	`tunnels > show > IKE > peer <Internal Peer IP>`
	Note - This sub-option is the same as:
	◦ In the main *"vpn tu" on page 1816* menu, the option **(3) List all IKE SAs for a given peer (GW)**.
	◦ The "`vpn tu [-w] list peer_ike <IP Address>`" command (see *"vpn tu list" on page 1823*).
	• Show all IPsec SAs:
	`tunnels > show > IPsec > all`
	Note - This sub-option is the same as:
	◦ In the main *"vpn tu" on page 1816* menu, the option **(2) List all IPsec SAs**.
	◦ The "`vpn tu [-w] list ipsec`" command (see *"vpn tu list" on page 1823*).
	• Show all IPsec SAs for a specified VPN peer:
	`tunnels > show > IPsec > peer <Internal Peer IP>`
	Note - This sub-option is the same as:
	◦ In the main *"vpn tu" on page 1816* menu, the option **(4) List all IPsec SAs for a given peer (GW)**.
	◦ The "`vpn tu [-w] list peer_ipsec <IP Address>`" command (see *"vpn tu list" on page 1823*).

Option	Description

	■ Delete Security Associations (SAs):
	`tunnels > delete`
	The available sub-options are:
	• Delete all IKE for a specified VPN peer:
	`tunnels > delete > IKE > peer <Internal Peer IP>`
	• Delete all IKE for a specified user:
	`tunnels > delete > IKE > user <Username>`
	• Delete all IKE SAs for all VPN peers and users:
	`tunnels > delete > IKE > all`
	`tunnels > delete > all > IKE`
	• Delete all IPsec SAs for a specified VPN peer:
	`tunnels > delete > IPsec > peer <Internal Peer IP>`
	Note - This sub-option is the same as:
	◦ In the main *"vpn tu" on page 1816* menu, the option **(5) Delete all IPsec SAs for a given peer (GW)**.
	◦ The "`vpn tu [-w] del ipsec <IP Address>`" command (see *"vpn tu del" on page 1820*).
	• Delete all IPsec SAs for a specified user:
	`tunnels > delete > IPsec > user <Username>`
	Note - This sub-option is the same as:
	◦ In the main *"vpn tu" on page 1816* menu, the option **(6) Delete all IPsec SAs for a given User (Client)**.
	◦ The "`vpn tu [-w] del ipsec <IP Address> <Username>`" command (see *"vpn tu del" on page 1820*).
	• Delete all IPsec SAs for all VPN peers and users:
	`tunnels > delete > IPsec > all`
	`tunnels > delete > all > IPsec`
	Note - This sub-option is the same as:
	◦ In the main *"vpn tu" on page 1816* menu, the option **(9) Delete all IPsec SAs for ALL peers and users**.
	◦ The "`vpn tu [-w] del ipsec all`" command (see *"vpn tu del" on page 1820*).

Option	Description

`license`	Shows the SecureClient Mobile (SCM) licenses.
	The available sub-options are:
	■ Show the current status of SCM licenses:
	`license > scm > status`
	■ Show the list of SCM licensed devices:
	`license > scm > list`

vpn show_tcpt

Description

Shows users connected in Visitor Mode.

Syntax

```
vpn show_tcpt
```

vpn tu

Description

Launches the `TunnelUtil` tool, which is used to control VPN tunnels.

General Syntax

`vpn tu`
`vpn tunnelutil`

Menu Options

```
[Expert@MyGW:0]# vpn tu

**********     Select Option     **********

(1)               List all IKE SAs
(2)             * List all IPsec SAs
(3)               List all IKE SAs for a given peer (GW)
(4)             * List all IPsec SAs for a given peer (GW)
(5)               Delete all IPsec SAs for a given peer (GW)
(6)               Delete all IPsec SAs for a given User (Client)
(7)               Delete all IPsec+IKE SAs for a given peer (GW)
(8)               Delete all IPsec+IKE SAs for a given User
(Client)
(9)               Delete all IPsec SAs for ALL peers
(0)               Delete all IPsec+IKE SAs for ALL peers

* To list data for a specific CoreXL instance, append "-i
<instance number>" to your selection.

(Q)               Quit

*****************************************
```

Note - When you view Security Associations for a specific VPN peer, you must specify the IP address in dotted decimal notation.

Advanced Syntax

```
vpn tu [-w]
      help
      conn <options>
      del <options>
      list <options>
      mstats
      tlist <options>
```

Parameters

Parameter	Description
`help`	Shows the available advanced commands.
`-w`	Shows various warnings on the screen.
`conn <options>`	Shows VPN information for the specified traffic connections. See *"vpn tu conn" on page 1818*.
`del <options>`	Deletes IPsec and IKE SAs. See *"vpn tu del" on page 1820*.
`list <options>`	Shows IPsec and IKE SAs. See *"vpn tu list" on page 1823*.
`mstats`	Shows distribution of VPN tunnels (SPIs) between CoreXL Firewall instances. See *"vpn tu mstats" on page 1825*.
`tlist <options>`	Shows information about VPN tunnels. See *"vpn tu tlist" on page 1826*.

vpn tu conn

Description

Shows VPN information for the specified traffic connections.

Syntax for IPv4

```
vpn tu [-w] conn {<Source IPv4 Address> | -} {<Source Port> | -}
{<Destination IPv4 Address> | -} {<Destination Port> | -} [<IPv4
Protocol> | -}]
```

Syntax for IPv6

```
vpn6 tu [-w] conn {<Source IPv6 Address> | -} {<Source Port> | -}
{<Destination IPv6 Address> | -} {<Destination Port> | -} [<IPv6
Protocol> | -}]
```

Parameters

Parameter	Description
`-w`	Shows various warnings on the screen.
<Source IPv4 Address> *<Source IPv6 Address>*	Specifies the Source Address. You must enter one of these: ■ A valid IP address. ■ The minus character "-" to act a wildcard.
<Source Port>	Specifies the Source Port. You must enter one of these: ■ A valid port number. ■ The minus character "-" to act a wildcard.
<Destination IPv4 Address> *<Destination IPv6 Address>*	Specifies the Destination Address. You must enter one of these: ■ A valid IP address. ■ The minus character "-" to act a wildcard.

Parameter	Description
<Destination Port>	Specifies the Destination Port. You must enter one of these: ■ A valid port number. ■ The minus character "-" to act a wildcard.
<IPv4 Protocol> *<IPv6 Protocol>*	Optional. Specifies the Protocol number. You must enter one of these: ■ A valid protocol number. ■ The minus character "-" to act a wildcard.

vpn tu del

Description

Deletes IPsec Security Associations (SAs) and IKE Security Associations (SAs).

Syntax for IPv4

```
vpn tu [-w] del
      all
      ipsec
            all
            <IPv4 Address>
            <IPv4 Address> <Username>
      <IPv4 Address>
      <IPv4 Address> <Username>
```

Syntax for IPv6

```
vpn tu [-w] del
      all
      ipsec
            all
            <IPv6 Address>
      <IPv6 Address>
      <IPv6 Address> <Username>
```

Parameters

Parameter	Description
`-w`	Shows various warnings on the screen.
`all`	Deletes all IPsec SAs and IKE SAs for all VPN peers and users. **Note** - This command is the same as: ■ In the main *"vpn tu" on page 1816* menu, the option **(0) Delete all IPsec+IKE SAs for ALL peers and users**. ■ In the *"vpn shell" on page 1808* menu, the option **tunnels > delete > all > IKE** and the option **tunnels > delete > all > IPsec**..

Parameter	Description

`ipsec <options>`	Deletes the specified IPsec SAs.
	The available <*options*> are:
	■ Delete all IPsec SAs for all peers and users:
	`vpn tu [-w] del ipsec all`
	Note - This command is the same as:
	• In the main *"vpn tu" on page 1816* menu, the option **(9) Delete all IPsec SAs for ALL peers and users**.
	• In the *"vpn shell" on page 1808* menu, the option **tunnels > delete > all > IPsec**.
	■ Delete all IPsec SAs for the specified VPN peer:
	`vpn tu [-w] del ipsec <IP Address>`
	Note - This command is the same as:
	• In the main *"vpn tu" on page 1816* menu, the option **(5) Delete all IPsec SAs for a given peer (GW)**.
	• In the *"vpn shell" on page 1808* menu, the option **tunnels > delete > IPsec > peer <*Internal Peer IP*>**.
	■ Delete all IPsec SAs for the specified VPN peer and the specified user:
	`vpn tu [-w] del ipsec <IPv4 Address> <Username>`
	Notes:
	• This command is the same as:
	◦ In the main *"vpn tu" on page 1816* menu, the option **(6) Delete all IPsec SAs for a given User (Client)**.
	◦ In the *"vpn shell" on page 1808* menu, the option **tunnels > delete > IPsec > user <*Username*>**.
	• This command does **not** support IPv6 addresses.

`<IP Address>`	Deletes all IPsec SAs and IKE SAs for the specified VPN peer. **Note** - This command is the same as the option **(7) Delete all IPsec+IKE SAs for a given peer (GW)** in the main *"vpn tu" on page 1816* menu.

Parameter	Description
<IP Address> *<Username>*	Deletes all IPsec SAs and IKE SAs for the specified VPN peer and the specified user. **Note** - This command is the same as the option **(8) Delete all IPsec+IKE SAs for a given User (Client)** in the main *"vpn tu" on page 1816* menu.

vpn tu list

Description

Shows IPsec SAs and IKE SAs.

Syntax for IPv4 and IPv6

```
vpn tu [-w] list
       ike
       ipsec
       peer_ike <IP Address>
       peer_ipsec <IP Address>
       tunnels
```

Parameters

Parameter	Description
`-w`	Shows various warnings on the screen.
`ike`	Shows all IKE SAs. **Note** - This command is the same as: ■ In the main *"vpn tu" on page 1816* menu, the option **(1) List all IKE SAs**. ■ In the *"vpn shell" on page 1808* menu, the option **show > tunnels > IKE > all** or the option **tunnels > show > IKE > all**.
`ipsec`	Shows all IPsec SAs. **Note** - This command is the same as: ■ In the main *"vpn tu" on page 1816* menu, the option **(2) List all IPsec SAs**. ■ In the *"vpn shell" on page 1808* menu, the option **show > tunnels > IPsec > all** or the option **tunnels > show > IPsec > all**.

Parameter	Description
`peer_ike <IP Address>`	Shows all IKE SAs for the specified VPN peer. **Note** - This command is the same as: ■ In the main *"vpn tu" on page 1816* menu, the option **(3) List all IKE SAs for a given peer (GW)**. ■ In the *"vpn shell" on page 1808* menu, the option **show > tunnels > IKE > peer <*Internal Peer IP*>** or the option **tunnels > show > IKE > peer <*Internal Peer IP*>**.
`peer_ipsec <IP Address>`	Shows all IPsec SAs for the specified VPN peer. **Note** - This command is the same as: ■ In the main *"vpn tu" on page 1816* menu, the option **(4) List all IPsec SAs for a given peer (GW)**. ■ In the *"vpn shell" on page 1808* menu, the option **show > tunnels > IPsec > peer <*Internal Peer IP*>** or the option **tunnels > show > IPsec > peer <*Internal Peer IP*>**.
`tunnels`	Shows information about VPN tunnels. In addition, see the *"vpn tu tlist" on page 1826* command.

vpn tu mstats

Description

Shows the distribution of VPN traffic between CoreXL Firewall instances.

For more information, see sk118097 - MultiCore Support for IPSec VPN in R80.10 and above.

Syntax for IPv4

```
vpn tu [-w] mstats
```

Syntax for IPv6

```
vpn6 tu [-w] mstats
```

Parameters

Item	Description
`-w`	Shows various warnings on the screen.

Example for IPv4

```
[Expert@MyGW:0]# vpn tu mstats

   Instance# # of inSPIs # of outSPIs
           0 182 170
           1 184 176
           2 191 174
           3 215 197
           4 237 227
           5 191 176
           6 180 170
           7 190 166
           8 171 160
           9 199 187
   ----------------------------------------
   Summary: 1940 1803

[Expert@MyGW:0]#
```

Example for IPv6

```
[Expert@MyGW:0]# vpn6 tu mstats

   Instance# # of inSPIs # of outSPIs
           0 238 228
           1 224 214
   ----------------------------------------
   Summary: 462 442

[Expert@MyGW:0]#
```

vpn tu tlist

Description

Shows information about VPN tunnels.

Syntax for IPv4

```
vpn tu [-w] tlist
      {-h | -help}
      [clear]
      [start]
      [state]
      [stop]
      [<Sort Options>]
```

Syntax for IPv6

```
vpn6 tu [-w] tlist
      {-h | -help}
      [clear]
      [start]
      [state]
      [stop]
      [<Sort Options>]
      [<Output Options>]
```

Parameters

Parameter	Description
`-w`	Shows various warnings on the screen.
`-h | -help`	Shows the built-in usage.
`clear`	Clears the Tunnel List volume statistics.
`start`	Turns on the Tunnel List volume statistics.
`state`	Shows the current Tunnel List volume statistics state.
`stop`	Turns off the Tunnel List volume statistics.

Parameter	Description

<Sort Options>	The available sort options are:
	■ `-b`
	Sorts by total (encrypted + decrypted) bytes.
	■ `-d`
	Sorts by inbound (decrypted) bytes.
	■ `-e`
	Sorts by outbound (encrypted) bytes.
	■ `-i`
	Combines list rows for each CoreXL Firewall instance with accumulated traffic.
	The default order is descending by total bytes.
	■ `-m`
	Sorts by MSPI values.
	■ `-n`
	Sorts by VPN peer name.
	■ `-p` *<IP Address>*
	Shows tunnels only for a VPN peer with the specified IP address.
	■ `-r`
	Sorts in reverse order.
	■ `-s`
	Sorts by SPI.
	■ `-t`
	Combines list rows for each VPN peer with accumulated traffic.
	The default order is descending by total bytes.
	■ `-v`
	Verbose mode, shows a header message for each option.
	
	If you specify more than one sort option, you can:
	■ Separate the options with spaces:
	`... -<option1> -<option2> -<option3>`
	For example: `-v -t -b -r`
	■ Write the options together:
	`... -<option1><option2><option3>`
	For example: `-vtbr`

Parameter	Description
<Output Options>	The available output options are (you can specify more than one output option): ■ `-a {on | off}` Shows only accelerated tunnels ("`-a on`") or only non-accelerated tunnels ("`-a off`"). ■ `-c {ra_nat_t | ra_vm | ra_ssl | ra_l2tp | ra_strongSwan | ra_android | ra_ios}` Shows only the tunnels with the corresponding type. ■ `-w` *<Width of Column 1>*,*<Width of Column 2>*,*<Width of Column 3>* Configures the width of the table columns. You must always enter 3 values. Example: `-w 46,33,20` ■ `-y` Shows only the peer summary, without the list of VPN tunnels. ■ `-z` Shows a summary for traffic handled by the IKE daemon "`iked`" instances.

Example for IPv4

```
+-----------------------------------------+-----------------------
+---------------------+
| Peer: 172.16.10.1 (c05ea6c62d82122c)    | MSA: ffffc90047aa08d8
| i: 3  ref:     1    |
| Client public IP: 10.20.4.12           |
|                     |
| Authenticated at:    Aug 1 17:22:01    |
|                     |
| Methods: SSL Tunnel 3DES MDS           |
|                     |
| My TS:   0.0.0.0/0                     |
|                     |
| Peer TS: 172.16.10.1                   |
|                     |
| User: user_1                           |
|                     |
| MSPI:   1c00001 (i:  3, p:  -)         |
|                     |
| Tunnel created:        Aug 1 17:22     |  SSL
|                     |
| Tunnel expiration:     Aug 1 17:31:58  |  Connected
|                     |
+-----------------------------------------+-----------------------
+---------------------+
| Peer: 10.20.3.198 - SGW4               |  MSA: ffffc90047aa0ae
|i: 9   ref: --57/60  |
| Methods: ESP Tunnel AES-128 SHA1       |
|                     |
| My TS: 10.20.5.4/31                    |
|                     |
| Peer TS:                               |
|                     |
| MSPI:                                  |  No outbound SPI
|                     |
| Tunnel created:                        |  IPsec
|                     |
| Tunnel expiration:                     |  Disconnected
|                     |
+-----------------------------------------+-----------------------
+---------------------

(1) Site-to-Site tunnels are up:
IPSEC           1
NAT-T           0

(1) Number of Active Clients:
NAT-T           0
```

```
Visitor Mode    0
SSL             1
L2TP            0
```

Explanations About Output

The output of the "`vpn tu tlist`" command is a table with counters below it.

Each row of the table shows information for one VPN peer.

These fields can appear in the **left column** of the table:

Field in Left Column	Explanation
`Peer: [`**`IP ADDRESS`**`]`	IP address of the remote peer that communicates with the VPN Gateway through the VPN tunnel.
`Client public IP`	In a Remote Access VPN tunnel, shows the public IP address of the Remote Access client.
`Authenticated at`	Date and time when the VPN Gateway finished establishing the tunnel with a Remote Access VPN client.
`Methods`	Encryption methods configured for the VPN tunnel. Examples: ■ tunnel type - SSL, ESP ■ encryption type - 3DES, AES-128 ■ data integrity algorithm - MD5, SHA1
`My TS`	Traffic Selector - Subnets, sections of subnets, or a single IP address behind the VPN Gateway that can be destinations for traffic that passes through the VPN Tunnel.
`Peer TS`	Peer Traffic Selector: ■ In a Site to Site VPN tunnel, shows subnets, sections of subnets, or a single IP address behind the peer gateway that can be destinations for traffic that passes through the VPN tunnel. ■ In a Remote Access VPN tunnel, shows the IP address of a computer connected to Remote Access VPN.
`User`	In a Remote Access VPN tunnel, shows the username of the remote access user.

<table>
<tr><th>Field in Left Column</th><th>Explanation</th></tr>
<tr><td>MSPI</td><td>
<table>
<tr><th>Indicator</th><th>Value</th><th>Explanation</th></tr>
<tr><td>Hash</td><td>[STRING]</td><td>Unique indicator for the VPN tunnel to a Security Gateway.
If the VPN peer is a Cluster, each Cluster Member has its own hash.</td></tr>
<tr><td>i</td><td>[INTEGER]</td><td>The number of the firewall instance on which the VPN tunnel is opened.</td></tr>
<tr><td>p</td><td>-</td><td>The tunnel is not accelerated.</td></tr>
<tr><td></td><td>[INTEGER]</td><td>The tunnel is accelerated.
The number indicates the SecureXL instance that handles the tunnel.</td></tr>
<tr><td>d</td><td>[INTEGER]</td><td>The number of the IKE daemon "iked" instance that handles traffic in the VPN tunnel.</td></tr>
</table>
</td></tr>
<tr><td>Tunnel created</td><td>If the VPN tunnel is connected, shows the date and time when the VPN tunnel was created.
If the VPN tunnel is disconnected, shows no value.</td></tr>
<tr><td>Tunnel expiration</td><td>If the VPN tunnel is connected, shows the date and time when the VPN tunnel will expire.
If the VPN tunnel is disconnected, shows no value.</td></tr>
</table>

These fields can appear in the **middle column** of the table:

Field in Middle Column	Explanation
`MSA` [**HASH ID**]	The unique hash ID of the Security Association.
`IPsec`	The VPN tunnel is of type IPsec.
`SSL`	the VPN tunnel is of type SSL.
`No outbound SPI`	There is no Security Parameter Index (SPI) for outbound traffic.
`Connected`	the VPN Gateway has encryption keys for the VPN tunnel.
`Disconnected`	the VPN Gateway does **not** have encryption keys for the VPN tunnel.
`Eclipsed Narrow`	When the initiator of the negotiation requests Traffic Selectors (TS) that are wider than the one the responder is willing to accept, the responder replies with a narrower range. The final TS is set to the narrowed range. ■ If there is narrowing and the local Security Gateway is the initiator, you see the text: `* * * Eclipsed * * *` ■ If narrowing occurred and the local Security Gateway is the responder, you see the text: `* * * Narrow * * *`

These fields can appear in the **right column** of the table:

Field in Right Column	Value	Explanation
`i`	**[INTEGER]**	The number of the firewall instance on which the VPN tunnel is opened.
`ref`	**[INTEGER]**	The number of connections that the firewall instance handles.
	`--` **[INTEGER]/ [INTEGER**	The tunnel is disconnected and there is a countdown until termination or re-establishment of the tunnel. The integer before the slash is the number of seconds left in the countdown backwards to 0. The integer after the slash is the total length of the countdown. Example: `ref: -- 57/60` means the tunnel is disconnected. There are 57 seconds left in a 60-second countdown until tunnel termination or re-establishment.

These counters appear below "`Site-to-Site tunnels are up:`"

Field	Explanation
`IPsec`	the number of Site to Site VPN tunnels of type IPsec connected to the VPN Gateway
`NAT-T`	the number of Site to Site VPN tunnels of type NAT-Tconnected to the VPN Gateway

These counters appear below "`Number of Active Clients:`"

Field	Explanation
`NAT-T`	the number of Remote Access clients connected to the VPN Gateway in NAT Traversal (NAT-T) mode
`Visitor Mode`	the number of Remote Access clients connected to the VPN Gateway in Visitor Mode
`SSL`	the number of Remote Access clients connected to the VPN Gateway in SSL mode
`L2TP`	the number of Remote Access clients connected to the VPN Gateway in L2TP mode
`strongSwan`	the number of Remote Access clients connected to the VPN Gateway in strongSwan mode

vpn ver

Description

Shows the major version number and build number of the VPN kernel module.

Syntax

```
vpn ver [-k] [-f <filename>]
```

Parameters

Parameter	Description
-k	Shows the version name and build number and the kernel build number.
-f	Saves the information to the specified text file.

Example

```
[Expert@MyGW:0]# vpn ver -k
This is Check Point VPN-1(TM) R81.20 - Build 123
kernel: R81.20 - Build 456
[Expert@MyGW:0]#
```

mcc

Description

The VPN Multi-Certificate CA (MCC) commands let you manage certificates and Certificate Authorities on a Security Management Server or Domain Management Server:

- Shows Certificate Authorities
- Shows certificates
- Adds certificates
- Deletes certificates

Important:

- Before you run this command, you must close all SmartConsole clients, *Database Tool (GuiDBEdit Tool)* clients, and "`dbedit`" clients (see sk13301) to prevent a lock of the management database. The only exceptions are the "`mcc lca`" and "`mcc show`" commands.
- The `mcc` commands require the `cpca` process to be up and running. Run this command:

  ```
  ps auxw | egrep "cpca|COMMAND"
  ```

- On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

  ```
  mdsenv <IP Address or Name of Domain Management Server>
  ```

Syntax

```
mcc
      -h
      add <options>
      add2main <options>
      del <options>
      lca
      main2add <options>
      show <options>
```

Parameters

Parameter	Description
`-h`	Shows the built-in usage.

Parameter	Description
`add <options>`	Adds certificates. See *"mcc add" on page 1840*.
`add2main <options>`	Promotes an additional certificate to be the main certificate. See *"mcc add2main" on page 1841*.
`del <options>`	Deletes certificates. See *"mcc del" on page 1842*.
`lca`	Shows Certificate Authorities. See *"mcc lca" on page 1843*.
`main2add <options>`	Adds main certificate to additional certificates. See *"mcc main2add" on page 1844*.
`show <options>`	Shows certificates. See *"mcc show" on page 1845*.

mcc add

Description

Adds a certificate stored in DER format in a specified file, as an additional certificate to the specified CA. The new certificate receives an index number higher by one than the highest existing certificate index number.

The new certificate receives an index number higher by one than the highest existing certificate index number.

Syntax

```
mcc add <CA Name> <Certificate File>
```

Note
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Important - Before you run this command, you must close all SmartConsole clients, *Database Tool (GuiDBEdit Tool)* clients, and "`dbedit`" clients (see sk13301) to prevent a lock of the management database.

Parameters

Parameter	Description
<CA Name>	Specifies the name of the CA, as defined in the Management Server database.
<Certificate File>	Specifies the path and the name of the certificate file. To show the main certificate of a CA, omit this parameter.

Example - Add the certificate stored in the `/var/log/Mycert.cer` file to the CA called "MyCA"

```
mcc add MyCA /var/log/Mycert.cer
```

mcc add2main

Description

Copies the additional certificate of the specified index number of the specified CA to the main position and overwrites the previous main certificate.

Syntax

```
mcc add2main <CA Name> <Certificate Index Number>
```

Note
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Important - Before you run this command, you must close all SmartConsole clients, *Database Tool (GuiDBEdit Tool)* clients, and "`dbedit`" clients (see sk13301) to prevent a lock of the management database.

Parameters

Parameter	Description
<CA Name>	Specifies the name of the CA, as defined in the Management Server database.
<Certificate Index Number>	Specifies the certificate index number.

Example - Copy certificate #1 of a CA called "MyCA" to the main position

```
mcc add2main MyCA 1
```

mcc del

Description

Removes the additional certificate of the specified index number from the specified CA.

Greater index numbers (of other additional certificates) are reduced by one.

Syntax

```
mcc del <CA Name> <Certificate Index Number>
```

Note
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Important - Before you run this command, you must close all SmartConsole clients, *Database Tool (GuiDBEdit Tool)* clients, and "`dbedit`" clients (see sk13301) to prevent a lock of the management database.

Parameters

Parameter	Description
<CA Name>	Specifies the name of the CA, as defined in the Management Server database.
<Certificate Index Number>	Specifies the certificate index number.

Example - Remove certificate #1 of a CA called "MyCA"

```
mcc del MyCA 1
```

mcc lca

Description

Shows all Certificate Authorities (CAs) defined in the Management Server database, with the number of additional CA certificates for each CA.

Syntax

```
mcc lca
```

Note
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Example

```
[Expert@MGMT:0]# mcc lca
MCC: Here is a list of the CAs, with the number of additional CA certificates
    1. internal_ca (0)
[Expert@MGMT:0]#
```

mcc main2add

Description

Copies the main certificate of the specified CA to an additional position.

The copied certificate receives an index number higher by one than the highest existing certificate index number.

Syntax

```
mcc main2add <CA Name>
```

Note
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Important - Before you run this command, you must close all SmartConsole clients, *Database Tool (GuiDBEdit Tool)* clients, and "`dbedit`" clients (see sk13301) to prevent a lock of the management database.

Parameters

Parameter	Description
<CA Name>	Specifies the name of the CA, as defined in the Management Server database.

Example

The CA called "`MyCA`" has a main certificate and one additional certificate.

If you run this command, then the CA will have two additional certificates, and additional certificate #2 will be identical to the main certificate:

```
mcc main2add MyCA
```

mcc show

Description

Shows details for a specified certificate of a specified CA.

Syntax

```
mcc show <CA Name> [<Certificate Index Number>]
```

Note
On a Multi-Domain Server, you must run this command in the context of the applicable Domain Management Server:

```
mdsenv <IP Address or Name of Domain Management Server>
```

Parameters

Parameter	Description
<CA Name>	Specifies the name of the CA, as defined in the Management Server database.
<Certificate Index Number>	Optional. Specifies the certificate index number. To show the main certificate of a CA, omit this parameter.

Example 1 - Show certificate #1 of a CA called `MyCA`

```
mcc show MyCA 1
```

Example 2 - Show certificate of a CA called "`internal_ca`"

```
[Expert@MGMT:0]# mcc lca
MCC: Here is a list of the CAs, with the number of additional CA certificates
    1. internal_ca (0)
[Expert@MGMT:0]#

[Expert@MGMT:0]# mcc show internal_ca
  PubKey:
  Modulus:
  ae b3 75 36 64 e4 1a 40 fe c2 ad 2f 9b 83 0b 45 f1 00 04 bc
  3f 77 77 76 d1 de 8a cf 9f 32 78 8b d4 b1 b4 be db 75 cc c8
  ... ... ...
  a3 9d 8b 0a de 05 fb 5c 44 2e 29 e3 3e f4 dd 50 01 0f 86 9d
  55 16 a3 4d f8 90 2d 13 c6 c1 28 57 f8 3e 7c 59
  Exponent: 65537 (0x10001)

X509 Certificate Version 3
refCount: 1
Serial Number: 1
Issuer: O=MyServer.checkpoint.com.s6t98x
Subject: O=MyServer.checkpoint.com.s6t98x
Not valid before: Sun Apr 8 13:41:00 2018 Local Time
Not valid after: Fri Jan 1 05:14:07 2038 Local Time
Signature Algorithm: RSA with SHA-256 Public key: RSA (2048 bits)
Extensions:
        Key Usage:
                digitalSignature
                keyCertSign
                cRLSign
        Basic Constraint (Critical):
                is CA

[Expert@MGMT:0]#
```

Mobile Access Commands

For more information about Mobile Access, see the *R81.20 Mobile Access Administration Guide*.

admin_wizard

Description

Runs the administration client wizard to test connectivity to websites, Exchange server services, or LDAP server.

Note - This wizard saves its log messages in these files:

- `$CVPNDIR/log/AdminWizardLog.elg`
- `$CVPNDIR/log/wizard.elg`
- `$CVPNDIR/log/wizardDns`
- `$CVPNDIR/log/wizardEstimation`
- `$CVPNDIR/log/wizardLdap`
- `$CVPNDIR/log/wizardProxy`

Syntax

```
admin_wizard
      cancel
      estimation
      exchange_wizard <Exchange Server Address> <User Name>
<Password> [<Options>]
      ldap <LDAP server>
      wizard <Web Site Address>
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
No Parameters	Shows the built-in help.
`cancel`	Kills the administration client wizard that already runs.
`estimation`	Estimates how many seconds the wizard will run.

Parameter	Description
`exchange_wizard <Exchange Server Address> <User Name> <Password> [<Options>]`	Tests the response from an Exchange server: ■ Finds the address protocol (HTTP or HTTPS) and authentication method (Basic or NTLM) of the Exchange server services. ■ Checks accessibility of Mobile Access ActiveSync and EWS services for users. ■ For Web command, checks access to the URL. ■ For OWA command, returns the URL to the outlook web access. The parameters are: ■ *<Exchange Server Address>* - Specifies the Exchange server by its IP address or hostname. ■ *<User Name>* - Specifies the user name on the Exchange Server. ■ *<Password>* - Specifies the password on the Exchange Server. ■ *<Options>* - Specifies the test options.

Parameter	Description
	The available test options are: ■ `-t {as | ews | owa | all}` - Specifies the services to test on the Exchange server: **Note** - To specify more than one service, separate them with a comma. For example: `as,ews` • `all` - Tests all of the services (default) • `as` - Tests ActiveSync • `ews` -Tests Exchange Web Services • `owa` - Searches for the Outlook Web Application (OWA) address of the Exchange server ■ `-d <DNS Servers>` - Specifies the DNS servers. ■ `-x <Proxy Servers>` - Specifies the Proxy servers. ■ `-c <Username>:<Password>` - Specifies the user name and password for Proxy server authentication. ■ `-n` - Allows only NTLM authentication instead of Basic and NTLM. ■ `-m <Domain Name>` - Specifies the user domain name. ■ `-s <ActiveSync Path>` - Tests a specified ActiveSync service path (Default: `/Microsoft-Server-ActiveSync`). ■ `-e <EWS Path>` - Tests a specified Exchange Web Services service path (Default: `/EWS/Exchange.asmx`). ■ `-f <File Name>` - Writes the test results to the specified file ■ `-r` - Sends a request with the configured Proxy, DNS, HTTP protocol, and authentication method. • If you also specify the "`-n`" option, then the NTLM authentication method is used. • If you do not specify the "`-n`" option, then only the Basic authentication method is used.

Parameter	Description
	■ `-v` - Makes the HTTP requests verbose. The verbose result files are saved in the `$CVPNDIR/log/trace_log/` directory. ■ `-p` - Validates the SSL certificate of the web server.
`ldap <LDAP server>`	Tests connectivity to the specified LDAP server. You can specify the LDAP server by its IP address or hostname.
`wizard <Web Site Address>`	Tests connectivity to the specified URL.

Example 1 - Check URL accessibility of 'www.checkpoint.com'

```
admin_wizard wizard www.checkpoint.com
```

Example 2 - Check accessibility to the LDAP server 192.168.0.55

```
admin_wizard ldap 192.168.0.55
```

Example 3 - Check accessibility for username 'user1' to ActiveSync and EWS on the Exchange server 'exchange.example.com'

```
admin_wizard exchange_wizard exchange.example.com username user1 -
t as,ews
```

cvpnd_admin

Description

Changes the behavior of the Mobile Access **cvpnd** process.

Syntax

```
cvpnd_admin
      appMonitor status
      clear_kernel_tables
      clear_portal_cache
      debug <options>
      ics_update
      isEnabled
      license <options>
      policy [{graceful | hard}]
      revoke <Certificate Serial Number>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`appMonitor` *<options>*	Controls the Application Monitor. The Application Monitor is a software component that monitors internal servers to track their up time. If problems are found, a system alert log is created. The available <*options*> are: ▪ `restart` - Restarts the Application Monitor. ▪ `start` - Start the Application Monitor. ▪ `status` - Shows the status of the Application Monitor feature, the applications monitored by the Application Monitor and their status. ▪ `stop` - Stops the Application Monitor.
`clear_kernel_tables`	Clears all Mobile Access kernel tables.

Parameter	Description
`clear_portal_cache`	Clears the cache for the applications presented in the Mobile Access Portal for all open sessions.
`debug set TDERROR_ALL_ALL=5`	Enables all `cvpnd debug` output for the running **cvpnd** process. The output is in the `$CVPNDIR/log/cvpnd.elg` file. **Note** - When you enable all debug topics, it might impact the performance. Debug topics are provided by *Check Point Support*.
`debug off`	Disables all `cvpnd debug` output.
`debug trace on` `debug trace users=<Username>`	The `TraceLogger` feature generates full captures of incoming and outgoing authenticated Mobile Access traffic. The output is saved in the `$CVPNDIR/log/trace_log/` directory. ▪ `debug trace on` - Enables the `TraceLogger` feature for all users. ▪ `debug trace users=<Username>` - Enables the `TraceLogger` feature for a specified username **Important:** ▪ The `TraceLogger` feature has a major effect on performance, because all traffic is saved as files. ▪ The `TraceLogger` feature uses a lot of disk space, because all traffic is saved as files. After a maximum number of files is saved, the oldest files are removed from the disk, which also has a performance cost. ▪ The `TraceLogger` feature creates a security concern: end-user passwords that are sent to internal resources might appear in the capture files.
`ics_update`	Updates the Mobile Access services after you published a new ICS update.
`isEnabled`	Checks if Mobile Access is enabled by policy.
`license <options>`	Shows Mobile Access license count and status: ▪ `all` - Shows information about the MOB and MOBMAIL licenses. ▪ `mob` - Shows information about the MOB license. ▪ `mobmail` - Shows information about the MOBMAIL license.

Parameter	Description
`policy [{graceful | hard}]`	Updates the Mobile Access services according to the current policy: ■ `policy` - For Apache services, each `httpd` process waits until its current request is finished, then exits. ■ `policy graceful` - For Apache services, each `httpd` process waits until its current request is finished, then exits. ■ `policy hard` - For Apache services, all `httpd` processes exit immediately, terminating all current `http` requests.
`revoke <Certificate Serial Number>`	Notifies about revocation of a certificate with a given serial number.

cvpnd_settings

Description

Changes a Mobile Access Gateway local configuration file `$CVPNDIR/conf/cvpnd.C`.

The `cvpnd_settings` commands allow to get attribute values or set them in order to configure the **cvpnd** process.

Important:

- Changes made by with the `cvpnd_settings` command are **not** saved during the Mobile Access Gateway upgrade. Keep a backup of your `$CVPNDIR/conf/cvpnd.C` file after you make manual changes.
- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Warning - The **cvpnd** process may not start, if you make a mistake in the syntax - attribute names or their values.

General Syntax

```
cvpnd_settings [<Configuration File>] {get | set | add | listAdd |
listRemove | internal} <Attribute-Name> [<Attribute-Value>]
```

Syntax for DynamicID Resend

```
cvpnd_settings [<Configuration File>] {set | get}
smsMaxResendRetries [<Number>]
```

Syntax for Kerberos Authentication

```
cvpnd_settings [<Configuration File>] {set | get} useKerberos
{true | false}
```

```
cvpnd_settings [<Configuration File>] {listAdd | listRemove}
kerberosRealms [<Your AD Name>]
```

Parameters

Run this command to see the full explanation of the parameters: `cvpnd_settings -h`

Parameter	Description
`-h`	Shows built-in help with full explanation of the parameters.
<Configuration File>	Specifies the path and the name of configuration file to change.
`get`	Gets the value of an existing attribute, or values of a list.
`set`	Sets the value of an attribute. If the specified attribute does not exist in the configuration file, then the command adds it.
`add`	Adds a new attribute. If the specified attribute already exists in the configuration file, then the command does not change it.
`listAdd`	Adds the specified attribute to a list.
`listRemove`	Removes the specified attribute from a list.
`internal`	Specifies that the command must change the `$CVPNDIR/conf/cvpnd_internal_settings.C` file instead of the `$CVPNDIR/conf/cvpnd.C` file.
<Attribute-Name>	Specifies the attribute name.
<Attribute-Value>	Specifies the attribute value.
<Number>	Specifies the number of SMS resend attempts.
<Your AD Name>	Specifies the Active Directory name.

Examples 1 - Set the value of the attribute 'myFlag' to 1

```
cvpnd_settings set myFlag 1
```

Examples 2 - See the current value of the attribute 'myFlag'

```
cvpnd_settings get myFlag
```

Examples 3 - Empty the value of the attribute 'myFlag', or create a new attribute/list 'myFlag'

```
cvpnd_settings set myFlag
```

Examples 4 - Add the attribute 'myFlag' with the value 'a.example.com' to a list

```
cvpnd_settings listAdd myFlag a.example.com
```

cvpn_ver

Description

Shows the version of the Mobile Access Software Blade.

Best Practice - Run the "`fw ver -k`" command to get all version details (see *"fw ver" on page 1249*).

Syntax

```
cvpn_ver
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Example

```
[Expert@MyGW:0]# cvpn_ver
This is Check Point Mobile Access R81.20 - Build 123
[Expert@MyGW:0]#
```

cvpnrestart

Description

Restarts all Mobile Access Software Blade services.

Warning - While this command does not terminate sessions, it closes all TCP connections. End-users might lose their work.

Syntax

```
cvpnrestart [--with-pinger]
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`--with-pinger`	Restarts the **Pinger** service, responsible for ActiveSync and Outlook Web Access push mail notifications.

cvpnstart

Description

Starts all Mobile Access Software Blade services, after you stopped them with the *"cvpnstop" on page 1861* command.

Syntax

```
cvpnstart
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

cvpnstop

Description

Stops all Mobile Access Software Blade services.

Warning - While this command does not terminate sessions, it closes all TCP connections. End-users might lose their work.

Syntax

```
cvpnstop
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

deleteUserSettings

Description

Deletes all persistent settings (favorites, cookies, credentials) of one or more end-users.

Syntax

```
deleteUserSettings [-s] <Username1> [<Username2> ...]
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`-s`	Runs in silent mode with no output to the end-user's screen.
<Username>	Specifies the user name, whose settings to delete. **Notes:** ■ When you refer to an internal user, use its username. ■ When you refer to an LDAP user, use the full DN according to your LDAP settings.

Example 1 - Delete an internal user named 'user1

```
deleteUserSettings [-s] user1
```

Example 2 - Delete an LDAP user named 'user1', whose DN is 'CN=user1,OU=users,DC=example,DC=com':

```
deleteUserSettings [-s] CN=user1,OU=users,DC=example,DC=com
```

fwpush

Description

Sends command interrupts to the **fwpushd** process on the Mobile Access Gateway.

Note - Users get the push notifications only while they are logged in.

Syntax

```
fwpush
      debug <options>
      del <options>
      info
      print
      send <options>
      unsub <options>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`debug {off | on | reset | set all all | stat}`	Controls the debug of the Mobile Access Push Notifications daemon. For more information, see sk109039.

Parameter	Description

`del {-token <Token> | -uid <User-UID>}`	Deletes a specified token, or all tokens for a specified user.
	The available options are:
	■ Delete the specified token for all users:
	`fwpush del -token <Token>`
	■ Delete all tokens for a specified user:
	`fwpush del -uid <User-UID>`

`info`	Gets data on notifications in the push queue: ■ Number of items in queues ■ Number of seconds the oldest item is in the queue ■ Number of seconds the newest item is in the queue ■ Number of seconds a batch waits in the queue ■ Number of seconds to the sending of the next batch ■ Number of batch errors and authentication request timeouts
`print`	Shows the push notifications queue and the pending batches.
`send -token <Token> -os {iPhone | Android} -msg "<Notification Message>"` `send {-user <Username> | -uid <User-UID>} -msg "<Notification Message>"`	Sends an on-demand push notification message from a command line. **Important** - Before you use the "`fwpush send`" command, make sure the user is: (A) registered on the Exchange Server, (B) connected.

Parameter	Description

`unsub {<Token> | -user <Username> | -uid <User-UID> | -all}`	Unsubscribes a user from push notifications.
	The available options are:
	■ Unsubscribe all users from the specified token:
	`fwpush unsub <Token>`
	■ Unsubscribe the specified user from all tokens:
	`fwpush unsub -user <Username>`
	or
	`fwpush unsub -uid <User-UID>`
	■ Unsubscribe all users from all tokens:
	`fwpush unsub -all`

Viewing the details of connected users

```
UserSettingsUtil show_exchange_registered_users
```

Example output:

```
[Expert@MyGW:0]# UserSettingsUtil show_exchange_registered_users
User Name: CN=JohnD,OU=USERS,OU=RND,OU=PO,OU=USA,DC=AD,DC=CHECKPOINT,DC=COM User Settings id:
c4b6c6fbb0c4xxxxxxxx265e93e0e372
Push Token: xxxxxxxxxxxxx65b48e424023ebxxxxxxxxca22ea788cfb3cxxxxxxxxx Device id:
46c5XXXXcc1d10b4e18cf5a1xxxxxxxx
[Expert@MyGW:0]#
```

Notes:

- To use the "*<Token>*" parameter in the "`fwpush`" commands, use the value of the **Push Token** attribute.
  In the above example:
  `xxxxxxxxxxxxx65b48e424023ebxxxxxxxxca22ea788cfb3cxxxxxxxxx`
- To use the "*<Username>*" parameter in the "`fwpush`" commands, use the value of the **CN** attribute.
  In the above example: `JohnD`
- To use the "*<User-UID>*" parameter in the "`fwpush`" commands, use the value of the **User Settings id** attribute.
  In the above example: `c4b6c6fbb0c4xxxxxxxx265e93e0e372`

Example

```
[Expert@MyGW:0]# fwpush send -uid JohnD -msg "Hello - push"
```

ics_updates_script

Description

Manually starts an Endpoint Security on Demand (ESOD) update on the Mobile Access Gateway.

For more information, see the contents of the `$CVPNDIR/bin/ics_updates_script` file.

Syntax

```
$CVPNDIR/bin/ics_updates_script <Path to Local ICS Updates Package>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
<Path to Local ICS Updates Package>	Specifies the full path to the local ICS Updates package. Do **not** specify the name of the ICS Updates package.

listusers

Description

Shows a list of end-users connected to the Mobile Access Gateway, along with their source IP addresses.

Syntax

```
listusers
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Example

```
[Expert@MyGW:0]# listusers
------------------------------
UserName    | IP
------------------------------
Tom , 192.168.0.51
John , 192.168.0.130
Jane , 192.168.0.7
[Expert@MyGW:0]#
```

rehash_ca_bundle

Description

Imports all of the Certificate Authority (CA) files from the `$CVPNDIR/var/ssl/ca-bundle/` directory into the Mobile Access trusted CA bundle.

The trusted CA bundle is used when the Mobile Access Gateway accesses an internal server (such as OWA) through HTTPS.

If the SSL server certificate of the internal server is not trusted by the Mobile Access Gateway, the Mobile Access Gateway responds based on the settings for the Internal Web Server Verification feature. The default setting is **Monitor**.

To accept certificates from a specified server, add its server certificate CA to the CA bundle.

Syntax

```
rehash_ca_bundle
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Example

```
[Expert@MyGW:0]# rehash_ca_bundle
Doing /opt/CPcvpn-R81.20/var/ssl/ca-bundle/
AC_Ra__z_Certic__mara_S.A..pem => 6f2c1157.0
AOL_Time_Warner_Root_Certification_Authority_1.pem => ed9bb25c.0
... ... ...
beTRUSTed_Root_CA_-_RSA_Implementation.pem => 16b3fe3c.0
thawte_Primary_Root_CA.pem => 2e4eed3c.0
[Expert@MyGW:0]#
```

UserSettingsUtil

Description

Shows details of users connected to the Mobile Access Gateway.

Syntax

```
UserSettingsUtil show_exchange_registered_users [<Username>]
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
<Username>	Specifies the user name. **Notes:** ■ When you refer to an internal user, use its username. ■ When you refer to an LDAP user, use the full DN according to your LDAP settings.

Example 1 - To show all users

```
[Expert@MyGW:0]# UserSettingsUtil show_exchange_registered_users
User Name: CN=JohnD,OU=USERS,OU=RND,OU=PO,OU=USA,DC=AD,DC=CHECKPOINT,DC=COM User Settings id:
c4b6c6fbb0c4xxxxxxxx265e93e0e372
Push Token: xxxxxxxxxxxxx65b48e424023ebxxxxxxxxca22ea788cfb3cxxxxxxxxxx Device id:
46c5XXXXcc1d10b4e18cf5a1xxxxxxxx
[Expert@MyGW:0]#
```

Example 2 - To show an internal user named 'user1'

```
[Expert@MyGW:0]# UserSettingsUtil show_exchange_registered_users user1
```

Example 3 - To show an LDAP user named 'user1', whose DN is 'CN=user1,OU=users,DC=example,DC=com'

```
[Expert@MyGW:0]# UserSettingsUtil show_exchange_registered_users CN=user1,OU=users,DC=example,DC=com
```

Data Loss Prevention Commands

For more information about Data Loss Prevention, see the *R81.20 Data Loss Prevention Administration Guide*.

dlpcmd

Description

Control the Data Loss Prevention Engine on a Security Gateway.

Syntax

```
dlpcmd [-s]
      action_by_admin <options>
      getquarantined
      getquarantinedcount
      getquarantinedsize
      ramdisk <options>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`-s`	Silent mode - does not print failure messages on the screen.

`action_by_admin <options>`	Sends or deletes the specified quarantined email by its public GUID from quarantine.
	The available options are:
	■ Send (Release) the specified quarantined email:
	`dlpcmd action_by_admin 1 {Public GUID of the Quarantined Email} ["Justification for Sending or Deleting"] ["Administrator Name"]`
	■ Delete (Discard) the specified quarantined email:
	`dlpcmd action_by_admin 2 {Public GUID of the Quarantined Email} ["Justification for Sending or Deleting"] ["Administrator Name"]`
	Notes:
	■ You must enclose the email ID in curly brackets `{}`.
	■ You can see this action in Audit Logs in SmartConsole. For example, see sk117753.

`getquarantined`	Shows the list of all quarantined emails.
`getquarantinedcount`	Shows the number of all quarantined emails.
`getquarantinedsize`	Shows the total size of all emails in quarantine.
`ramdisk <options>`	Shows and controls the DLP RAM Disk. The available options are: ■ `off` - Disables the DLP RAM Disk ■ `on` - Enables the DLP RAM Disk ■ `size <Size in MBytes>` - Configures the size of the DLP RAM Disk ■ `status` - Shows the DLP RAM Disk information **Important** - All operations except "`status`" require a restart of all services (*"cpstop" on page 1029* and *"cpstart" on page 1018*).

Example

```
[Expert@MyGW:0]# dlpcmd getquarantined
Printing quarantined mails:
Mail GUID: {8698E6EC-340C-9115-0AB6-F6CA9986147F}; Arrival date: Sun Dec  1 13:38:32 2019; exp
date: Sun Dec  8 13:38:32 2019; sender: dataowner-JOHNDOE;
... ... ...
[Expert@MyGW:0]#
[Expert@MyGW:0]# dlpcmd action_by_admin 1 {8698E6EC-340C-9115-0AB6-F6CA9986147F} "Released an
Email" "Main Admin"
[Expert@MyGW:0]#
[Expert@MyGW:0]# dlpcmd getquarantined
No quarantined mails
[Expert@MyGW:0]#
```

VSX Commands

For more information about VSX, see the *R81.20 VSX Administration Guide*.

cpconfig

Description

This command starts the Check Point Configuration Tool.

This tool configures specific settings for the installed Check Point products.

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms (Maestro and Chassis), you must connect to the applicable Security Group.

Syntax on a Security Gateway / Cluster Member in Gaia Clish or the Expert mode

```
cpconfig
```

Syntax on a Scalable Platform Security Group in Gaia gClish or the Expert mode

```
cpconfig
```

Menu Options

Note - The options shown depend on the configuration and installed products.

Menu Option	Description
Licenses and contracts	Manages Check Point licenses and contracts on this Security Gateway or Cluster Member.
SNMP Extension	Obsolete. Do **not** use this option anymore. To configure SNMP, see the *R81.20 Gaia Administration Guide* - Chapter *System Management* - Section *SNMP*.
PKCS#11 Token	Register a cryptographic token, for use by Gaia Operating System. See details of the token, and test its functionality.
Random Pool	Configures the RSA keys, to be used by Gaia Operating System.

Menu Option	Description
Secure Internal Communication	Manages SIC on the Security Gateway or Cluster Member. This change requires a restart of Check Point services on the Security Gateway or Cluster Member. For more information, see: ■ The *R81.20 Security Management Administration Guide*. ■ sk65764: How to reset SIC.
Enable cluster membership for this gateway	Enables the cluster membership on the Security Gateway. This change requires a reboot of the Security Gateway. For more information, see the: ■ *R81.20 Installation and Upgrade Guide*. ■ *R81.20 ClusterXL Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (Maestro and Chassis).
Disable cluster membership for this gateway	Disables the cluster membership on the Security Gateway. This change requires a reboot of the Security Gateway. For more information, see the: ■ *R81.20 Installation and Upgrade Guide*. ■ *R81.20 ClusterXL Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (Maestro and Chassis).
Enable Check Point Per Virtual System State	Enables Virtual System Load Sharing on the VSX Cluster Member. For more information, see the *R81.20 VSX Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (Maestro and Chassis).
Disable Check Point Per Virtual System State	Disables Virtual System Load Sharing on the VSX Cluster Member. For more information, see the *R81.20 VSX Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (Maestro and Chassis).

Menu Option	Description
Enable Check Point ClusterXL for Bridge Active/Standby	Enables Check Point ClusterXL for Bridge mode. This change requires a reboot of the Cluster Member. For more information, see the: ■ *R81.20 Installation and Upgrade Guide*. ■ *R81.20 ClusterXL Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (Maestro and Chassis).
Disable Check Point ClusterXL for Bridge Active/Standby	Disables Check Point ClusterXL for Bridge mode. This change requires a reboot of the Cluster Member. For more information, see the: ■ *R81.20 Installation and Upgrade Guide*. ■ *R81.20 ClusterXL Administration Guide*. **Note** - This section does **not** apply to Scalable Platforms (Maestro and Chassis).
Check Point CoreXL	Manages CoreXL and Firewall mode on the Security Gateway / Cluster Member / Scalable Platform Security Group. After all changes in CoreXL configuration, you must reboot the Security Gateway / Cluster Member / Security Group. For more information, see the *R81.20 Performance Tuning Administration Guide*.
Automatic start of Check Point Products	Shows and controls which of the installed Check Point products start automatically during boot.
Exit	Exits from the Check Point Configuration Tool.

Example 1 - Menu on a single Security Gateway

```
[Expert@MySingleGW:0]# cpconfig
This program will let you re-configure
your Check Point products configuration.


Configuration Options:
----------------------
(1) Licenses and contracts
(2) SNMP Extension
(3) PKCS#11 Token
(4) Random Pool
(5) Secure Internal Communication
(6) Enable cluster membership for this gateway
(7) Check Point CoreXL
(8) Automatic start of Check Point Products

(9) Exit

Enter your choice (1-9) :
```

Example 2 - Menu on a Cluster Member

```
[Expert@MyClusterMember:0]# cpconfig
This program will let you re-configure
your Check Point products configuration.


Configuration Options:
----------------------
(1) Licenses and contracts
(2) SNMP Extension
(3) PKCS#11 Token
(4) Random Pool
(5) Secure Internal Communication
(6) Disable cluster membership for this gateway
(7) Enable Check Point Per Virtual System State
(8) Enable Check Point ClusterXL for Bridge Active/Standby
(9) Check Point CoreXL
(10) Automatic start of Check Point Products

(11) Exit

Enter your choice (1-11) :
```

vsenv

Description

Changes the shell's current context to the specified Virtual Device.

Syntax

```
vsenv [{<VSID> | <Name of Virtual Device>}]
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
No Parameters	Changes the context to the default Virtual Device 0.
<VSID>	Specifies the Virtual Device by its ID.
<Name of Virtual Device>	Specifies the Virtual Device by its Name.

Note - To see the configured Virtual Devices, run the "`vsx stat -v`" command.

Example 1 - Changing the context to the default Virtual Device 0

```
[Expert@MyVsxGW:0]# vsenv
Context is set to Virtual Device VSX2_192.168.3.242 (ID 0).
[Expert@MyVsxGW:0]#
```

Example 2 - Changing the context to the specific Virtual Device

```
[Expert@MyVsxGW:0]# vsenv 2
Context is set to Virtual Device VS2 (ID 2).
[Expert@MyVsxGW:2]#
```

VSX

Description

- Shows VSX configuration.
- Fetches VSX configuration.
- Shows and configures Memory Resource Control.

Syntax

```
vsx
      fetch <options>
      fetch_all_cluster_policies
      fetchvs <options>
      get
      mstat <options>
      resctrl
      showncs <options>
      sicreset
      stat <options>
      unloadall
      vspurge
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Note - The `fw6 vsx` commands are **not** supported.

Parameters

Parameter	Description
`fetch <options>`	Fetches configuration for VSX Gateway. See *"vsx fetch" on page 1886*.
`fetch_all_cluster_policies`	Fetches security policy for all Virtual Systems and Virtual Routers from cluster peers. See *"vsx fetch_all_cluster_policies" on page 1888*.
`fetchvs <options>`	Fetches configuration for a Virtual System. See *"vsx fetchvs" on page 1889*.

Parameter	Description
`get`	Shows the information about the current VSX context. See *"vsx get" on page 1890*.
`mstat <options>`	Shows and configures Memory Resource Control. See *"vsx mstat" on page 1891*.

Parameter	Description

`resctrl`	From R80.40, the CPU Resource Control is integrated into the CPView utility.
	1. Go to the context of Virtual System 0:
	■ In the Expert mode:
	`vsenv`
	■ In Gaia Clish:
	`set virtual-system 0`
	2. Run the CPView:
	`cpview`
	See *"cpview" on page 41*.
	3. From the top, click:
	Advanced > VSX > VSs > Physical-Resources
	Notes:
	■ This tab shows the CPU consumption by Virtual Systems and by Virtual Routers.
	■ The "**CPU %**" column shows the percentage of CPU used by all the processes of each Virtual System.
	The column shows a percentage of a single CPU (the same behavior as in the "`top`" command).
	Example:
	• There are 4 CPU cores on the VSX Gateway.
	• The processes of the Virtual System "VS1" are using:
	◦ 30% of CPU 0
	◦ 40% of CPU 1
	◦ 50% of CPU 2
	◦ 10% of CPU 3
	In such case, the "**CPU %**" column shows 130% for VS1.
	■ To get the CPU usage for the VSX Gateway / VSX Cluster Member, divide the "**CPU %**" value in the **Total Resource Consumption** section by the number of the CPU cores.

`showncs <options>`	Shows Check Point Network Configuration Script (NCS) for Virtual Device. See *"vsx showncs" on page 1895*.

Parameter	Description
`sicreset`	Resets SIC for Virtual System or Virtual Router in the current VSX context. See *"vsx sicreset" on page 1896*.
`stat <options>`	Shows status information for VSX Gateway. See *"vsx stat" on page 1897*.
`unloadall`	Unloads security policy for all Virtual Systems and Virtual Routers. See *"vsx unloadall" on page 1900*.
`vspurge`	Cleans unused entries for Virtual Devices. Fetches configuration file for Virtual Devices. See *"vsx vspurge" on page 1901*.

vsx fetch

Description

Fetches the most current configuration files from the Security Management Server or Main Domain Management Server, and applies it to the VSX Gateway.

Syntax

```
vsx fetch [-v] [-q] [-s] local
vsx fetch [-v | -q | -s] [-f <Configuration File>]
vsx fetch [-v | -q] -C "NCS Command"
vsx fetch [-v | -q | -c | -n | -s] [<Management Server>]
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`-c`	Specifies that this is a VSX Cluster.
`-n`	Specifies not to apply the `local.vsall`, if VSX configuration, as fetched from Management Server, is up-to-date.
`-q`	Specifies to run in quiet mode - shows only summary information.
`-s`	Specifies to fetch concurrently for multi-processor environment.
`-v`	Specifies to run in verbose mode - shows detailed information.
`local`	Reads the configuration file `$FWDIR/state/local/VSX/local.vsall` and executes the Network Configuration Script (NCS).
`-f <Configuration File>`	Fetches the specified configuration with NCS commands file instead of the default `local.vsall` file.
`-C "NCS Command"`	Executes the specified NCS command.

Parameter	Description
<Management Server>	Fetches the `local.vsall` from the specified Management Server (by resolvable hostname, or IP address), replaces and runs it. **Note** - If you do not specify the Management Server explicitly, the command takes it from the `$FWDIR/conf/masters` file on the VSX Gateway.

Return Values

- 0 (zero) indicates that the command executed successfully.
- Any other value indicates an error.

Example

```
[Expert@MyVsxGW:0]# vsx fetch
Fetching VSX Configuration From: 192.168.30.40

 Local VSX Configuration is Up-To-Date.
 Cleaning un-used Virtual Systems entries (local.vskeep).

 Purge operation succeeded.
 Fetching Virtual Systems configuration file (local.vsall).

SecureXL device has been enabled for vsid 1
SecureXL device has been enabled for vsid 2
SecureXL device has been enabled for vsid 3
Virtual Systems configuration file installed successfully
[Expert@MyVsxGW:0]#
```

vsx fetch_all_cluster_policies

Description

Fetches security policy for all Virtual Systems and Virtual Routers from cluster peers.

Syntax

```
vsx fetch_all_cluster_policies [-v]
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`-v`	Specifies to run in verbose mode - shows detailed information.

Return Values

- 0 (zero) indicates that the command executed successfully.
- Any other value indicates an error.

vsx fetchvs

Description

Fetches configuration file for the specified Virtual Device based on information stored locally on the VSX Gateway.

Syntax

```
vsx fetchvs [-v | -q] [{<VSID> | <Name of Virtual Device>}]
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`-q`	Specifies to run in quiet mode - shows only summary information.
`-v`	Specifies to run in verbose mode - shows detailed information.
<Name of Virtual Device>	Specifies the name of the Virtual Device.
<VSID>	Specifies the ID of the Virtual Device.

Return Values

- 0 (zero) indicates that the command executed successfully.
- Any other value indicates an error.

Example

```
[Expert@MyVsxGW:0]# vsx fetchvs 2
```

vsx get

Description

Shows the information about the current VSX context.

Syntax

```
vsx get
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Return Values

- 0 (zero) indicates that the command executed successfully.
- Any other value indicates an error.

Example

```
[Expert@MyVsxGW:0]# vsx get
Current context is VSX Gateway MyVsxGW (ID 2).
[Expert@MyVsxGW:0]#
```

vsx mstat

Description

Shows and configures Memory Resource Control.

Output shows these global memory resources:

Resource	Description
Memory Total	Total physical memory on the VSX Gateway.
Memory Free	Available physical memory.
Swap Total	Total of swap memory.
Swap Free	Available swap memory.
Swap-in rate	Total memory swaps per second.

In addition:

1. Run the `cpview` command (see *"cpview" on page 41*).
2. From the top, click:

   Advanced > VSX > VSs > Physical-Resources

Syntax

```
vsx mstat help
```

```
vsx mstat
      [-vs <VSID>] [unit <Unit>] [sort {<Number> | all}]
      debug
      disable
      enable
      status
      swap <Minutes>
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`help`	Shows the built-in usage.

Parameter	Description
No Parameters	Shows the total memory consumption for each Virtual System.
`-vs <VSID>`	Specifies the Virtual Systems by their IDs. You can specify: ■ One Virtual System. Example: `-vs 1` ■ Many individual Virtual Systems (separate their IDs with spaces). Example: `-vs 2 3` ■ A range of Virtual Systems. Example: `-vs 4-6` **Note** - You can combine all the available options (separate them with spaces). Example: `-vs 1 4-6`
`unit <Unit>`	Specifies the memory measurement unit shown in the command output: ■ `B` - bytes ■ `K` - kilobytes ■ `M` - megabytes (default) ■ `G` - gigabytes
`sort {<Number> | all}`	Sorts the Virtual Systems in the output by their memory size. Specifies the number of Virtual Systems shown in the command output. Use `all` to show all Virtual Systems. If you do not specify this flag, the Virtual Systems in the output are sorted by their VSID.
`debug`	Shows memory consumption debug information for each Virtual System by fields, which are defined in the configuration file.
`disable`	Disables the Memory Resource Control. **Note** - This change applies immediately and does not require a reboot.
`enable`	Enables the Memory Resource Control. **Note** - This change requires a reboot.
`status`	Shows the current Memory Resource Control status.

Parameter	Description
`swap <Minutes>`	Specifies the swap-in sample rate in minutes. Enter the number of minutes that the system measures memory swaps to determine the swap-in rate. Only integers are valid values. The default swap-in sample rate is `10`. **Notes:** ■ Swap-in sample rate is a system-wide Linux setting. When you change the value for memory monitoring, all the swap-in rates are calculated according to the new value. ■ When you enable the monitoring memory resources feature, the swap-in rate setting is saved. When you disable the feature, the system restores the saved setting.

Return Values

- 0 (zero) indicates that the command executed successfully.
- Any other value indicates an error.

Example 1

```
[Expert@MyVsxGW:0]# vsx mstat unit M sort all

VSX Memory Status
=================
Memory Total: 7753.95 MB
Memory Free: 7168.71 MB
Swap Total: 3992.71 MB
Swap Free: 3992.71 MB
Swap-in rate: 8796093022208.00 MB

 VSID | Memory Consumption
======+====================
    0 | 260.79 MB
    1 | 0.00 MB

[Expert@MyVsxGW:0]#
```

Example 2

```
[Expert@MyVsxGW:0]# vsx mstat -vs 0 unit G

VSX Memory Status
=================
Memory Total: 7.572 GB
Memory Free: 7.001 GB
Swap Total: 3.899 GB
Swap Free: 3.899 GB
Swap-in rate: 8589934592.000 GB

 VSID | Memory Consumption
======+====================
    0 |          0.255 GB

[Expert@MyVsxGW:0]#
```

Example 3

```
[Expert@MyVsxGW:0]# vsx mstat debug

VSX Memory Status
=================
Memory Total: 7940048.00 KB
Memory Free: 7339864.00 KB
Swap Total: 4088532.00 KB
Swap Free: 4088532.00 KB
Swap-in rate: 9007199254740992.00 KB

 VSID | Private_Clean | Private_Dirty | DispatcherGConn | DispatcherHTab |    SecureXL |
DispatcherGConn6 | DispatcherHTab6 | SecureXL6

======+===============+===============+=================+================+=============+=======
===========+=================+===========
    0 |   34456.00 KB |  182104.00 KB |         6.09 KB |        0.00 KB | 51071.91 KB |
 0.00 KB |         0.00 KB |   0.00 KB
    1 |       0.00 KB |       0.00 KB |         0.00 KB |        0.00 KB |     0.00 KB |
 0.00 KB |         0.00 KB |   0.00 KB

Note: To add a field to memory table please uncomment the required field (delete the leading
'#')
      To remove a field from memory table please comment out the required field (add a leading
'#')
      Configuration is done in the file /opt/CPsuite-R81.20/fw1/conf/memoryinfo.conf

[Expert@MyVsxGW:0]#
```

vsx showncs

Description

Shows Check Point Network Configuration Script (NCS) for a Virtual Device.

Syntax

```
vsx showncs {<VSID> | <Name of Virtual Device>}
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
<Name of Virtual Device>	Specifies the name of the Virtual Device.
<VSID>	Specifies the ID of the Virtual Device.

Return Values

- 0 (zero) indicates that the command executed successfully.
- Any other value indicates an error.

vsx sicreset

Description

Resets SIC for Virtual System or Virtual Router in the current VSX context.

Notes:

- This operation is **not** supported for the context of VSX Gateway itself (VS0).
- On the Management Server, run the *"cpca_client revoke_cert" on page 116* command to cancel the old certificate.
- In SmartConsole, open the Virtual System object and immediately click **OK**. This action creates a new certificate, and transfers the certificate to the VSX Gateway.

Syntax

```
vsenv {<VSID> | <Name of Virtual Device>}
vsx sicreset {<VSID> | <Name of Virtual Device>}
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
<Name of Virtual Device>	Specifies the name of the Virtual Device.
<VSID>	Specifies the ID of the Virtual Device.

Return Values

- 0 (zero) indicates that the command executed successfully.
- Any other value indicates an error.

vsx stat

Description

Shows status information for VSX Gateway.

Syntax

```
vsx stat [-l] [-v] [<VSID>]
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`-l`	Shows a list of all Virtual Devices and their applicable information.
`-v`	Shows a summary table with all Virtual Devices.
<VSID>	Specifies a Virtual Device by its ID.

Return Values

- 0 (zero) indicates that the command executed successfully.
- Any other value indicates an error.

Example 1 - Show a summary table with all Virtual Devices.

```
[Expert@MyVsxGW:2]# vsx stat -v
VSX Gateway Status
==================
Name:            VSX1_192.168.3.241
Access Control Policy: VSX_Cluster_VSX
Installed at:    20Sep2019 22:06:33
Threat Prevention Policy: <No Policy>
SIC Status:      Trust

Number of Virtual Systems allowed by license:          25
Virtual Systems [active / configured]:                  2 / 2
Virtual Routers and Switches [active / configured]:     0 / 0
Total connections [current / limit]:                    5 / 44700

Virtual Devices Status
======================

 ID  | Type & Name | Access Control Policy | Installed at    | Threat Prevention Policy | SIC
Stat
-----+-------------+-----------------------+-----------------+--------------------------+-------
--
   1 | S VS1       | VS_Policy             | 20Sep2019 22:07 | <No Policy>              | Trust
   2 | S VS2       | VS_Policy             | 20Sep2019 22:07 | <No Policy>              | Trust

Type: S - Virtual System, B - Virtual System in Bridge mode,
      R - Virtual Router, W - Virtual Switch.

[Expert@MyVsxGW:2]#
```

Example 2 - Show a list of all Virtual Devices and their applicable information.

```
[Expert@MyVsxGW:2]# vsx stat -l

VSID:            0
VRID:            0
Type:            VSX Gateway
Name:            VSX1_192.168.3.241
Security Policy: VSX_Cluster_VSX
Installed at:    20Sep2019 22:06:33
SIC Status:      Trust
Connections number: 5
Connections peak:   43
Connections limit:  14900

VSID:            1
VRID:            1
Type:            Virtual System
Name:            VS1
Security Policy: VS_Policy
Installed at:    20Sep2019 22:07:03
SIC Status:      Trust
Connections number: 0
Connections peak:   3
Connections limit:  14900

VSID:            2
VRID:            2
Type:            Virtual System
Name:            VS2
Security Policy: VS_Policy
Installed at:    20Sep2019 22:07:01
SIC Status:      Trust
Connections number: 0
Connections peak:   2
Connections limit:  14900
[Expert@MyVsxGW:2]#
```

Example 3 - Shows the information for the specified Virtual Device

```
[Expert@MyVsxGW:2]# vsx stat 2

VSID:            2
VRID:            2
Type:            Virtual System
Name:            VS2
Security Policy: VS_Policy
Installed at:    20Sep2019 22:07:01
SIC Status:      Trust
Connections number: 0
Connections peak:   2
Connections limit:  14900
[Expert@MyVsxGW:2]#
```

vsx unloadall

Description

Unloads security policy for all Virtual Systems and Virtual Routers.

See sk33065: Unloading policy from a VSX Security Gateway.

Syntax

```
vsx unloadall
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Return Values

- 0 (zero) indicates that the command executed successfully.
- Any other value indicates an error.

vsx vspurge

Description

Removes Virtual Devices that are no longer defined in the management database, but were not removed from the VSX Gateway, because the VSX Gateway was down or disconnected when the management server pushed the updated VSX configuration.

This command cleans all unused Virtual Devices entries (from the NCS `local.vskeep`) and fetches the VSX configuration file (NCS `local.vskeep`) again.

Syntax

```
vsx vspurge [-q | -v] [-f <purge_file>]
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`-q`	Specifies to run in quiet mode - shows only summary information.
`-v`	Specifies to run in verbose mode - shows detailed information.
`-f <purge_file>`	Specifies the path and the name of the file, in which the command saves the purged information.

Return Values

- 0 (zero) indicates that the command executed successfully.
- Any other value indicates an error.

vsx_util

Description

Performs various VSX maintenance tasks.

You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main* Domain Management Server on Multi-Domain Server).

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util -h
```

```
vsx_util <Command> [-s <Mgmt Server>] [-u <UserName>] [-c <Name of VSX Object>] [-m <Name of VSX Cluster Member>]
```

Parameters

Parameter	Description
`-h`	Shows the built-in usage.
`<Command>`	Specifies the `vsx_util` sub-command. See the table below.
`-s` *`<Mgmt Server>`*	Specifies the IP address or resolvable hostname of the Security Management Server, or Main Domain Management Server.
`-u` *`<UserName>`*	Specifies the administrator username.
`-c` *`<Name of VSX Object>`*	Specifies the name of the VSX Gateway or VSX Cluster object.
`-m` *`<Name of VSX Cluster Member>`*	Specifies the name of the VSX Gateway or VSX Cluster Member object.

Important - The `vsx_util` command requires you to enter this information:

- IP address or Hostname of the Security Management Server, or *Main* Domain Management Server.
- Management Server Administrator user name and password.
- The applicable VSX object, on which the command operates.
- Most of the `vsx_util` sub-commands are interactive and require additional user input.

The 'vsx_util' sub-commands

Sub-command	Description
`vsx_util add_member`	Adds a new Cluster Member to a VSX Cluster and pushes the VSX Cluster configuration to the new VSX Cluster Member. See *"vsx_util add_member" on page 1907*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).
`vsx_util change_ interfaces`	Automatically replaces designated existing interfaces with new interfaces on all Virtual Devices, to which the existing interfaces connect. See *"vsx_util change_interfaces" on page 1909*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).
`vsx_util change_mgmt_ ip`	Changes the VSX Management IP address (within the same subnet) of a VSX Gateway or VSX Cluster Member. See *"vsx_util change_mgmt_ip" on page 1913*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).
`vsx_util change_mgmt_ subnet`	Changes (or adds) the VSX Management IP address of a VSX Gateway or VSX Cluster Member to a new subnet. See *"vsx_util change_mgmt_subnet" on page 1914*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).
`vsx_util change_ private_net`	Changes the IP address of the Internal Communication Network in a VSX Cluster. See *"vsx_util change_private_net" on page 1916*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).
`vsx_util convert_ cluster`	Converts the VSX Cluster mode between High Availability (default) and Virtual System Load Sharing. See *"vsx_util convert_cluster" on page 1918*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).

Sub-command	Description
`vsx_util downgrade`	Downgrades the version of a VSX Gateway or VSX Cluster in the management database. See *"vsx_util downgrade" on page 1920*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).
`vsx_util reconfigure`	Restores VSX configuration on a VSX Gateway or VSX Cluster Member. See *"vsx_util reconfigure" on page 1921*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).
`vsx_util remove_ member`	Removes a Cluster Member from a VSX Cluster. See *"vsx_util remove_member" on page 1927*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).
`vsx_util show_ interfaces`	Shows configuration of selected interfaces - interface types, connections to Virtual Devices, and IP addresses. See *"vsx_util show_interfaces" on page 1928*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).
`vsx_util upgrade`	Upgrades the version of a VSX Gateway or VSX Cluster in the management database. See *"vsx_util upgrade" on page 1932*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).
`vsx_util view_vs_conf`	Shows configuration of a Virtual Device on the Management Server versus the VSX Gateway or VSX Cluster. See *"vsx_util view_vs_conf" on page 1933*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).

Sub-command	Description
`vsx_util vsls`	Shows the configuration menu for Virtual System Load Sharing - see status, redistribute, export and import configuration. See *"vsx_util vsls" on page 1937*. You run this command from the Expert mode on the Management Server (Security Management Server, or a *Main*Domain Management Server on Multi-Domain Server).

Notes

- This command writes its messages to the `vsx_util_YYYYMMDD_HH_MM.log` file on the Management Server:
  - On a Security Management Server:

    ```
    $FWDIR/log/vsx_util_YYYYMMDD_HH_MM.log
    ```

  - On a Multi-Domain Server - if executed the command in the MDS context:

    ```
    /opt/CPsuite-R81.20/fw1/log/vsx_util_YYYYMMDD_HH_MM.log
    ```

  - On a Multi-Domain Server - if executed the command in the context of a Domain Management Server:

    ```
    /opt/CPmds-R81.20/customers/<Name of Domain Management
    Server>/CPsuite-R81.20/fw1/log/vsx_util_YYYYMMDD_HH_
    MM.log
    ```

- If it is necessary to exit from the `vsx_util` command's menu, press the **CTRL C** keys.

  Important - Do **not** press these keys, it this command already started to perform a change. If you press these keys during the operation, the command does not save its log file.

vsx_util add_member

Description

Adds a new Cluster Member to a VSX Cluster and pushes the VSX Cluster configuration to the new VSX Cluster Member.

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util add_member
```

Required Input

- The applicable VSX Cluster object.
- Name of the new VSX Cluster Member.
- IP address for the management interface.
- IP address for the synchronization interface.
- The one-time Activation Key (SIC activation key)

Comments

- Execute the command and follow the instructions on the screen.
- After the command adds a new Cluster Member to the management database, the command prompts you to reconfigure the new VSX Cluster Member (to push the VSX Cluster configuration to it).
  - If you enter "**y**" to reconfigure the new VSX Cluster Member at this time, then the *"vsx_util reconfigure" on page 1921* operation starts automatically on the new VSX Cluster Member.

    Important - You must reboot the new VSX Cluster Member after the reconfigure operation finishes.
  - If you enter "**n**" to cancel the reconfigure operation on the new VSX Cluster Member at this time, then later you must manually run the *"vsx_util reconfigure" on page 1921* command for the new VSX Cluster Member.

vsx_util change_interfaces

Description

Automatically replaces designated existing interfaces with new interfaces on all Virtual Devices, to which the existing interfaces connect.

This command is useful when converting a deployment to use Link Aggregation, especially where VLANs connect to many Virtual Devices.

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util change_interfaces
```

Required Input

- The applicable VSX Gateway or VSX Cluster object.
- Where to apply the change (Management Server only, or Management Server and VSX Gateway / VSX Cluster Members).
- Name of the interface to be replaced.
- Name of the new (replacement) interface.

Comments

- Execute the command and follow the instructions on the screen.
- This command supports the resume feature.
- You can use this command to migrate a VSX deployment from an Open Server to a Check Point appliance by using the **Management Only** mode.
- Refer to the **Notes** section below for additional information.

Procedure

Step	Instructions
1	Close all SmartConsole clients that are connected to the Security Management Server or Domain Management Servers.
2	Connect to the command line on the Management Server.
3	Log in to the Expert mode.
4	On Multi-Domain Server, go to the context of the *Main* Domain Management Server that manages the applicable VSX Gateway (VSX Cluster) object: `mdsenv <IP address or Name of Domain Management Server>`
5	Run: `vsx_util change_interfaces`
6	Enter the IP address of the Security Management Server or Main Domain Management Server.
7	Enter the Management Server administrator username and password.
8	Select the VSX Gateway (VSX Cluster) object.
9	When prompted, select one of the following options: ■ **Apply changes to the management database and to the VSX Gateway/Cluster members immediately** Changes the interface on the Management Server and on the VSX Gateway (each VSX Cluster Member). ■ **Apply changes to the management database only** Changes the interface on the Management Server only. You must run the *"vsx_util reconfigure" on page 1921* command to push the updated VSX configuration to VSX Gateways (each VSX Cluster Member).
10	Select the interface to be replaced.

Step	Instructions
11	Select the new (replacement) interface. a. You can optionally add a new interface, if you select the **A new interface name** option. This interface must physically exist on the VSX Gateway (all VSX Cluster Members). Otherwise, the operation fails. b. At the prompt, enter the new interface name. If the new interface is a Bond interface, the interface name must match the name of the configured Bond interface exactly.
12	The command prompts you: `Would you like to change another interface? (y|n) [n]:` ■ To replace additional interfaces, enter **y**. ■ To complete the process, enter **n**.
13	If you selected the option **Apply changes to the management database only**, you can remove the old (replaced) interfaces from the management database. When prompted, enter **y**: `Would you like to remove the old interfaces from the database? (y|n) [n]: y`
14	Reboot the VSX Gateway (all VSX Cluster Members).

Notes

- The option "**Apply changes to the management database and to the VSX Gateway/Cluster members immediately**" verifies connectivity between the Management Server and the VSX Gateway or VSX Cluster Members. In the event of a connectivity failure one of the following actions occur:

  1. If **all** of the newly changed interfaces fail to establish connectivity, the process terminates unsuccessfully.
  2. If one or more interfaces successfully establish connectivity, while one or more other interfaces fail, you may optionally continue the process.

     In this case, those interfaces for which connectivity was established successfully will be changed.

     For those interfaces that failed, you must then resolve the issue and then run the *"vsx_util reconfigure" on page 1921* command to complete the process.

- If you select the option "**Apply changes to the management database only**", you can select one of these:

  - Another interface from list (if any are available).
  - Option to add a new interface.

vsx_util change_mgmt_ip

Description

Changes the VSX Management IP address of a VSX Gateway or VSX Cluster Member.

This command changes the Management IP address within the same subnet.

For more information, see sk92425.

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util change_mgmt_ip
```

Required Input

- The applicable VSX Cluster object.
- The applicable VSX Cluster Member object.
- New management IP address.

Comments

- Execute the command and follow the instructions on the screen.

vsx_util change_mgmt_subnet

Description

Changes the VSX Management IP address of a VSX Gateway or VSX Cluster Member.

This command changes the Management IP address from the current subnet to a different subnet.

For more information, see sk92425.

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util change_mgmt_subnet
```

Required Input

- The applicable VSX Gateway or VSX Cluster object.
- New management IPv4 address.
- New management IPv4 netmask.
- New management IPv6 address.
- New management IPv6 prefix.
- New IPv4 default gateway.
- New IPv6 default gateway.

Comments

- Execute the command and follow the instructions on the screen.
- This command updated only routes that were automatically generate.

  You must remove and/or change all manually created routes that use the previous management subnet.
- You must reboot the VSX Gateway (all VSX Cluster Members) after the command finishes.

vsx_util change_private_net

Description

Changes the IP address of the Internal Communication Network in a VSX Cluster (cluster private network).

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util change_private_net
```

Required Input

- The applicable VSX Cluster object.
- New IPv4 address for the cluster private network.
- New IPv4 netmask for the cluster private network.
- New IPv6 address and prefix for the cluster private network.

Comments

- Run the command and follow the instructions on the screen.
- The IP address of the Internal Communication Network must be unique.

  This IP address must **not** be used anywhere in your environment, including the Virtual Devices on this VSX Cluster.
- The illegal IPv4 addresses are: `0.0.0.0`, `127.0.0.0`, and `255.255.255.255`
- For IPv4 address, the network mask must be one of these:
  - `255.255.0.0`, or `/16`
  - `255.255.128.0`, or `/17`
  - `255.255.192.0`, or `/18`
  - `255.255.224.0`, or `/19`
  - `255.255.240.0`, or `/20`
  - `255.255.248.0`, or `/21`
  - `255.255.252.0`, or `/22` (this is the default)
- For IPv6 address, the new prefix must be `/80`.

vsx_util convert_cluster

Description

Converts the VSX Cluster mode between High Availability (default) and Virtual System Load Sharing.

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Important:

- The only mode available for a VSX Cluster that was installed as R81.10 and higher is **Virtual System Load Sharing (VSLS)**.
- The **High Availability** mode is available only if you upgrade a VSX Cluster from R81 or lower to R81.20.
  You can also convert a VSLS cluster to the High Availability mode (see the *R81.20 VSX Administration Guide* > section "Changing the VSX Cluster Type").
- It is not supported to run the `vsx_util convert_cluster` command to convert a VSX Cluster from the High Availability mode to the VSLS mode when the VSX Cluster contains a Virtual Switch that is not assigned to any physical interface or to a VLAN interface.

Syntax

```
vsx_util convert_cluster
```

Required Input

- The applicable VSX Cluster object.
- The ClusterXL mode (case sensitive).

Comments

- Execute the command and follow the instructions on the screen.
- When you convert from Virtual System Load Sharing to High Availability:

- All Virtual Systems are **Active** on the same VSX Cluster Member by default.
- Peer Virtual Systems are **Standby** on other VSX Cluster Members.

vsx_util downgrade

Description

Downgrades the version of a VSX Gateway or VSX Cluster in the management database.

Important - You can use this command only if you did **not** make any configuration changes after you used the "`vsx_util upgrade`" command.

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util downgrade
```

Required Input

- The applicable VSX Gateway or VSX Cluster object.
- The applicable Check Point version.

Comments

- Used only to revert the upgraded VSX Gateway or VSX Cluster object.
- Execute the command and follow the instructions on the screen.
- To deploy the version change to the VSX Cluster Members, you must run the *"vsx_util reconfigure" on page 1921* command.

vsx_util reconfigure

Description

Restores VSX configuration on a VSX Gateway or VSX Cluster Member (for example, after you perform clean install after a system failure).

Syntax

```
vsx_util reconfigure
```

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Important - Before you run this command on the Management Server, you must configure specific settings on the cleanly installed VSX Gateway or VSX Cluster Member as they were:

- IP address of Gaia management interface
- Enable IPv6 support in Gaia
- Configure the applicable interfaces (Bond, VLAN, and so on)
- Configure kernel parameters and their values:
  - `$FWDIR/boot/modules/fwkern.conf`
  - `$PPKDIR/conf/simkern.conf`
- Configure CoreXL:
  - Number of CoreXL Firewall instances (for IPv4 and IPv6) in the context of VS0 (run the `cpconfig` command and select the option **Check Point CoreXL**)
  - `$FWDIR/conf/fwaffinity.conf`

Required Input

- The applicable VSX Gateway or VSX Cluster object.
- The one-time Activation Key (SIC activation key).

Comments

- Execute the command and follow the instructions on the screen.
- The new VSX Gateway or VSX Cluster Member:
  - Must be a *new* installation.

    You cannot use a VSX Gateway or VSX Cluster Member with a previous VSX configuration.
  - Must have the same hardware specifications as the original.

    Most importantly, it must have *at least* the same number of interfaces.
  - Must have the same Gaia OS configuration as the original.

    Most importantly, it must have the same VSX Management IP address.

Limitations

The reconfigure process does **not** restore the local configuration that was performed on VSX Gateway or VSX Cluster Member itself (because this configuration is not stored on the Management Server).

Important - After the reconfigure process is complete and you rebooted VSX Gateway or VSX Cluster Member, you must manually configure these settings from scratch or from backed up files.

These settings and files are **not** restored during the reconfigure process and you must manually configure them again:

- Per Virtual System State - run the "`cpconfig`" command and examine the option "`Per Virtual System State`". The title of this option must be the same on each VSX Cluster Member - either "`Enable Check Point Per Virtual System State`" or "`Disable Check Point Per Virtual System State`". To change this configuration, enter the number of this option and follow the instructions on the screen.

  Note - Do not change the value of the kernel parameter "`fwha_enable_state_machine_by_vs`" in the `$FWDIR/boot/modules/fwkern.conf` file. The VSX Cluster changes this value automatically.

- Any OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on).
- Backup files and Gaia snapshots saved in the past on the VSX Gateway or VSX Cluster Member.
- Any settings manually defined in various configuration files on the VSX Gateway or VSX Cluster Member.
- Any Check Point configuration files.

  Note - Some of these files do not exist by default. Some files are configured on each VSX Gateway and VSX Cluster Member, and some files are configured for each Virtual System.

  List of the most important files

  Note - Some of these files do not exist by default. Some files are configured on each VSX Gateway and VSX Cluster Member, and some files are configured in the context of each Virtual System.

  This list is sorted alphabetically.

  - `$CVPNDIR/conf/cvpnd.C`
  - `$FWDIR/boot/modules/fwkern.conf`
  - `$FWDIR/conf/cpha_bond_ls_config.conf`

- `$FWDIR/conf/cpha_specific_vlan_data.conf` (see sk92784)
- `$FWDIR/conf/discntd.if`
- `$FWDIR/conf/fw_fast_accel_export_configuration.conf` (see sk156672)
- `$FWDIR/conf/fwaffinity.conf`
- `$FWDIR/conf/fwauthd.conf`
- `$FWDIR/conf/hsm_configuration.C`
- `$FWDIR/conf/identity_broker.C`
- `$FWDIR/conf/ipassignment.conf`
- `$FWDIR/conf/local.arp` (see sk30197)
- `$FWDIR/conf/malware_config`
- `$FWDIR/conf/prioq.conf` (see sk105762)
- `$FWDIR/conf/rad_conf.C`
- `$FWDIR/conf/synatk.conf`
- `$FWDIR/conf/te.conf`
- `$FWDIR/conf/thresholds.conf`
- `$FWDIR/conf/trac_client_1.ttm`
- `$FWDIR/conf/vsaffinity_exception.conf`
- `$PPKDIR/conf/simkern.conf`
- `/var/ace/sdconf.rec`
- `/var/ace/sdopts.rec`
- `/var/ace/sdstatus.12`
- `/var/ace/securid`

Example

This example shows how the VSX configuration is restored on a VSX Cluster Member.

```
[Expert@MDS:0]# vsx_util reconfigure

************************************************************************************
* Note: the operation you are about to perform changes the information in the management *
* database. Back up the database before continuing.                                  *
************************************************************************************

Enter Security Management Server/main Domain Management Server IP address (Hit 'ENTER' for
'localhost'): 192.168.3.240
Enter Administrator Name: ******
Enter Administrator Password: ******
Select VSX gateway/cluster object name:
  1)    VSX_Cluster
Select: 1


Select VSX member name to reconfigure:
  1)    VSX1_192.168.3.241
  2)    VSX2_192.168.3.242
Select: 1
You are about to perform reconfigure on VSX gateway/cluster, please read sk97552.
Are you sure you want to continue [y/n]? y
Enter Activation Key:
Retype Activation Key:


 1/10 : Certificate Revocation              [########################################] 100%
00:00:01
 2/10 : Certificate Replacement             [########################################] 100%
00:00:06
 3/10 : Connectivity Check                  [########################################] 100%
00:00:05
 4/10 : Fetching Configuration              [########################################] 100%
00:00:02
 5/10 : Verifying Configuration             [########################################] 100%
00:00:00
 6/10 : Installing policy on: VSX_Cluster   [########################################] 100%
00:00:21
 7/10 : Converting Gateway to VSX           [########################################] 100%
00:02:13
 8/10 : Generating Activation Keys          [########################################] 100%
00:00:00
 9/10 : Reconfiguring                       [########################################] 100%
00:00:03
10/10 : Pushing Configuration               [########################################] 100%
00:00:44

Database saved successfully.
```

```
====================== SUMMARY ======================
---- Reconfigure gateway operation completed successfully

************************************************************
IMPORTANT:
   When you are managing a VSX cluster,
   make sure that the new reconfigured member has the same number of
   IPv4, and IPv6 firewall instances as the other VSX cluster members.
   Run cpconfig command to show and edit CoreXL settings.
NOTE:
   In case of adding a new cluster member to a VSX Cluster,
   while using 'ClusterXL Virtual System Load Sharing'
   make sure to run 'vsx_util vsls' after rebooting the
   gateway in order for the Virtual Systems to become active
   on the newly added VSX cluster member.

IMPORTANT: Please reboot the gateway

************************************************************

Logging details are available at /opt/CPmds-R81.20/customers/MyDomain_Server/CPsuite-
R81.20/fw1/log/vsx_util_20190917_13_16.log

[Expert@MDS:0]#
```

vsx_util remove_member

Description

Removes a Cluster Member from a VSX Cluster.

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util remove_member
```

Required Input

- The applicable VSX Cluster object.
- The applicable VSX Cluster Member object.

Comments

- Before you run this command:
  - Make sure to remove (detach) the license from the VSX Cluster Member.
  - Make sure to run the *"cphastop" on page 1379* command to avoid unexpected failover from the VSX Cluster Member.
  - Make sure to disconnect the VSX Cluster Member from all networks, except from the Management Server.
- Execute the command and follow the instructions on the screen.

vsx_util show_interfaces

Description

Shows configuration of selected interfaces - interface types, connections to Virtual Devices, and IP addresses.

The command shows the information on the screen and also saves it to the `interfacesconfig.csv` file in the current working directory.

Important - On a Multi-Domain Security Management Server, you must switch to the context of the **Main**Domain Management Server that manages the VSX Gateway / VSX Cluster object.
Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util show_interfaces
```

Required Input

- The applicable VSX Gateway or VSX Cluster object.
- Which interfaces to show:

Menu Option	Description
1) All Interfaces	Shows all interfaces (Physical and Warp).
2) All Physical Interfaces	Shows only Physical interfaces.
3) All Warp Interfaces	Shows only Warp interfaces.
4) A Specific Interface	Prompts you to enter the name of the specific interface to show. **Note** - You cannot specify a VLAN tag as a parameter. You can, however, specify an interface used as a VLAN (without the tag) to see all VLAN tags associated with that interface. See the example below.

Example

```
[Expert@MGMT:0]# vsx_util show_interfaces
Enter Security Management Server/main Domain Management Server IP address (Hit 'ENTER' for
'localhost'): 172.16.16.240
Enter Administrator Name: admin
Enter Administrator Password:

Select VSX gateway/cluster object name:
  1)    VSX_Cluster_1
  2)    VSX_Cluster_2
  3)    VSX_GW_1
  4)    VSX_GW_2
Select: 1

Which interface would you like to display?
  1)    All Interfaces
  2)    All Physical Interfaces
  3)    All Warp Interfaces
  4)    A Specific Interface
Enter your choice: 1

+-------------------+---------------------+----+-----------------------------------------------
--+
| Type & Interface  | Virtual Device Name |VSID| IP / Mask length
 |
+-------------------+---------------------+----+-----------------------------------------------
--+
|M eth0             |VSX_Cluster_1        |0   |v4 172.16.16.98/24 v6 2001:0DB8::98/64
 |
+-------------------+---------------------+----+-----------------------------------------------
--+
|S eth1             |VSX_Cluster_1        |0   |v4 10.0.0.0/24
 |
+-------------------+---------------------+----+-----------------------------------------------
--+
|U eth2             |VS1                  |1   |v4 192.0.2.2/24 v6 2001:0DB8:c::1/64
 |
+-------------------+---------------------+----+-----------------------------------------------
--+
|U eth3             |VS1                  |1   |v4 192.168.3.3/24 v6 2001:0DB8:b::1/64
 |
+-------------------+---------------------+----+-----------------------------------------------
--+
|A eth4             |                     |    |
 |
+-------------------+---------------------+----+-----------------------------------------------
--+
|U eth5             |VS2                  |2   |v4 10.10.10.10/24 v6 2001:0DB8:a::1/64
 |
+-------------------+---------------------+----+-----------------------------------------------
--+
|A eth6             |                     |    |
 |
+-------------------+---------------------+----+-----------------------------------------------
--+

#Type: M - Management Interface    S - Synchronization Interface
#      V - VLAN Interface          W - Warp Interface
#      U - Used Interface          A - Available Interface
#      X - Unknown Interface       E - Error in Interface Properties

Logging details are available at /opt/CPsuite-R81.20/fw1/log/vsx_util_20210625_17_45.log

[Expert@MGMT:0]#
[Expert@MGMT:0]# cat interfacesconfig.csv
 Interface Name , Type ,Virtual Device Name , VSID , IPv4 Address , IPv4 mask length, IPv6 Address,
IPv6 mask length
```

```
eth0,M,VSX_Cluster_1,0,172.16.16.98,24,2001:0DB8::98,64
eth1,S,VSX_Cluster_1,0,10.0.0.0,24,,
eth2,U,VS1,192.0.2.2,24,2001:0DB8:c::1,64
eth3,U,VS1,192.168.3.3,24,2001:0DB8:b::1,64
eth4,A
eth5,U,VS2,10.10.10.10,24,2001:0DB8:a::1,64
eth6,A

#Type: M - Management Interface    S - Synchronization Interface
#      V - VLAN Interface          W - Warp Interface
#      U - Used Interface          A - Available Interface
#      X - Unknown Interface       E - Error in Interface Properties

[Expert@MGMT:0]#
```

vsx_util upgrade

Description

Upgrades the version of a VSX Gateway or VSX Cluster in the management database.

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util upgrade
```

Required Input

- The applicable VSX Gateway or VSX Cluster object.
- The applicable Check Point version.

Comments

- Execute the command and follow the instructions on the screen.
- After the command finishes, you must run the *"vsx_util reconfigure" on page 1921* command.
- To revert this upgrade, run the *"vsx_util downgrade" on page 1920* command.

vsx_util view_vs_conf

Description

Compares the configuration of all Virtual Devices on the Management Server and the actual configuration on the VSX Gateway or VSX Cluster Members.

Important - On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Syntax

```
vsx_util view_vs_conf
```

Required Input

- The applicable VSX Gateway or VSX Cluster object.
- The applicable Virtual Device object.

Example

```
[Expert@MGMT:0]# vsx_util view_vs_conf
Enter Security Management Server/main Domain Management Server IP address (Hit 'ENTER' for
'localhost'): 172.16.16.240
Enter Administrator Name: admin
Enter Administrator Password:

Select VSX gateway/cluster object name:
  1)    VSX_Cluster_1
  2)    VSX_Cluster_2
  3)    VSX_GW
  4)    VSX_GW_2
Select: 1

Select Virtual Device object name:
  1)    VS1
  2)    VS2
  3)    VS3
  4)    VSX_Cluster
Select: 1

Type: Virtual System

Interfaces configuration table:

+-------------------------------------------------+-----+-------------------+
|Interfaces                                       |Mgmt |VSX GW(s)          |
+----------+--------------------------------------+-----+---------+---------+
|Name      |IP / Mask length                      |     |mem 1    |mem2     |
+----------+--------------------------------------+-----+---------+---------+
|eth2      |v4 10.0.0.0/24 v6 2001:db8::abc::1/64   |  V  |    V    |    V    |
|eth3      |v4 10.10.10.10/24 v6 2001:db8::3121/64  |  V  |    V    |    V    |
+----------+--------------------------------------+-----+---------+---------+


Interfaces Table Legend:

  V   - Interface exists on the gateway and matches management information (if defined on the
management).
  -   - Interface does not exist on the gateway.
 N/A  - Fetching Virtual Device configuration from the gateway failed.
 !IP  - Interface exists on the gateway, but there is an IP address mismatch.
!MASK - Interface exists on the gateway, but there is a Net Mask mismatch.


Routing table:

+-----------------------------------------------------------+-----+-------------+
|Ipv4 Routes                                                |Mgmt |VSX GW(s)    |
+--------------------------+--------------------+-----------+-----+------+------+
|Destination / Mask Length |Gateway             |Interface  |     |mem1  |mem2  |
+--------------------------+--------------------+-----------+-----+------+------+
|2.2.2.0/24                |                    |eth2       |  V  |  V   |  V   |
|3.3.3.0/24                |                    |eth3       |  V  |  V   |  V   |
+--------------------------+--------------------+-----------+-----+------+------+
+--------------------------+--------------------+-----------+-----+------+------+


+-----------------------------------------------------------+-----+-------------+
|Ipv6 Routes                                                |Mgmt |VSX GW(s)    |
+--------------------------+--------------------+-----------+-----+------+------+
|Destination / Mask Length |Gateway             |Interface  |     |mem1  |mem2  |
+--------------------------+--------------------+-----------+-----+------+------+
|2001:db8::abc::/64        |                    |eth2       |  V  | !NH  | !NH  |
|2001:db8:0a::/64          |                    |eth3       |  V  | !NH  | !NH  |
+--------------------------+--------------------+-----------+-----+------+------+
|2001:db8::1ffe:0:0:0/112  |                    |eth2       |  -  |  V   |  V   |
```

```
|2001:db8::fd9a:0:1:0/112  |                    |eth3      |  -  |  V   |  V   |
+--------------------------+--------------------+----------+-----+------+------+


Routing Table Legend:

  V   - Route exists on the gateway and matches management information (if defined on the
management).
  -   - Route does not exist on the gateway.
 N/A  - Fetching Virtual Device configuration from the gateway failed.
 !NH  - Route exists on the gateway, but there is a Next Hop mismatch.

Note: Routes can be created automatically on the gateways by the Operating System.
Therefore, routes that appear on all gateways, but are not defined on the management,
do not necessarily indicate a problem.

Logging details are available at /opt/CPsuite-R81.20/fw1/log/vsx_util_20210625_18_11.log

[Expert@MGMT:0]#
```

vsx_util vsls

Description

Shows the configuration menu for Virtual System Load Sharing - status, redistribute, export, and import of configuration.

Important - *Before* you run the `vsx_util` commands:

- Back up the VSX environment. See sk100395: How to backup and restore VSX gateway.
- You must close all SmartConsole clients. Failure to do so may result in a database lock error.
- On a Multi-Domain Security Management Server, you must switch to the context of the **Main** Domain Management Server that manages the VSX Gateway / VSX Cluster object.
  Use the command "`mdsenv <IP Address or Name of Domain Management Server>`".

Important:

- The only mode available for a VSX Cluster that was installed as R81.10 and higher is **Virtual System Load Sharing (VSLS)**.
- The **High Availability** mode is available only if you upgrade a VSX Cluster from R81 or lower to R81.20.
  You can also convert a VSLS cluster to the High Availability mode (see the *R81.20 VSX Administration Guide* > section "Changing the VSX Cluster Type").

Syntax

```
vsx_util vsls
```

Required Input

- The applicable VSX Cluster object.
- The applicable redistribution option.

Comments

- Execute the command and follow the instructions on the screen.
- If the command output shows "`Operation not allowed. Object is not a Virtual System Load Sharing cluster.`", then run the *"vsx_util convert_cluster" on page 1918* command.

Example

```
[Expert@MGMT:0]# vsx_util vsls
Enter Security Management Server/main Domain Management Server IP address (Hit 'ENTER' for
'localhost'): 172.16.16.240
Enter Administrator Name: admin
Enter Administrator Password:

Select VSX gateway/cluster object name:
  1)    VSX_Cluster_1
  2)    VSX_Cluster_2
  3)    VSX_GW_1
  4)    VSX_GW_2
Select: 1


VS Load Sharing - Menu
__________________________________
1. Display current VS Load sharing configuration
2. Distribute all Virtual Systems so that each cluster member is equally loaded
3. Set all VSes active on one member
4. Manually set priority and weight
5. Toggle VSLS mode between Active Up and Primary Up
6. Import configuration from a file
7. Export configuration to a file
8. Exit

Enter redistribution option (1-8) [1]:
```

vsx_provisioning_tool

This section describes the **VSX Provisioning Tool** (the `vsx_provisioning_tool` command).

Description

This tool allows the VSX administrator to add and remove Virtual Devices (Virtual Systems, Virtual Routers, Virtual Switches), interfaces and routes from the command line of a Security Management Server or Domain Management Server.

This allows the automation of the required VSX Provisioning operations in the environment.

Syntax

```
vsx_provisioning_tool -h
```

```
vsx_provisioning_tool [-s <Mgmt Server>] {-u <Username> | -c
<Certificate>} -p <Password>
      -o <Commands> [-a] -L
      -f <Input File> [-l <Line>] [-a] -L
```

Parameters

Parameter	Description
`-h`	Shows the built-in usage.
`-s <Mgmt Server>`	Specifies the Security Management Server or the applicable Domain Management Server. Enter the IPv4 or IPv6 address, or the resolvable hostname name. This parameter is mandatory when you run the tool: ■ From a SmartConsole computer ■ On a Multi-Domain Server.
`-u <Username>`	Specifies the Management Server administrator's user name.
`-c <Certificate>`	Specifies the path and the name for the Management Server administrator's certificate file.

Parameter	Description
`-p <Password>`	Specifies the password of the: ■ Management Server administrator ■ Certificate file
`-o <Commands>`	Executes the commands you enter on the command line. See *"vsx_provisioning_tool Commands" on page 1943*.
`-f <Input File>`	Specifies the path and the name for the file with the commands to execute. The tool treats all text begins with a hash sign (#) as a comment and ignores it. This way you can add comments on separate lines, or in-line. See: ■ *"Transactions" on page 1942* ■ *"vsx_provisioning_tool Commands" on page 1943*
`-l <Line>`	Specifies the line number in `<Input File>`, from which to start to execute the commands. You can use this "`-l`" parameter only together with the "`-f`" parameter.
`-a`	Specifies that before the tool executes the specified commands, it must make sure it can connect to all VSX Gateways. **Note** - This does not guarantee that a VSX Gateway can successfully apply all the specified commands.
`-L`	Specifies local authentication mode.

Exit Codes

Exit Code	Description
0	The tool successfully applied all changes, on all VSX Cluster Members.
1	The tool successfully applied all changes to the management database, but not to all VSX Cluster Members.
2	The tool successfully applied all changes, but SIC communication failed to establish with at least one VSX Cluster Member.
3	Connectivity test failed with at least one VSX Cluster Member (if you used the "`-a`" parameter). The tool did not apply changes to the management database, or to the VSX Cluster Member.
4	The tool failed to apply changes (due to internal error, syntax error, or another reason).

Note - If commands are executed from a file with multiple transactions, the exit code refers to the last transaction processed.

Example 1

Run the tool on the Security Management Server.

Execute the commands from the text `/var/log/vsx.txt` file.

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -f /var/log/vsx.txt
```

Example 2

Run the tool on the Multi-Domain Server in the context of the Domain Management Server called `MyDomain`.

Create a new Virtual System object called `VS1` on the VSX Cluster object called `VSXCluster1`

In the new Virtual System object, on the interface `eth4`, add a VLAN interface with VLAN ID 100 and IPv4 address 1.1.1.1/24.

```
mdsenv MyDomain
vsx_provisioning_tool -s localhost -u admin -p mypassword -o add vd name VS1 vsx VSXCluster1, add interface name eth4.100 ip 1.1.1.1/24
```

Transactions

Notes:

- A transaction is a set of operations performed on one Virtual Device.
- The utility commits all operations to the management database together when the transaction ends.
  If the transaction fails, the utility discards all its commands.
- You must specify the name of the Virtual Device with a parameter in the first command.
  You do not need to specify this name again in other commands of the same transaction.
- You cannot send operations to different Virtual Devices in one transaction.
- You cannot start a new transaction until you exit the one before.
- When you send commands with the "`-o`" parameter, you can enter multiple commands (for example: add a Virtual System and then add interfaces and routes to it).
  Separate the commands with a comma (`,`).
  All the commands are one transaction.
  The "`-o`" parameter does not support explicit transaction commands.
- When you send commands with the "`-f`" parameter, you can use explicit transaction commands (see *"vsx_provisioning_tool Commands" on page 1943*).
- Commands from a file can be one or more transactions:
  - If not inside a transaction, the current line is one transaction, which the utility automatically commits.
    You can write multiple commands in one line (as one transaction), separated with a comma (`,`).
  - If currently inside a transaction, the utility processes the lines, but does not take action until the transaction ends.

vsx_provisioning_tool Commands

All `vsx_provisioning_tool` commands are pairs of a key and a value.

The first two words in each command must appear in the correct order.

Other pairs can be written in any order.

Explicit Transaction Commands

Operation	Command Syntax
Begin a new transaction	`transaction begin`
End a transaction	`transaction end`
Cancel a transaction	`transaction cancel`

Note - SIC with the Virtual System is established automatically. If it fails, operations continue, and the transaction returns error code **2**.

Adding a VSX Gateway

Description

This command adds a new VSX Gateway object.

Syntax

```
add vsx type gateway name <Name of VSX Gateway Object> version
<Version> main_ip <Main IPv4 Address> [main_ip6 <Main IPv6
Address>] sic_otp <Activation Key> [rule_snmp {enable | disable}]
[rule_ssh {enable | disable}] [rule_ping {enable | disable} [rule_
ping6 {enable | disable}] [rule_https {enable | disable}] [rule_
drop {enable | disable}]
```

Note - In this transaction, you can only add the "`set physical interface`" command.

Parameters

`type`	`gateway`	You must use the value "`gateway`" to add a new VSX Gateway object.
`name <Name of VSX Gateway Object>`	Object name	Defines the name of the VSX Gatewayobject. You cannot use spaces of Check Point reserved words.
`version <Version>`	Check Point version	Defines the Check Point version of the VSX Gateway object. You must enter the exact version as appears in SmartConsole (case-sensitive).
`main_ip <Main IPv4 Address>`	IPv4 Address	Defines the main IPv4 Address of the VSX Gateway object.
`main_ip6 <Main IPv6 Address>`	IPv6 Address	Defines the main IPv6 Address of the VSX Gateway object.
`sic_otp <Activation Key>`	SIC password	You must enter the same Activation Key you entered during the First Time Configuration Wizard of the VSX Gateway.

`rule_snmp {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all SNMP packets sent to the VSX Gateway: ■ `enable` - Allows all SNMP packets ■ `disable` - Drops all SNMP packets (default)
`rule_ssh {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all SSH packets sent to the VSX Gateway: ■ `enable` - Allows all SSH packets ■ `disable` - Drops all SSH packets (default)
`rule_ping {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all ICMP Echo Request (ping) packets sent to the VSX Gateway: ■ `enable` - Allows all IPv4 ping packets ■ `disable` - Drops all IPv4 ping packets (default)
`rule_ping6 {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all ICMPv6 Echo Request (ping) packets sent to the VSX Gateway: ■ `enable` - Allows all IPv6 ping packets ■ `disable` - Drops all IPv6 ping packets (default)
`rule_https {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all HTTPS packets sent to the VSX Gateway: ■ `enable` - Allows all HTTPS packets ■ `disable` - Drops all HTTPS packets (default)
`rule_drop {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all packets (other than SNMP, SSH, ICMP, ICMPv6, HTTPS) sent to the VSX Gateway: ■ `enable` - Drops all other packets (default) ■ `disable` - Allows all other packets

Example

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o add vsx name VSX_GW1 type gateway main_ip 192.168.20.1 version R81.20 sic_
otp ABCDEFG rule_ssh enable rule_ping enable
```

Adding a VSX Cluster

Description

This command adds a new VSX Cluster object.

Syntax

```
add vsx type cluster name <Name of VSX Cluster Object> version
<Version> main_ip <Main Virtual IPv4 Address> main_ip6 <Main
Virtual IPv6 Address> cluster_type {vsls | ha | crbm} sync_if_name
<Name of Sync Interface> sync_netmask <Sync Interface Netmask>
[rule_snmp {enable | disable}] [rule_ssh {enable | disable}]
[rule_ping {enable | disable} [rule_ping6 {enable | disable}]
[rule_https {enable | disable}] [rule_drop {enable | disable}]
```

Important - You must run the "`add vsx_member`" command for each VSX Cluster Member in the same transaction as the "`add vsx type cluster name`" command.

Syntax

```
add vsx_member name <Member Name> [main_ip <Member Main
IPv4 Address>] [main_ip6 <Member Main IPv6 Address>] sync_
ip <Sync Interface IPv4 Address> sic_otp <SIC Password>
```

Parameters

Parameter	Value	Notes
`type`	`cluster`	You must use the value "`cluster`" to add a new VSX Cluster object.
`name <Name of VSX Cluster Object>`	Object name	Defines the name of the VSX Cluster object. You cannot use spaces of Check Point reserved words.
`version <Version>`	Check Point version	Defines the Check Point version of the VSX Cluster object. You must enter the exact version as appears in SmartConsole (case-sensitive).
`main_ip <Main Virtual IPv4 Address>`	IPv4 Address	Defines the main IPv4 Virtual Address of the VSX Cluster object.

Parameter	Value	Notes
`main_ip6 <Main Virtual IPv6 Address>`	IPv6 Address	Defines the main IPv6 Virtual Address of the VSX Cluster object.
`cluster_type {vsls | ha | crbm}`	Cluster type	Defines the cluster type. Enter one of these: ■ `vsls` - Virtual System Load Sharing mode ■ `ha` - High Availability mode ■ `crbm` - X-Series appliances (former BlueCoat / Crossbeam)
`sync_if_name <Name of Sync Interface>`	Sync interface name	Defines the name of the Cluster Synchronization interface.
`sync_netmask <Sync Interface Netmask>`	IPv4 Network mask	Defines an IPv4 Netmask for the Cluster Synchronization interface (in a dot-quad format X.X.X.X).
`rule_snmp {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all SNMP packets sent to the VSX Cluster Members: ■ `enable` - Allows all SNMP packets ■ `disable` - Drops all SNMP packets (default)
`rule_ssh {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all SSH packets sent to the VSX Cluster Members: ■ `enable` - Allows all SSH packets ■ `disable` - Drops all SSH packets (default)
`rule_ping {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all ICMP Echo Request (ping) packets sent to the VSX Cluster Members: ■ `enable` - Allows all IPv4 ping packets ■ `disable` - Drops all IPv4 ping packets (default)

Parameter	Value	Notes
`rule_ping6 {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all ICMPv6 Echo Request (ping) packets sent to the VSX Cluster Members: ■ `enable` - Allows all IPv6 ping packets ■ `disable` - Drops all IPv6 ping packets (default)
`rule_https {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all HTTPS packets sent to the VSX Cluster Members: ■ `enable` - Allows all HTTPS packets ■ `disable` - Drops all HTTPS packets (default)
`rule_drop {enable | disable}`	■ `enable` ■ `disable`	Controls how to process all packets (other than SNMP, SSH, ICMP, ICMPv6, HTTPS) sent to the VSX Cluster Members: ■ `enable` - Drops all other packets (default) ■ `disable` - Allows all other packets

Example

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o add vsx name VSX1 type cluster cluster_type vsls main_ip 192.168.1.1 version
R81.20 sync_if_name eth3 sync_netmask 255.255.255.0 rule_ssh enable rule_ping enable
```

Adding a Virtual Device

Description

This command adds a new Virtual Device object:

- Virtual System
- Virtual System in Bridge Mode
- Virtual Switch
- Virtual Router

Syntax

```
add vd name <Name of Virtual Device Object> vsx <Name of VSX
Gateway or VSX Cluster Object > [type {vs | vsbm | vsw | vr}] [vs_
mtu <MTU>] [instances <Number of IPv4 CoreXL Firewall instances>]
[instances6 <Number of IPv6 CoreXL Firewall instances>] [main_ip
<Main IPv4 Address>] [main_ip6 <Main IPv6 Address>] [calc_topo_
auto {true | false}]
```

Parameters

Parameter	Value	Notes
`name <Name of Virtual Device Object>`	Object name	Defines the name of the Virtual Device object. Mandatory parameter, if this is the first command in a transaction.
`vsx <Name of VSX Gateway or VSX Cluster Object >`	Parent object name	Defines the name of the applicable VSX Gateway or VSX Cluster object, in which you create this Virtual Device. You cannot use spaces or Check Point reserved words. Mandatory parameter.
`type {vs | vsbm | vsw | vr}`	Type of Virtual Device	Defines the type of the Virtual Device: ■ `vs` - Virtual System (default) ■ `vsbm` - Virtual System in Bridge Mode ■ `vsw` - Virtual Switch ■ `vr` - Virtual Router

Parameter	Value	Notes
`vs_mtu <MTU>`	Integer	Defines the Global MTU value for all interfaces. This parameter is applicable only for a: ■ Virtual System in Bridge Mode (`type vsbm`) ■ Virtual Switch (`type vsw`) Default is 1500 bytes. **Note** - For a Virtual Switch, if you do not add a VLAN or physical interface in the same transaction, the utility ignores this value.
`instances <Number of IPv4 CoreXL Firewall instances>`	Integer	Defines the number of IPv4 CoreXL Firewall instances. This parameter is applicable only for a: ■ Virtual System (`type vs`) ■ Virtual System in Bridge Mode (`type vsbm`) Default is 1. For more information about CoreXL, see *R81.20 Performance Tuning Administration Guide*.
`instances6 <Number of IPv6 CoreXL Firewall instances>`	Integer	Defines the number of IPv6 CoreXL Firewall instances. This parameter is applicable only for a: ■ Virtual System (`type vs`) ■ Virtual System in Bridge Mode (`type vsbm`) Default is 1. For more information about CoreXL, see *R81.20 Performance Tuning Administration Guide*.

Parameter	Value	Notes
`main_ip <Main IPv4 Address>`	IPv4 Address	Defines the main IPv4 Address of the Virtual Device object. This parameter is applicable only for a: ■ Virtual System (`type vs`) ■ Virtual Router (`type vr`) **Note** - If you do not specify this value explicitly, the utility uses the IPv4 address of the first interface added to the new device.
`main_ip6 <Main IPv6 Address>`	IPv6 Address	Defines the main IPv6 Address of the Virtual Device object. This parameter is applicable only for a: ■ Virtual System (`type vs`) ■ Virtual Router (`type vr`) **Note** - If you do not specify this value explicitly, the utility uses the IPv6 address of the first interface added to the new device.
`calc_topo_auto {true | false}`	■ `true` ■ `false`	Defines how to calculate topology based on routes: ■ `true` - Automatically calculate topology based on routes (default) ■ `false` - Does not calculate topology based on routes (administrator can configure it manually) This parameter is applicable only for a: ■ Virtual System (`type vs`) ■ Virtual Router (`type vr`)

Example - Adding a Virtual Switch "VirtSwitch1" to the VSX Gateway "VSX_GW1"

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o add vd name VirtSwitch1 vsx VSX_GW1 type vsw
```

Deleting a Virtual Device

Description

This command deletes a Virtual Device object:

- Virtual System
- Virtual System in Bridge Mode
- Virtual Switch
- Virtual Router

You cannot delete a Virtual Device if:

- It is referenced by a policy rule.
- It is referenced by other objects.
- It is enabled for global use in a Multi-Domain Security Management environment.

Important - After you delete a Virtual Device, you cannot have more commands in the same transaction.

Syntax

```
remove vd name <Name of Virtual Device Object>
```

Parameters

Parameter	Value	Notes
`name <Name of Virtual Device Object>`	Object name	Specifies the name of the Virtual Device object. Mandatory parameter, if this is the first command in a transaction.

Example

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o remove vd name VirtSwitch1
```

Modifying Settings of a Virtual Device

Description

This command changes the settings of an existing Virtual Device object:

- Virtual System
- Virtual System in Bridge Mode
- Virtual Switch
- Virtual Router

Syntax

```
set vd name <Name of Virtual Device Object> [vs_mtu <MTU>]
[instances <Number of IPv4 CoreXL Firewall instances>] [instances6
<Number of IPv6 CoreXL Firewall instances>] [main_ip <Main IPv4
Address>] [main_ip6 <Main IPv6 Address>] [calc_topo_auto {true |
false}]
```

Parameters

Parameter	Value	Notes
`name <Name of Virtual Device Object>`	Object name	Specifies the name of the Virtual Device object. Mandatory parameter, if this is the first command in a transaction.
`vs_mtu <MTU>`	Integer	Specifies the Global MTU value for all interfaces. This parameter is applicable only for a: ▪ Virtual System in Bridge Mode ▪ Virtual Switch Default is 1500 bytes.

Parameter	Value	Notes
`instances <Number of IPv4 CoreXL Firewall instances>`	Integer	Specifies the number of IPv4 CoreXL Firewall instances. This parameter is applicable only for a: ■ Virtual System ■ Virtual System in Bridge Mode Default is 1. For more information about CoreXL, see *R81.20 Performance Tuning Administration Guide*.
`instances6 <Number of IPv6 CoreXL Firewall instances>`	Integer	Specifies the number of IPv6 CoreXL Firewall instances. This parameter is applicable only for a: ■ Virtual System ■ Virtual System in Bridge Mode Default is 1. For more information about CoreXL, see *R81.20 Performance Tuning Administration Guide*.
`main_ip <Main IPv4 Address>`	IPv4 Address	Specifies the main IPv4 Address of the Virtual Device object. This parameter is applicable only for a: ■ Virtual System ■ Virtual Router **Note** - To remove the current IPv4 address, set the value to "`empty`". For example: `set vd name VS1 main_ip empty`
`main_ip6 <Main IPv6 Address>`	IPv6 Address	Specifies the main IPv6 Address of the Virtual Device object. This parameter is applicable only for a: ■ Virtual System ■ Virtual Router **Note** - To remove the current IPv6 address, set the value to `empty`. For example: `set vd name VS1 main_ip6 empty`

Parameter	Value	Notes
`calc_topo_auto {true | false}`	■ `true` ■ `false`	Specifies how to calculate topology based on routes: ■ `true` - Automatically calculate topology based on routes (default) ■ `false` - Does not calculate topology based on routes (administrator can configure it manually) This parameter is applicable only for a: ■ Virtual System ■ Virtual Router

Example

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o set vd name VS1 instances 8 main_ip 192.0.2.6 calc_topo_auto false
```

Adding an Interface to a Virtual Device

Description

This command adds an interface to an existing Virtual Device object:

- Virtual System
- Virtual System in Bridge Mode
- Virtual Switch
- Virtual Router

Syntax

```
add interface vd <Name of Virtual Device Object> {name <Name of
Interface> | leads_to <Name of VSW or VR Object>} ip <IPv4
Address>{/<IPv4 Prefix Length> | netmask <IPv4 Netmask> | prefix
<IPv4 Prefix>} ip6 <IPv6 Address>{/<IPv6 Prefix Length> | netmask6
<IPv6 Netmask> | prefix6 <IPv6 Prefix>} [propagate {true | false}]
[propagate6 {true | false}] [topology {external | internal_
undefined | internal_this_network | internal_specific [specific_
group <Name of Network Group Object>]}] [mtu <MTU>]
```

Parameters

Parameter	Value	Notes
`vd <Name of Virtual Device Object>`	Object name	Specifies the name of the Virtual Device object. Mandatory parameter, if this is the first command in a transaction.
`name <Name of Interface>`	Interface name	Specifies the name of the physical or VLAN interface. **Note** - You must use the "`name`" or "`leads_to`" parameter, but not both.
`leads_to <Name of VSW or VR Object>`	Object name	Specifies the name of the Virtual Switch or Virtual Router object, to which this interface connects. This parameter is applicable only for a Virtual System. **Note** - You must use the "`name`" or "`leads_to`" parameter, but not both.

Parameter	Value	Notes
`ip <IPv4 Address> {/<IPv4 Prefix> | netmask <IPv4 Netmask> | prefix <IPv4 Prefix>}`	IPv4 configuration	Specifies the IPv4 settings: ■ `<IPv4 Address>` - IPv4 address ■ `<IPv4 Prefix>` - Integer between 1 and 32 ■ `<IPv4 Netmask>` - Number in a format X.X.X.X This parameter is applicable only for a: ■ Virtual System ■ Virtual Router For interfaces on a Virtual System that connect to a Virtual Router, you must use the possible maximum for the IPv4 address family: ■ Netmask 255.255.255.255 ■ Prefix 32
`ip6 <IPv6 Address> {/<IPv6 Prefix> | netmask6 <IPv6 Netmask> | prefix6 <IPv6 Prefix>}`	IPv6 configuration	Specifies the IPv6 settings: ■ `<IPv6 Address>` - IPv6 address ■ `<IPv6 Prefix>` - Integer between 64 and 128 ■ `<IPv6 Netmask>` - Number in a format XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX This parameter is applicable only for a: ■ Virtual System ■ Virtual Router For interfaces on a Virtual System that connect to a Virtual Router, you must use the possible maximum for the IPv6 address family: ■ Netmask FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF ■ Prefix 128

Parameter	Value	Notes
`propagate {true | false}`	▪ `true` ▪ `false`	Controls how to propagate the IPv4 routes to adjacent Virtual Devices: ▪ `true` - Propagate the IPv4 routes ▪ `false` - Do not propagate the IPv4 routes (default) **Note** - This parameter is applicable only for a Virtual System with VLAN or physical interfaces.
`propagate6 {true | false}`	▪ `true` ▪ `false`	Controls how to propagate the IPv6 routes to adjacent Virtual Devices: ▪ `true` - Propagate the IPv6 routes ▪ `false` - Do not propagate the IPv6 routes (default) **Note** - This parameter is applicable only for a Virtual System with VLAN or physical interfaces.
`topology {external | internal_undefined | internal_this_network | internal_specific }`	▪ `external` ▪ `internal_undefined` ▪ `internal_this_network` ▪ `internal_specific`	Specifies the Topology configuration of the interface: ▪ `external` - External interface. ▪ `internal_undefined` - Internal interface with undefined topology. This is the default for a Virtual System in Bridge Mode. ▪ `internal_this_network` - Internal interface. This is the default for a Virtual System and Virtual Router. Virtual System in Bridge Mode does not support this topology. ▪ `internal_specific [specific_group <Name of Network Group Object>]` - Internal interface with topology defined by the specified Network Group object. This parameter is applicable only for a: ▪ Virtual System ▪ Virtual System in Bridge Mode ▪ Virtual Router

Parameter	Value	Notes
`specific_group <Network Group Object Name>`	Name of Network Group Object	If you specified the "`topology internal_specific`" parameter, then specify the name of the Network Group object that contains the applicable Network objects. **Note** - This parameter is applicable only if you disable the automatic topology calculation with the "`set vd ... calc_topo_auto false`" command (see *"Modifying Settings of a Virtual Device" on page 1955*).
`mtu <MTU>`	Integer	Specifies the MTU value for this interface. Default is 1500 bytes. This parameter is applicable only for a: ■ Virtual System ■ Virtual Router

Example - Add VLAN interface eth4.100 with IPv4 1.1.1.1/24 to the Virtual System 'VirtSystem1'

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o add interface vd VirtSystem1 name eth4.100 ip 1.1.1.1/24
```

Adding a Bridge Interface to a Virtual System

Description

Some Software Blades and features are not supported on a Virtual System in Bridge Mode, because it may not have an IP address.

For example: Threat Emulation, Identity Awareness, Identity Awareness Captive Portal, and UserCheck Portal are not supported.

This command adds a Bridge interface to an existing regular Virtual System object that always has an IP address.

As a result, the Virtual System can support these Software Blades and features for the traffic that passes over the configured bridge interface.

Notes:

- Names of bridge interfaces have a template "`brX`", where "`X`" is a digit.
- It is necessary to add subordinate interfaces in pairs to a bridge interface.
- To see the bridge interfaces you configured in the Virtual System object:
  1. Connect to the command line on the VSX Gateway (each VSX Cluster Member).
  2. Log in to the Expert mode.
  3. Go to the context of the Virtual System:
     ```
     vsenv <VSID>
     ```
  4. Examine the list of interfaces:
     ```
     ifconfig
     ```
- You can delete bridge interfaces from a Virtual System either in SmartConsole, or with the "`vsx_provisioning_tool`" command (see *"Removing an Interface from a Virtual Device" on page 1966*).

Syntax

```
attach bridge vd <Name of Virtual System Object> ifs1 <Name of First Subordinate Interface> ifs2 <Name of Second Subordinate Interface>
```

Parameters

Parameter	Value	Notes
`vd <Name of Virtual System Object>`	Object name	Specifies the name of the Virtual System object. Mandatory parameter, if this is the first command in a transaction.
`ifs1 <Name of First Subordinate Interface>`	Interface name	Specifies the name of the physical interface to be the first subordinate interface of a bridge interface. **Note** - This physical interface must not have an IP address
`ifs2 <Name of First Second Interface>`	Interface name	Specifies the name of the physical interface to be the second subordinate interface of a bridge interface. **Note** - This physical interface must not have an IP address

Example 1 - Adding a Bridge interface with subordinate interfaces "eth2" and "eth3" in the Virtual System "VS1"

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o attach bridge vd VS1 ifs1 eth2 ifs2 eth3
```

Example 2 - Adding a Multi Bridge interface in the Virtual System "VS1"

In this example, we add pairs of VLAN interfaces to the Virtual System "VS1" to add a Multi Bridge interface (for more information, see the *R81.20 VSX Administration Guide* > section "*Virtual System in Bridge Mode*"):

- VLANs eth2.403 and eth3.403 as the first bridge interface
- VLANs eth2.504 and eth3.504 as the second bridge interface

The prerequisite is to configure both physical interfaces "eth2" and "eth3" as VLAN Trunks (see *"Configuring a Physical Interface as VLAN Trunk" on page 1972*).

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o attach bridge vd VS1 ifs1 eth2.403 ifs2 eth3.403, attach bridge ifs1
eth2.504 ifs2 eth3.504
```

Adding a VPN Tunnel Interface to a Virtual Device

Description

Virtual Tunnel Interface (VTI) is a virtual interface that is used for establishing a Route-Based VPN tunnel.

This command adds a VTI to an existing Virtual System object.

The VPN tunnel and its properties are defined by the VPN community that contains the two Security Gateways.

You must define the VPN community and its member Security Gateways before you can create a VTI.

To learn more about Route Based VPN, see the *R81.20 Site to Site VPN Administration Guide* > Chapter *Route Based VPN*.

Syntax

```
add interface vd <Name of Virtual System Object> vpn_tunnel
numbered peer <Name of VPN Peer Object> local <Tunnel Local IP>
remote <Tunnel Remote IP> [tunnel_id <Tunnel ID>]
```

Parameters

Parameter	Value	Notes
`vd <Name of Virtual System Object>`	Object name	Specifies the name of the Virtual System object (as configured in SmartConsole). Mandatory parameter, if this is the first command in a transaction.
`vpn_tunnel numbered`	■ `true` ■ `false`	Specifies the type of the VPN tunnel as numbered. Uses a specified, static IPv4 addresses for local and remote connections.
`peer <Name of VPN Peer Object>`	Object name	Specifies the name of the remote peer object as defined in the VPN community in SmartConsole.

Parameter	Value	Notes
`local <Tunnel Local IP> remote <Tunnel Remote IP>`	IPv4 configuration	Specifies the IPv4 addresses in dotted decimal format for the VPN tunnel endpoints: ■ `local <Tunnel Local IP>` - IPv4 address of the VPN tunnel on this Virtual System ■ `remote <Tunnel Remote IP>` - IPv4 address of the VPN tunnel on the remote VPN peer Applies to the Numbered VTI only.
`tunnel_id <Tunnel ID>`	Integer	Specifies the unique Tunnel ID (integer from 1 to 32768). **Note** - If the specified ID is already used by another VPN tunnel on this VSX Gateway or VSX Cluster Member, this parameter is ignored and the next available ID is used instead.

Example - Numbered VTI

```
vsx_provisioning_tool -o add interface vd vs1 vpn_tunnel numbered peer AWS_Peer local 169.254.46.238 remote 169.254.46.237 tunnel_id 10
```

Note - Unnumbered VTIs are not supported.

Removing an Interface from a Virtual Device

Description

This command removes an interface from an existing Virtual Device object:

- Virtual System
- Virtual System in Bridge Mode
- Virtual Switch
- Virtual Router

Important:

- If the interface you remove leads to a Virtual Router, all routes through that interface are removed automatically.
- You must remove **all** subordinate interfaces of a bridge interface in the same transaction. This also removes the bridge interface.

Note - If there are routes that have a next-hop IP address, which would become inaccessible without this interface, the transaction fails.

Syntax

```
remove interface vd <Name of Virtual Device Object> {name <Name of Interface> | leads_to <Name of VSW or VR Object>}
```

Parameters

Parameter	Value	Notes
`vd <Name of Virtual Device Object>`	Object name	Specifies the name of the Virtual Device object. Mandatory parameter, if this is the first command in a transaction.
`name <<Name of Interface>>`	Interface name	Specifies the name of the physical or VLAN interface. **Note** - You must use the "`name`" or "`leads_to`" parameter, but not both.
`leads_to <Name of VSW or VR Object>`	Object name	Specifies the name of the Virtual Switch or Virtual Router object, to which this interface connects. This parameter is applicable only for a Virtual System. **Note** - You must use the "`name`" or "`leads_to`" parameter, but not both.

Example 1 - Removing a VLAN interface from a Virtual System "VS1"

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o remove interface vd VS1 name eth4.100
```

Example 2 - Removing all subordinate interfaces "eth2" and "eth3" of a bridge interface in the Virtual System "VS1"

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o remove interface vd VS1 name eth2, remove interface vd VS1 name eth3
```

Modifying Settings of an Interface

Description

This command changes the settings of an interface that belongs to an existing Virtual Device object:

- Virtual System
- Virtual System in Bridge Mode
- Virtual Switch
- Virtual Router

Note - You cannot change or remove the IP address or netmask of an existing interface with this command. You can remove the interface and add a new interface with a different IP address, but not all the previous interface settings are kept.

Syntax

```
set interface vd <Name of Virtual Device Object> {name <Name of
Interface> [new_name <Name of New Interface>] | leads_to <Name of
VSW or VR Object> [new_leads_to <Name of New VSW or VR Object>]}
[propagate {true | false}] [propagate6 {true | false}] [topology
{external | internal_undefined | internal_this_network | internal_
specific [specific_group <Network Group Object Name>]}] [mtu
<MTU>]
```

Parameters

Parameter	Value	Notes
`vd <Name of Virtual Device Object>`	Object name	Specifies the name of the Virtual Device object. Mandatory parameter, if this is the first command in a transaction.
`name <Name of Interface>`	Interface name	Specifies the name of the physical or VLAN interface. **Note** - You must use the "`name`" or "`leads_to`" parameter, but not both.

Parameter	Value	Notes
`new_name <Name of New Interface>`	Interface name	You can change the name, but not the type of interface. **Note** - You can change a VLAN or physical interface only to a VLAN or physical interface.
`leads_to <Name of VSW or VR Object>`	Object name	Specifies the name of the Virtual Switch or Virtual Router object, to which this interface connects. This parameter is applicable only for a Virtual System. **Note** - You must use the "`name`" or "`leads_to`" parameter, but not both.
`new_leads_to <Name of New VSW or VR Object>`	Object name	You can where the interface leads: ■ You can change an interface that leads to a Virtual Switch only to lead to a different Virtual Switch. ■ You can change an interface that leads to a Virtual Router only to lead to a different Virtual Router.
`propagate {true | false}`	■ `true` ■ `false`	Controls how to propagate the IPv4 routes to adjacent Virtual Devices: ■ `true` - Propagate the IPv4 routes ■ `false` - Do not propagate the IPv4 routes (default) **Note** - This parameter is applicable only for a Virtual System with VLAN or physical interfaces.

Parameter	Value	Notes
`propagate6 {true | false}`	■ `true` ■ `false`	Controls how to propagate the IPv6 routes to adjacent Virtual Devices: ■ `true` - Propagate the IPv6 routes ■ `false` - Do not propagate the IPv6 routes (default) **Note** - This parameter is applicable only for a Virtual System with VLAN or physical interfaces.
`topology {external | internal_undefined | internal_this_network | internal_specific}`	■ `external` ■ `internal_undefined` ■ `internal_this_network` ■ `internal_specific`	Specifies the Topology configuration of the interface: ■ `external` - External interface. ■ `internal_undefined` - Internal interface with undefined topology. This is the default for Virtual System in Bridge Mode. ■ `internal_this_network` - Internal interface. This is the default for Virtual System and Virtual Router. Virtual System in Bridge Mode does not support this topology. ■ `internal_specific [specific_group <Network Group Object Name>]` - Internal interface with topology defined by the specified Network Group object. This parameter is applicable only for a: ■ Virtual System ■ Virtual System in Bridge Mode ■ Virtual Router

Parameter	Value	Notes
`specific_group <Network Group Object Name>`	Name of Network Group Object	If you specified the "`topology internal_specific`" parameter, then specify the name of the Network Group object that contains the applicable Network objects. **Note** - This parameter is applicable only if you disable the automatic topology calculation with the "`set vd ... calc_topo_auto false`" command (see *"Modifying Settings of a Virtual Device" on page 1955*).
`mtu <MTU>`	Integer	Specifies the MTU value for this interface. Default is 1500 bytes. This parameter is applicable only for: ■ Virtual System ■ Virtual Router

Example - On the Virtual System "VS1", change the VLAN interface eth4.10 to the physical interface eth5

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o set interface vd VS1 name eth4.100 new_name eth5 propagate true topology
internal_specific specific_group NYGWs
```

Configuring a Physical Interface as VLAN Trunk

Description

This command configures a physical interface as VLAN Trunk.

This is required to configure VLAN interfaces the physical interface.

Important - Make sure the physical interface you configure as VLAN Trunk does not have an IP address.

Syntax

```
set physical_interface vd <Name of VSX Gateway or VSX Cluster Object> name <Name of Interface> vlan_trunk {true | false}
```

Parameters

Parameter	Value	Notes
`vd <Name of VSX Gateway or VSX Cluster Object>`	Object name	Specifies the name of the VSX Gateway or VSX Cluster object. Mandatory parameter, if this is the first command in a transaction.
`name <Name of Interface>`	Interface name	Specifies the name of the physical interface.
`vlan_trunk {true | false}`	■ `true` ■ `false`	Controls whether this physical interface is a VLAN Trunk: ■ `true` - VLAN Trunk interface ■ `false` - Regular physical interface (default)

Example - On the VSX Gateway "VSX1" configure the physical interface eth2 as VLAN Trunk

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o set physical_interface vd VSX1 name eth2 vlan_trunk true
```

Adding a Route

Description

This command adds an IPv4 or IPv6 route to an existing Virtual System or Virtual Router object.

Note - This command detects IPv4 and IPv6 automatically.

Syntax

```
add route vd <Name of VS or VR Object> destination {<IP Address>
[/<IP Prefix>] | default | default6} [{netmask <IP Netmask> |
prefix <IP Prefix>}] {next_hop <Next Hop IP Address> | leads_to
<Name of VS or VR Object>} [propagate {true | false}]
```

Parameters

Parameter	Value	Notes
`vd <Name of VS or VR Object>`	Object name	Specifies the name of the Virtual System or Virtual Router object. Mandatory parameter, if this is the first command in a transaction.
`destination {<IP Address> [/<IP Prefix>] | default | default6}`	See the *Notes* column on the right	Specifies the route destination settings: ■ `<IP Address>` - IPv4 or IPv6 address ■ `<IP Prefix>` - • For IPv4 - Integer between 1 and 32 • For IPv6 - Integer between 64 and 128 ■ `default` - Use the default IPv4 route ■ `default6` - Use the default IPv6 route
`netmask <IP Netmask>`	Number	Specifies an IP Netmask: ■ For IPv4 - Number in a format X.X.X.X ■ For IPv6 - Number in a format XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX
`prefix <IP Prefix>`	Integer	Specifies the IP address prefix length: ■ For IPv4 - Integer between 1 and 32 ■ For IPv6 - Integer between 64 and 128

Parameter	Value	Notes
`next_hop <Next Hop IP Address>`	IP Address	Specifies the IP address of the next hop of the route. **Notes:** ■ This IP address must be on a subnet of an existing interface. ■ You must use the "`next_hop`" or "`leads_to`" parameter, but not both.
`leads_to <Name of VS or VR Object>`	Object name	Specifies the name of the Virtual System or Virtual Router object, which is the next hop for the configured route. **Note** - You must use the "`next_hop`" or "`leads_to`" parameter, but not both.
`propagate {true | false}`	■ `true` ■ `false`	Controls how to propagate the IP routes to adjacent Virtual Devices: ■ `true` - Propagate the IP routes ■ `false` - Do not propagate the IP routes (default) **Note** - The "`propagate`" parameter is applicable only if you specified the "`next_hop`" parameter.

Example - Adding a route on the Virtual System "VS1" that uses the default IPv4 route as a destination and the Virtual Router "VR3" as a next hop

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o add route vd VS1 destination default leads_to VR3
```

Removing a Route

Description

This command removes an IPv4 or IPv6 route from an existing Virtual System or Virtual Router object.

Note - This command detects IPv4 and IPv6 automatically.

Syntax

```
remove route vd <Name of VS or VR Object> destination {<IP
Address>[/<IP Prefix>] | default | default6} [{netmask <IP
Netmask> | prefix <IP Prefix>]
```

Parameters

Parameter	Value	Notes
`vd <Name of VS or VR Object>`	Object name	Specifies the name of the Virtual System or Virtual Router object. Mandatory parameter, if this is the first command in a transaction.
`destination {<IP Address> [/<IP Prefix>] | default | default6}`	See the *Notes* column on the right	Specifies the route destination settings: ■ `<IP Address>` - IPv4 or IPv6 address ■ `<IP Prefix>` - • For IPv4 - Integer between 1 and 32 • For IPv6 - Integer between 64 and 128 ■ `default` - Use the default IPv4 route ■ `default6` - Use the default IPv6 route
`netmask <IP Netmask>`	Number	Specifies an IP Netmask: ■ For IPv4 - Number in a format X.X.X.X ■ For IPv6 - Number in a format XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX
`prefix <IP Prefix>`	Integer	Specifies the IP address prefix length: ■ For IPv4 - Integer between 1 and 32 ■ For IPv6 - Integer between 64 and 128

Example - Removing a route from the Virtual System "VS1" that uses the default IPv6 route as a destination

```
vsx_provisioning_tool -s localhost -u admin -p mypassword -o remove route vd VS1 destination default6
```

Showing Virtual Device Data

Description

This command shows the information about an existing Virtual Device object.

Syntax

```
show vd name <Name of Virtual Device Object>
```

Parameters

Parameter	Value	Notes
`vd <Name of Virtual Device Object>`	Name of the Virtual Device	Specifies the name of the Virtual Device object. Mandatory parameter.

Comments

- The command shows only non-automatic routes.
- The command does not show routes that are created automatically with route propagation.
- For a Virtual Router and Virtual Switch:

  The command does not show the `wrpj` interfaces (created automatically) that connect to Virtual Systems.

Script Examples

Note - Line numbers in the left column are written only to make it easier to read the script examples.

Example 1

Create a Virtual System connected to a Virtual Router.

Add a default route on the Virtual System that routes the traffic to the Virtual Router.

Add applicable routes on the Virtual Router to route the traffic to the Virtual System.

Line	Command
1	`transaction begin`
2	`add vd name VR1 vsx VSX1 type vr`
3	`add interface name eth3.100 ip 10.0.0.1/24`
4	`transaction end`
5	`transaction begin`
6	`add vd name VR2 vsx VSX2 type vr`
7	`add interface name eth3.200 ip 20.0.0.1/24`
8	`transaction end`
9	`transaction begin`
10	`add vd name VS1 vsx VSX1`
11	`add interface leads_to VR1 ip 192.168.1.1/32`
12	`add interface name eth4.20 ip 192.168.20.1/24 propagate true`
13	`add route destination default leads_to VR1`
14	`add route destination 192.168.40.0/25 next_hop 192.168.20.254`
15	`transaction end`

Example 2

Create a Virtual System connected to a Virtual Switch, with manual topology.

Line	Command
1	`transaction begin`
2	`add vd name VSW1 vsx VSX1 type vsw vs_mtu 1400`
3	`add interface name eth3.100`
4	`transaction end`
5	`transaction begin`
6	`add vd name VS1 vsx VSX1 calc_topo_auto false`
7	`add interface leads_to VSW1 ip 10.0.0.1/24 ip6 2001::1/64 topology external`
8	`add interface name eth4.20 ip 192.168.20.1/25 ip6 2020::1/64 topology internal_this_network`
9	`add route destination default next_hop 10.0.0.254`
10	`add route destination default6 next_hop 2001::254`
11	`transaction end`

Example 3

Add CoreXL Firewall instances to the Virtual System made in the last example.

Turn on automatic calculation of topology.

Change the name of the internal interface, and decrease its MTU.

Line	Command
1	`transaction begin`
2	`set vd name VS1 instances 4 instances6 2 calc_topo_auto true`
3	`set interface name eth4.20 new_name eth4.21 mtu 1400`
4	`transaction end`

QoS Commands

For more information about QoS, see the *R81.20 QoS Administration Guide*.

etmstart

Description

Starts the QoS Software Blade on the Security Gateway - starts the QoS daemon `fgd50`, and fetches the QoS policy from the Management Servers configured in the `$FWDIR/conf/masters` file on the Security Gateway.

For more information, see:

- *R81.20 QoS Administration Guide*
- sk41585: How to control and debug QoS (FloodGate-1)

Syntax

```
etmstart
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Example

```
[Expert@MyGW:0]# etmstart
QoS: Starting fgd50

QoS: Fetching QoS Policy from masters
Fetching QoS Software Blade Policy:
 Received Policy. Downloading...

eth0(inbound), eth0(outbound).
Download OK.
Done.
QoS started
[Expert@MyGW:0]#
```

etmstop

Description

Stops the QoS Software Blade on the Security Gateway - kills the QoS daemon `fgd50` and then unloads the QoS policy.

For more information, see:

- *R81.20 QoS Administration Guide*
- sk41585: How to control and debug FloodGate-1 (QoS)

Syntax

```
etmstop
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Example

```
[Expert@CXL1_192.168.3.52:0]# etmstop
 Unloading QoS Policy:
 Target(s): CXL1_192.168.3.52
   CXL1_192.168.3.52: QoS policy unloaded successfully.
 Done.
QoS stopped
[Expert@CXL1_192.168.3.52:0]#
```

fgate

This section describes:

The 'fgate' command on Management Server

Description

Installs and uninstalls the QoS policy on the managed Security Gateways.

Shows the status of the QoS Software Blade on the managed Security Gateways.

For more information, see:

- *R81.20 QoS Administration Guide*
- sk41585: How to control and debug FloodGate-1 (QoS)

Syntax

```
fgate [-d]
      load <Name of QoS Policy>.F <GW1> <GW2> ... <GWN>
      stat
            -h
            <GW1> <GW2> ... <GWN>
      unload <GW1> <GW2> ... <GWN>
      ver
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.

Parameter	Description
`load <Name of QoS Policy>.F <GW1> <GW2> ... <GWN>`	Runs a verifier on the QoS policy <*Name_of_QoS_Policy*>. If the QoS policy is valid, the Management Server compiles and installs the QoS Policy on the specified Security Gateways `<GW1> <GW2> ... <GWN>`. **Notes:** ■ The maximal supported length of the <*Name of QoS Policy*> string is 32 characters. ■ To specify a Security Gateway, enter the main IP address of the name of its object as configured in SmartConsole. You can specify several Security Gateways or cluster members in the same command.
`stat -h`	Shows the built-in usage for the "`stat`" parameter.
`stat <GW1> <GW2> ... <GWN>`	Shows the status of the QoS Software Blade and policy on the managed Security Gateways. **Note** - To specify a Security Gateway, enter the main IP address of the name of its object as configured in SmartConsole. You can specify several Security Gateways or cluster members in the same command. **Important** - This command is outdated and exists only for backward compatibility with very old versions. Use the "*"cpstat" on page 1019*" command.
`unload <GW1> <GW2> ... <GWN>`	Uninstalls the QoS Policy from the specified Security Gateways `<GW1> <GW2> ... <GWN>`. **Note** - To specify a Security Gateway, enter the main IP address of the name of its object as configured in SmartConsole. You can specify several Security Gateways or cluster members in the same command.
`ver`	Shows the QoS Software Blade version on the Management Server.

Examples

Example 1 - Installing the QoS policy on one Security Gateway specified by its IP address

```
[Expert@MGMT:0]# fgate load MyPolicy.F 192.168.3.52
 QoS rules verified OK!
 Downloading QoS Policy: MyPolicy.F...
 Target(s): MyGW
   MyGW: QoS policy transferred to module: MyGW.
   MyGW: QoS policy installed succesfully.
 Done.
[Expert@MGMT:0]#
```

Example 2 - Installing the QoS policy on two cluster members specified by their object names

```
[Expert@MGMT:0]# fgate load MyPolicy.F MyClusterMember1 MyClusterMember2
 QoS rules verified OK!
 Downloading QoS Policy: MyPolicy.F...
   MyClusterMember1: QoS policy transferred to module: MyClusterMember1.
   MyClusterMember1: QoS policy installed succesfully.
   MyClusterMember2: QoS policy transferred to module: MyClusterMember2.
   MyClusterMember2: QoS policy installed succesfully.
 Done.
[Expert@MGMT:0]#
```

Example 3 - Viewing the QoS status on one Security Gateway specified by its object name

```
[Expert@MGMT:0]# fgate stat MyGW

Module name: MyGW
=======================

Product: QoS Software Blade
Version: R81.20
Kernel Build: 456
Policy Name: MyPolicy
Install time: Wed Dec 4 19:53:48 2019
Interfaces Num: 1


Interface table
------------------------------------------------------------------
|Name|Dir|Limit (Bps)|Avg Rate (Bps)|Conns|Pend pkts|Pend bytes|
------------------------------------------------------------------
|eth0|in | 1250000000|             0|    0|        0|         0|
|eth0|out| 1250000000|             0|    0|        0|         0|
------------------------------------------------------------------

[Expert@MGMT:0]#
```

Example 4 - Viewing the QoS Software Blade version

```
[Expert@MGMT:0]# fgate ver
This is Check Point QoS Software Blade R81.20 - Build 123
[Expert@MGMT:0]#
```

The 'fgate' command on Security Gateway

Description

Installs and uninstalls the QoS policy on the managed Security Gateways.

Shows the status of the QoS Software Blade on the managed Security Gateways.

Controls the QoS debug.

For more information, see:

- *R81.20 QoS Administration Guide*
- sk41585: How to control and debug FloodGate-1 (QoS)

Syntax

```
fgate [-d]
      ctl
            -h
            <QoS Module> {on | off}
      debug
            on
            off
      fetch
            -f
            <Management Server>
      kill [-t <Signal Number>] <Name of QoS Process>
      load
      log
            on
            off
            stat
      stat [-h]
      ver [-k]
      unload
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`ctl -h`	Shows the expected syntax and the list of the available QoS modules.
`ctl <QoS Module> {on | off}`	Controls the specified QoS module: ■ `on` - Enables the module (default) ■ `off` - Disables the module **Note** - In R81.20, the only available QoS module is `etmreg`.
`debug {on | off}`	Controls the debug mode of the QoS user space daemon `fgd50` (see sk41585): ■ `on` - Enables the debug ■ `off` - Disables the debug (default) This sends additional debugging information to the `fgd50` daemon's log file `$FGDIR/log/fgd.elg`.
`fetch -f`	Fetches and installs the QoS Policy from all the Management Servers configured in the `$FWDIR/conf/masters` file.
`fetch <Management Server>`	Fetches and installs the QoS Policy from the specified Management Server. Enter the main IP address or the name of the Management Server object as configured in SmartConsole.

Parameter	Description
`kill [-t <Signal Number>] <Name of QoS Process>`	Sends the specified signal to the specified QoS user space process. **Notes:** ■ In R81.20, the only available QoS user space process is `fgd50`. ■ The QoS `fgd50` daemon, upon its startup, writes the PIDs of the applicable QoS user spaces processes to the `$FWDIR/tmp/<Name of QoS Process>.pid` files. For example: `$FWDIR/tmp/fgd50.pid` ■ If the file `$FWDIR/tmp/<Name of QoS Process>.pid` exists, then this command sends the specified Signal Number to the PID in that file. ■ If you do not specify the signal explicitly, the command sends Signal 15 (`SIGTERM`). ■ For the list of available signals and their numbers, run the `kill -l` command. For information about the signals, see the manual pages for the `kill` and `signal`. ■ To restart the QoS `fgd50` daemon manually, run the *"etmstop" on page 1983* and then *"etmstart" on page 1982* commands.
`load`	Installs the local QoS Policy on the Security Gateway. If this command fails, run the *"etmstop" on page 1983* and then *"etmstart" on page 1982* commands.
`log {on | off | stat}`	Controls the state of QoS logging in the Security Gateway kernel: ■ `on` - Enables the QoS logging (default) ■ `off` - Disables the QoS logging ■ `stat` - Shows the current QoS logging status You can disable the QoS logging to save resources without reinstalling the QoS policy.

Parameter	Description
`stat [-h]`	Shows the status of the QoS Software Blade and policy on the Security Gateway. The `-h` parameter shows the built-in usage for the "`stat`" parameter. **Important** - This command is outdated and exists only for backward compatibility with very old versions. Use the "*"cpstat" on page 1019*" command.
`unload`	Uninstalls the QoS Policy from the Security Gateway.
`ver [-k]`	Shows the QoS Software Blade version. If you specify the "`-k`" parameter, the output also shows the kernel version.

Examples

Example 1 - Fetching the QoS policy based on the $FWDIR/conf/masters file

```
[Expert@MyGW]# fgate fetch -f
Fetching QoS Software Blade Policy:
 Received Policy. Downloading...

eth0(inbound), eth0(outbound).
Download OK.
Done.
[Expert@MyGW]#
```

Example 2 - Fetching the QoS policy from the Management Server specified by its IP address

```
[Expert@MyGW]# fgate fetch 192.168.3.240
Fetching QoS Software Blade Policy:
 Received Policy. Downloading...

eth0(inbound), eth0(outbound).
Download OK.
Done.
[Expert@MyGW]#
```

Example 3 - Viewing the QoS status

```
[Expert@MyGW]# fgate stat

Product:        QoS Software Blade
Version:        R81.20
Kernel Build:   456
Policy Name:    MyPolicy
Install time:   Wed Dec 4 19:53:48 2019
Interfaces Num: 1


Interface table
-------------------------------------------------------------------
|Name|Dir|Limit (Bps)|Avg Rate (Bps)|Conns|Pend pkts|Pend bytes|
-------------------------------------------------------------------
|eth0|in | 1250000000|             0|    0|        0|         0|
|eth0|out| 1250000000|             0|    0|        0|         0|
-------------------------------------------------------------------

[Expert@MyGW]#
```

Example 4 - Viewing the QoS Software Blade version

```
[Expert@MyGW:0]# fgate ver
This is Check Point QoS Software Blade R81.20 - Build 123
[Expert@MyGW:0]#
[Expert@MyGW:0]# fgate ver -k
This is Check Point QoS Software Blade R81.20 - Build 123
kernel: R81.20 - Build 456
[Expert@MyGW:0]#
```

IPS Commands

For more information about IPS, see the *R81.20 Threat Prevention Administration Guide*.

IPS commands let you configure and show the IPS on the Security Gateway without installing a new policy.

Important - Changes in the IPS configuration made with these commands are not persistent. If you install a policy or restart the Security Gateway, the changes are deleted.

ips

Description

Shows various information about the IPS Software Blade.

Controls the IPS Software Blade.

Syntax

```
ips
      bypass <options>
      debug <options>
      off
      on
      refreshcap
      stat
      stats <options>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
No Parameters	Shows the built-in usage.
`bypass <options>`	Controls the IPS Bypass mode. See *"ips bypass" on page 1995*.
`debug <options>`	Collects the IPS debug. See *"ips debug" on page 1997*.
`off`	Disables the IPS Software Blade on-the-fly. See *"ips off" on page 1998*.
`on`	Enables the IPS Software Blade on-the-fly. See *"ips on" on page 1999*.
`refreshcap`	Refreshes the IPS sample capture repository. See *"ips refreshcap" on page 2000*.

Parameter	Description
`stat`	Shows the IPS status. See *"ips stat" on page 2001*.
`stats <options>`	Shows statistics for the IPS performance and Pattern Matcher. See *"ips stats" on page 2002*.

ips bypass

Description

Controls the IPS Bypass mode:

- When CPU and/or Memory utilization reaches the configured higher threshold, IPS Software Blade disables itself.
- When CPU and/or Memory utilization goes down to the configured lower threshold, IPS Software Blade enables itself.

Syntax

```
ips bypass
      off
      on
      set <options>
      stat
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
No Parameters	Shows the applicable built-in usage.
`off`	Disables the IPS Bypass mode.
`on`	Enables the IPS Bypass mode.

Parameter	Description

`set <options>`	Configures the utilization thresholds (in per cent), at which to engage (higher threshold) or disengage (lower threshold) the IPS Bypass mode. The available options are:
	■ Configure the lower CPU threshold:
	`ips bypass set cpu low <0-100>`
	■ Configure the higher CPU threshold:
	`ips bypass set cpu high <0-100>`
	■ Configure the lower Memory threshold:
	`ips bypass set mem low <0-100>`
	■ Configure the higher Memory threshold:
	`ips bypass set mem high <0-100>`
	Example:
	`ips bypass set cpu low 80`

`stat`	Shows the status of the IPS Bypass Under Load: ■ IPS bypass mode ■ CPU thresholds ■ Memory thresholds

ips debug

Description

Collects the IPS debug information.

Note - For information about the kernel debug, see the *R81.20 Security Gateway Guide* - Chapter *Kernel Debug on Security Gateway*.

Syntax

```
ips debug [-e <Filter>] -o <Output File>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`-e <Filter>`	Specifies the INSPECT filter to capture packets. For more information, see the explanation for the "*"fw monitor" on page 1151*" command in sk30583: What is FW Monitor?
`-o <Output File>`	Specifies the path and the name of the output debug file.

Example

```
ips debug -o /var/log/IPS_debug.txt
```

ips off

Description

Disables the IPS Software Blade on-the-fly.

Note - To enable, run the "*"ips on" on page 1999*" command.

Syntax

```
ips off
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Example 1

```
[Expert@MyGW:0]# ips off
IPS is disabled
Please note that for the configuration to apply for connections from existing templates, you have to run this command with -n flag which
deletes existing templates.
Without '-n', it will fully take effect in a few minutes.
[Expert@MyGW:0]#
```

Example 2

```
[Expert@MyGW:0]# ips off -n
IPS is disabled
Deleting templates

Clearing table cphwd_tmpl
[Expert@MyGW:0]#
```

ips on

Description

Enables the IPS Software Blade on-the-fly, if it was disabled with the "*"ips off" on page 1998*" command.

Syntax

```
ips on [-n]
```

Example 1

```
[Expert@MyGW:0]# ips on
IPS is enabled
Please note that for the configuration to apply for connections from existing templates, you have to run this command with -n flag which
deletes existing templates.
Without '-n', it will fully take effect in a few minutes.
[Expert@MyGW:0]#
```

Example 2

```
[Expert@MyGW:0]# ips on -n
IPS is enabled
Deleting templates

Clearing table cphwd_tmpl
[Expert@MyGW:0]#
```

ips refreshcap

Description

After you install a new policy, the IPS Software Blade captures the first packet for each IPS protection and saves it in the packet capture repository.

This command refreshes the packet capture repository.

The IPS designates the next packet of each IPS protection as the first packet.

The new first packet replaces the previous one in the packet capture repository.

Syntax

```
ips refreshcap
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Example

```
[Expert@MyGW:0]# ips refreshcap
Refreshed IPS sample capture
- A single new packet capture will be issued upon the next detection of each attack. You can see
the packet capture attached to the log or in the Packet Capture Repository.
[Expert@MyGW:0]#
```

ips stat

Description

Shows this information:

- IPS Status (Enabled or Disabled)
- IPS Update Version
- Global Detect (On or Off)
- Bypass Under Load (On or Off)

Syntax

```
ips stat
```

Important - On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Example

```
[Expert@MyGW:0]# ips stat
Active Profiles:
My_IPS_Profile
IPS Status: Enabled
IPS Update Version: 635158746
Global Detect: Off
Bypass Under Load: Off
[Expert@MyGW:0]#
```

ips stats

Description

This tool generates a report that includes both IPS and Pattern Matcher statistics.

The report can help administrators and protection writers analyze, which IPS protections or IPS components cause performance issues.

The output files are located in the `$FWDIR/ips/statistics_results/` directory.

On a Standalone, the tool creates a directory for each specified IP address.

The output files are:

File	Description
`ips.dbg`	Contains the raw report, which contains all the information.
`ips_stat_output_file.csv`	Contains the report with the IPS statistics.
`pm_output_file.csv`	Contains the statistics for the Pattern Matcher.
`tier1_output_file.csv`	Contains the statistics for the Pattern Matcher first tier.
`tier2_output_file.csv`	Contains the statistics for the Pattern Matcher second tier.

Syntax

```
ips stats -h
ips stats
ips stats <Seconds>
ips stats <IP Address of Gateway>
ips stats <IP Address of Gateway> <Seconds>
ips stats <IP Address of Gateway> -m
```

Important:

- To generate a report on a VSX Gateway, you must use the Manual Mode.
- On Scalable Platforms, you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`ips stats -h`	Shows the applicable built-in usage.
`ips stats`	Available only in Standalone configurations. Collects the IPS and Pattern Matcher statistics on the Standalone computer during 20 seconds.
`ips stats <Seconds>`	Available only in Standalone configurations. Collects the IPS and Pattern Matcher statistics on the Standalone computer during the specified number of seconds.
`ips stats <IP Address of Gateway>`	Collects the IPS and Pattern Matcher statistics for the Security Gateway with the main specified IP address during 20 seconds.
`ips stats <IP Address of Gateway> <Seconds>`	Collects the IPS and Pattern Matcher statistics for the Security Gateway with the main specified IP address during the specified number of seconds.
`ips stats <IP Address of Gateway> -m`	Available only on the Management Server. Runs an analysis on the output file `/ips_tar.tgz` that you collected from the Security Gateway with the main specified IP address.

Related SK article

sk43733: How to measure CPU time consumed by IPS protections.

Example 1 - Collect the statistics on the Security Gateway with IP address 192.168.20.14 during 40 seconds

```
ips stats 192.168.20.14 40
```

Example 2 - Analyze the statistics you collected from the Security Gateway with IP address 192.168.20.14

```
ips stats 192.168.20.14 -m
```

Monitoring Commands

For more information, see the *R81.20 Logging and Monitoring Administration Guide*.

This section contains commands for the **Monitoring** Software Blade (former SmartView Monitor) on the Security Gateway / each Cluster Member.

rtm

Description

Controls the **Monitoring** Software Blade (former SmartView Monitor) on the Security Gateway / each Cluster Member.

Shows the information about the **Monitoring** Software Blade.

Syntax

```
rtm
      debug <options>
      drv <options>
      monitor <options>
      rtmd
      stat <options>
      ver <options>
```

Note - "RTM" stands for Real Time Monitoring.

Parameters

Parameter	Description
No Parameters	Shows the built-in usage.
"rtm debug" on page 2006	Collects the SmartView Monitor debug information.
"rtm drv" on page 2007	Starts, stops, or shows the status of the SmartView Monitor kernel driver.
"rtm rtmd" on page 2008	Starts the SmartView Monitor daemon manually.
"rtm monitor" on page 2009	Starts the monitoring process for an interface or a virtual link.
"rtm stat" on page 2015	Shows information about the SmartView Monitor.
"rtm ver" on page 2018	Shows the SmartView Monitor version.

rtm debug

Description

Collects the SmartView Monitor debug information in the `$FWDIR/log/rtmd.elg` file on the Security Gateway / each Cluster Member.

Syntax

```
rtm debug {on | off} [OPSEC_DEBUG_LEVEL | TDERROR_<AppName>_
<Topic>=<ErrLevel>]
```

Parameters

Parameter	Description
`on`	Start debug mode
`off`	Stop debug mode
`OPSEC_DEBUG_LEVEL`	Turn on OPSEC debug printouts
`TDERROR_RTM_ALL`	Turn on SmartView Monitor debug printouts

Example

```
rtm debug on TDERROR_RTM_ALL=5
```

rtm drv

Description

Starts, stops, or shows the status of the SmartView Monitor kernel driver on the Security Gateway / each Cluster Member.

Important - Do not run this command manually. Run the *"rtmstart" on page 2019* and *"rtmstop" on page 2020* commands.

Syntax

```
rtm drv
      off
      on
      stat
```

Parameters

Parameter	Description
`on`	Starts the SmartView Monitor kernel driver
`off`	Stops the SmartView Monitor kernel driver
`stat`	Shows the SmartView Monitor kernel driver status

rtm rtmd

Description

Starts the SmartView Monitor daemon manually on the Security Gateway / each Cluster Member.

This also occurs manually when you run the *"rtmstart" on page 2019* command.

Syntax

```
rtm [-d] rtmd
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.

rtm monitor

Description

Starts the monitoring process for an interface or a Virtual Link on the Security Gateway / each Cluster Member.

If options and grouping are not used, this command monitors all traffic, on all interfaces, in both directions.

Syntax

```
rtm monitor vl <Virtual_Link_Name> [-t {wire | application}] [-h <Module>]
```

```
rtm monitor <Key_1> [<Key_2> [<Key_3>] [<Key_4>]] <Value_Column_1> [<Value_Column_2> [<Value_Column_3>] [<Value_Column_4>] [<Value_Column_5>] [<Value_Column_6>]] [<Filter>] [<Options>]
```

Parameters

Parameter	Description
No Parameters	Shows the built-in usage and examples.
<Virtual_Link_Name>	Specifies the name of the monitored Virtual Link.
`-t {wire | application}`	Specifies how to show the data: ■ `wire` - Shows the data on the wire after compression, or encryption. ■ `application` - Shows the data as the application sees it (not compressed and not encrypted).
`-h` *<Module>*	Specifies the Security Gateway by its IP address, or resolvable hostname.
<Key_1> `[...` `[`*<Key_4>*`]]`	Specifies up to four keys in this format: `-k` *<Key_Type>* `[`*<Key_Atrr>*`]` `[`*<Entity_1>* `...` *<Entity_N>*`]`

Parameter	Description
	The <*Key_Type*> can be one of these: ■ `connId` - Monitors according to a connection ID. ■ `dst` - Monitors according to a network object (destination only). ■ `fgrule` - Monitors according to a QoS Policy rule. ■ `fwrule` - Monitors according to an Access Control Policy rule. ■ `interface` - Monitors according to an interface. Use comma "," to specify the direction for the `interface` filter: `,{in|out|both}` Default is `both`. ■ `ip` - Monitors according to a network object (source and destination). ■ `orientation` - Monitors according to connection's direction. ■ `pktRange` - Monitors according to a range of packet sizes. ■ `src` - Monitors according to a network object (source only). ■ `svc` - Monitors according to a service (for example, `http`). ■ `tunnel` - Monitors according to a VPN tunnel. ■ `tunnelType` - Monitors according to a VPN tunnel type: • `0` - reserved • `1` - regular • `2` - permanent ■ `url [<URL_Mode>]` - Monitors according to a URL. The <*URL_Mode*> can be one of these: • `url_mod=full` (default) • `url_mod=host` • `url_mod=host_path` • `url_mod=path` • `url_mod=scheme` • `url_mod=scheme_host` ■ `wdAttack` - Monitors according to web defense attacks.
<Value_Column_1> [... [<Value_ Column_6>]]	Specifies up to six column values in this format: `-v <Value Type> [<Accumulate Mode>] [<Sort Mode>] [<Direction Filter>] [<Encryption Filter>]`

Parameter	Description
	■ The <*Value Type*> can be one of these: • ab - Shows application bytes • conn - Shows connections • pkt - Shows packets • session - Shows sessions • wb - Shows wire-bytes
	■ The <*Accumulate Mode*> can be one of these: • If <*Value Type*>=ab: ◦ acc=lineUtil ◦ acc=rate (default) ◦ acc=sum • If <*Value Type*>=conn: ◦ acc=concurrent (default) ◦ acc=new • If <*Value Type*>=pkt: ◦ acc=rate (default) ◦ acc=sum • If <*Value Type*>=session: ◦ acc=new • If <*Value Type*>=wb: ◦ acc=lineUtil ◦ acc=rate (default) ◦ acc=sum
	■ The <*Sort Mode*> can be one of these: • sort=top (default for all views) • sort=bottom • sort=none (default for specific views)
	■ The <*Direction Filter*> can be one of these: • dir=in • dir=out • dir=both (default)
	■ The <*Encryption Filter*> can be one of these: • enc=yes • enc=no • enc=both (default)

Parameter	Description

<Filter>	Specifies the filter that can be one of these:
	■ For the atom filter:
	`-f <Filter_Type> [not] [<Entity_1> ... <Entity_N>]`
	■ For the hierarchy filter:
	`-f {and | or} [...]`

	The *<Filter_Type>* can be one of these: ■ `connId` - Monitors according to a connection ID. ■ `dst` - Monitors according to a network object (destination only). ■ `fgrule` - Monitors according to a QoS Policy rule. ■ `fwrule` - Monitors according to an Access Control Policy rule. ■ `interface` - Monitors according to an interface. Use comma ",", to specify the direction for the `interface` filter: `,{in|out|both}` Default is `both`. ■ `ip` - Monitors according to a network object (source and destination). ■ `orientation` - Monitors according to connection's direction. ■ `src` - Monitors according to a network object (source only). ■ `svc` - Monitors according to a service (for example, `http`). ■ `tunnel` - Monitors according to a VPN tunnel. ■ `tunnelType` - Monitors according to a VPN tunnel type: • `0` - reserved • `1` - regular • `2`- permanent ■ `url [<URL_Mode>]` - Monitors according to a URL. The *<URL_Mode>* can be one of these: • `url_mod=full` (default) • `url_mod=host` • `url_mod=host_path` • `url_mod=path` • `url_mod=scheme` • `url_mod=scheme_host` ■ `wdAttack` - Monitors according to web defense attacks.

Parameter	Description
<Options>	Specifies these options: ■ `-e <Export File Name>` Specifies the path and the name of the file, in which the command saves its output. ■ `-h <Module>` Specifies the Security Gateway by its IP address, or resolvable hostname. Default is `localhost`. ■ `-i <Interval in Seconds>` The command runs in the loop and shows the output every specified number of seconds. Default is 2 sec. ■ `-m {raw | resolve | both}` Specifies how to resolve the names. Default is `both`. ■ `-s {top | bottom | none} [index=<1...6>] [updates=<1...200>]` Specifies how to sort the output. If you specify `none`, the defaults are: `index=1` and `updates=50`.

Notes

- Use the tilde character "~~" to specify a subrule (`rule~~subrule`).

  To monitor for the QoS Policy, use: `rule~~fgrule`

- The specified entities correspond to the specified grouping option.

  For example, if the monitoring process works according to a service (`svc`), add all the monitored services, separated by a space.

Examples

Example 1

This command shows top services (based on bytes per seconds) on external interfaces in the inbound direction:

```
rtm monitor -f interface external,in -k svc -v wb
```

Example 2

This command shows top Access Control rules (based on average concurrent connections):

```
rtm monitor -k fwrule -v conn acc=concurrent
```

Example 3

This command shows Individual HTTP connections (bytes per second):

```
rtm monitor -f svc http -k svc -k connId -v wb
```

Example 4

This command shows bottom inbound IP addresses versus outbound IP addresses (based on packets per interval):

```
rtm monitor -k ip -v pkt dir=in acc=sum -v pkt dir=out acc=sum -
v pkt acc=sum sort=bottom -i 10
```

Example 5

This command shows top tunnels (based on average concurrent connections):

```
rtm monitor -f tunnelType not 0 -k tunnel -k tunnelType -v conn
-m resolve
```

Example 6

This command shows packet size distribution (based on packets per interval):

```
rtm monitor -k pktRange 0-99 100-499 500-999 1000-1999 ">2000" -
v pkt acc=sum -i 1
```

Example 7

This command shows top URLs (based on sessions per seconds) - host part only:

```
rtm monitor -k url url_mod=host -v session
```

rtm stat

Description

Show this information on the Security Gateway / each Cluster Member:

- The status of the Monitoring Software Blade
- The status of the SmartView Monitor daemon
- The status of the SmartView Monitor driver
- Number of opened Virtual Links
- Number of opened Views
- Some performance counters

Syntax

```
rtm stat -h
```

```
rtm stat [vl | view] [perf [{on | off | reset}] [-i <Interval>] [-r <View_ID>] [-v[v][v]]
```

Parameters

Parameter	Description
`-h`	Shows the built-in usage.
`vl`	Shows current Virtual Links
`view`	Shows current Views
`perf [{off | on | reset}]`	Controls whether to show performance information: ■ `off` - Disables the feature ■ `on` - Enables the feature ■ `reset` - Resets the counters The output shows these performance counters: ■ `New Connections` ■ `Packets` ■ `Inf Reclassify` ■ `View Reclassify` ■ `End Connections` ■ `Packets / connections ratio`

Parameter	Description
`-i <Interval>`	The command runs in the loop and shows the output every specified number of seconds.
`-r <View_ID>`	Specifies the View ID to show.
`-v[v][v]`	Verbose output: ■ `-v` - Verbose output ■ `-vv` - More verbose output ■ `-vvv` - Most verbose output

Examples

Example 1

```
[Expert@MyGW:0]# rtm stat
-------------------------------------------------------
SmartView Monitor Status:   Sun Mar 20 18:25:51 2022
-------------------------------------------------------
Product is Enabled
Daemon is ON
-------------------------------------------------------
Status for kernel instance 0
-------------------------------------------------------
Driver is ON
Open Virtual-Links: 0
Open Views: 0
-------------------------------------------------------
Status for kernel instance 1
-------------------------------------------------------
Driver is ON
Open Virtual-Links: 0
Open Views: 0
-------------------------------------------------------
Status for kernel instance ...
-------------------------------------------------------
... (truncated for brevity) ...
[Expert@MyGW:0]#
```

Example 2

```
[Expert@MyGW:0]# rtm stat view -vvv
-----------------------------------------------------
SmartView Monitor Status:   Sun Mar 20 18:25:51 2022
-----------------------------------------------------
Product is Enabled
Daemon is ON
-----------------------------------------------------
Status for kernel instance 0
-----------------------------------------------------
Driver is ON
Open Virtual-Links: 0
Open Views: 0
-----------------------------------------------------
Status for kernel instance 1
-----------------------------------------------------
Driver is ON
Open Virtual-Links: 0
Open Views: 0
-----------------------------------------------------
Status for kernel instance ...
-----------------------------------------------------
... (truncated for brevity) ...
-------------------------------------------------------------------
---------------------------
VIEW 1:  svc             |  wb(rate)     interval: 2   Seconds
         60016,60016     |  5148
         11008a,11008a   |  229
         Aggregate       |  5377

         Number of Entries(2)
         Keys(-k svc acc=replace )
         Values(-v wb acc=rate )
         Sort(-s top )
         Filter(-)
         Daemon id:5        kernel id:0 timeUntilUpdate: 1 [Sec]
-------------------------------------------------------------------
---------------------------
[Expert@MyGW:0]#
```

rtm ver

Description

Shows the SmartView Monitor version on the Security Gateway / each Cluster Member.

Syntax

```
rtm ver [-k]
```

Parameters

Parameter	Description
`-k`	Shows the SmartView Monitor kernel version.

rtmstart

Description

Loads the SmartView Monitor kernel module and starts the SmartView Monitor daemon on the Security Gateway / each Cluster Member.

Syntax

```
rtmstart
```

rtmstop

Description

Kills the SmartView Monitor daemon and unloads the SmartView Monitor kernel module on the Security Gateway / each Cluster Member.

Syntax

```
rtmstop
```

Working with Kernel Parameters

See the *R81.20 Security Gateway Guide* > Chapter "Working with Kernel Parameters".

Running Check Point Commands in Shell Scripts

To run Check Point commands in your shell scripts, it is necessary to add the calls to the required Check Point shell scripts.

You must add these calls below the top line "`#!/bin/bash`".

On a Security Management Server / Log Server / SmartEvent Server

You must add the call to the `/etc/profile.d/CP.sh` script.

```
#!/bin/bash

source /etc/profile.d/CP.sh

<Applicable Check Point Commands>

[mandatory last new line]
```

On a Multi-Domain Server / Multi-Domain Log Server

You must add the calls to these scripts (in the order listed below):

1. `/etc/profile.d/CP.sh`
2. `$MDSDIR/scripts/MDSprofile.sh`
3. `$MDS_SYSTEM/shared/mds_environment_utils.sh`
4. `$MDS_SYSTEM/shared/sh_utilities.sh`

```
#!/bin/bash

source /etc/profile.d/CP.sh
source $MDSDIR/scripts/MDSprofile.sh
source $MDS_SYSTEM/shared/mds_environment_utils.sh
source $MDS_SYSTEM/shared/sh_utilities.sh

<Applicable Check Point Commands>

[mandatory last new line]
```

On a Security Gateway / Cluster Members (non-VSX)

You must add the call to the `/etc/profile.d/CP.sh` script.

```
#!/bin/bash

source /etc/profile.d/CP.sh

<Applicable Check Point Commands>

[mandatory last new line]
```

On a VSX Gateway / VSX Cluster Members

You must add the calls to these scripts (in the order listed below):

1. `/etc/profile.d/CP.sh`
2. `/etc/profile.d/vsenv.sh`

```
#!/bin/bash

source /etc/profile.d/CP.sh
source /etc/profile.d/vsenv.sh

<Applicable Check Point Commands>

[mandatory last new line]
```

Glossary

#

3rd-party Cluster
Cluster of Check Point Firewalls that work together in a redundant configuration. These Check Point Firewalls are installed on an operating system other than [%Vars_Other.r_gaia%]. VRRP Cluster on [%Vars_Other.r_gaia%] OS is also considered a 3rd-party cluster. The 3rd-party cluster handles the traffic, and Check Point Firewalls perform only State Synchronization.

A

Accelerated Path
Packet flow on the Host appliance, when the packet is completely handled by the SecureXL device. It is processed and forwarded to the network.

Access Role
Access Role objects let you configure network access according to: Networks, Users and user groups, Computers and computer groups, Remote Access Clients. After you activate the Identity Awareness Software Blade, you can create Access Role objects and use them in the Source and Destination columns of Access Control Policy rules.

Active
State of a Cluster Member that is fully operational: (1) In ClusterXL, this applies to the state of the Check Point Firewall (2) In 3rd-party / OPSEC cluster, this applies to the state of the cluster State Synchronization mechanism.

Active-Active
A cluster mode (in versions R80.40 and higher), where Cluster Members are located in different geographical areas (different sites, different cloud availability zones). This mode supports the configuration of IP addresses from different subnets on all cluster interfaces, including the Sync interfaces. Each Cluster Member inspects all traffic routed to it and synchronizes the recorded connections to its peer Cluster Members. The traffic is not balanced between the Cluster Members.

Active Domain Server
The only Domain Management Server in a Management High Availability deployment that can manage a specified Domain.

Active Security Management Server
The Management Server in Management High Availability that is currently configured as Active.

Active Up
ClusterXL in High Availability mode that was configured as Maintain current active Cluster Member in the cluster object in SmartConsole: (1) If the current Active member fails for some reason, or is rebooted (for example, Member_A), then failover occurs between Cluster Members - another Standby member will be promoted to be Active (for example, Member_B). (2) When former Active member (Member_A) recovers from a failure, or boots, the former Standby member (Member_B) will remain to be in Active state (and Member_A will assume the Standby state).

Active(!)
In ClusterXL, state of the Active Cluster Member that suffers from a failure. A problem was detected, but the Cluster Member still forwards packets, because it is the only member in the cluster, or because there are no other Active members in the cluster. In any other situation, the state of the member is Down. Possible states: ACTIVE(!), ACTIVE(!F) - Cluster Member is in the freeze state, ACTIVE(!P) - This is the Pivot Cluster Member in the Load Sharing Unicast mode, ACTIVE(!FP) - This is the Pivot Cluster Member in the Load Sharing Unicast mode and it is in the freeze state.

AD Query
Check Point clientless identity acquisition tool. It is based on Active Directory integration and it is completely transparent to the user. The technology is based on querying the Active Directory Security Event Logs and extracting the user and computer mapping to the network address from them. It is based on Windows Management Instrumentation (WMI), a standard Microsoft protocol. The Check Point Firewall with Identity Awareness enabled communicates directly with the Active Directory domain controllers and does not require a separate server. No installation is necessary on the clients, or on the Active Directory server.

Affinity
The assignment of a specified CoreXL Firewall instance, Traditional VSX Virtual System, interface, user space process, or IRQ to one or more specified CPU cores.

Anti-Bot
Software Blade on a Check Point Firewall that blocks botnet behavior and communication to Command and Control (C&C) centers. Acronyms: AB, ABOT.

Anti-Spam
Software Blade on a Check Point Firewall that provides comprehensive protection for email inspection. Synonym: Anti-Spam & Email Security. Acronyms: AS, ASPAM.

Anti-Virus
Software Blade on a Check Point Firewall that uses real-time virus signatures and anomaly-based protections from ThreatCloud to detect and block malware at the Check Point Firewall before users are affected. Acronym: AV.

Application Control
Software Blade on a Check Point Firewall that allows granular control over specific web-enabled applications by using deep packet inspection. Acronym: APPI.

ARP Forwarding
Forwarding of ARP Request and ARP Reply packets between Cluster Members by encapsulating them in Cluster Control Protocol (CCP) packets. Introduced in R80.10 version.

Ask
UserCheck rule action that blocks traffic and files and shows a UserCheck message. The user can agree to allow the activity.

Audit Log
Log that contains administrator actions on a Management Server (login and logout, creation or modification of an object, installation of a policy, and so on).

B

Backup
(1) In VRRP Cluster on Gaia OS - State of a Cluster Member that is ready to be promoted to Master state (if Master member fails). (2) In Traditional VSX Cluster configured in the Virtual System Load Sharing mode with three or more Cluster Members - State of a Virtual System on a third (and so on) Traditional VSX Cluster Member. (3) A Cluster Member or Virtual System in this state does not process any traffic passing through cluster.

Blocking Mode
Cluster operation mode, in which Cluster Member does not forward any traffic (for example, caused by a failure).

Bot
Malicious software that neutralizes Anti-Virus defenses, connects to a Command and Control center for instructions from cyber criminals, and carries out the instructions.

Bridge Mode
Check Point Firewall or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

Browser-Based Authentication
Authentication of users in Check Point Identity Awareness web portal - Captive Portal, to which users connect with their web browser to log in and authenticate.

Burstiness
Data that is transferred or transmitted in short, uneven spurts. LAN traffic is typically bursty. Opposite of streaming data.

C

Captive Portal
A Check Point Identity Awareness web portal, to which users connect with their web browser to log in and authenticate, when using Browser-Based Authentication.

Check Point Firewall
Dedicated Check Point server that runs Check Point software to inspect traffic and enforce Security Policies for connected network resources. Formerly: Security Gateway.

Cloud Credentials
Specific credentials from identity providers used by the Identity Collector to connect seamlessly to the Check Point Portal. These credentials are essential for establishing a secure and efficient connection between the Identity Client and the Check Point Portal.

Cloud Services
Refers to a centralized identities solution provided by Identity and Trust and Directory Sync. These services offer identity management and directory synchronization capabilities, hosted and managed in the cloud.

Cluster
Two or more Check Point Firewalls that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Control Protocol
Proprietary Check Point protocol that runs between Cluster Members on UDP port 8116, and has the following roles: (1) State Synchronization (Delta Sync), (2) Health checks (state of Cluster Members and of cluster interfaces): Health-status Reports, Cluster-member Probing, State-change Commands, Querying for cluster membership. Note: CCP is located between the Check Point Firewall kernel and the network interface (therefore, only TCPdump should be used for capturing this traffic). Acronym: CCP.

Cluster Correction Layer
Proprietary Check Point mechanism that deals with asymmetric connections in Check Point cluster. The CCL provides connections stickiness by "correcting" the packets to the correct Cluster Member: In most cases, the CCL makes the correction from the CoreXL SND. In some cases (like Dynamic Routing, or VPN), the CCL makes the correction from the Firewall or SecureXL. Acronym: CCL.

Cluster Interface
An interface on a Cluster Member, whose Network Type was set as Cluster in SmartConsole in cluster object. This interface is monitored by cluster, and failure on this interface will cause cluster failover.

Cluster Member
Check Point Firewall that is part of a cluster.

Cluster Mode
Configuration of Cluster Members to work in these redundant modes: (1) One Cluster Member processes all the traffic - High Availability or VRRP mode (2) All traffic is processed in parallel by all Cluster Members - Load Sharing.

Cluster Topology
Set of interfaces on all members of a cluster and their settings (Network Objective, IP address / Net Mask, Topology, Anti-Spoofing, and so on).

ClusterXL
Cluster of Check Point Firewalls that work together in a redundant configuration. The ClusterXL both handles the traffic and performs State Synchronization. These Check Point Firewalls are installed on Gaia OS: (1) ClusterXL supports up to 5 Cluster Members, (2) VRRP Cluster supports up to 2 Cluster Members, (3) Traditional VSX VSLS Cluster supports up to 13 Cluster Members. Note: In the ClusterXL Load Sharing mode, configuring more than 4 Cluster Members significantly decreases the cluster performance due to amount of Delta Sync traffic.

Compliance
Software Blade on a Management Server to view and apply the Security Best Practices to the managed Check Point Firewalls. This Software Blade includes a library of Check Point-defined Security Best Practices to use as a baseline for good Check Point Firewall and Policy configuration.

Content Awareness
Software Blade on a Check Point Firewall that provides data visibility and enforcement. Acronym: CTNT.

Cooperative Enforcement
Integration of an on-premises Endpoint Security Management Server and Check Point Firewall.

CoreXL
Performance-enhancing technology for Check Point Firewalls on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

CoreXL Dynamic Dispatcher
Improved CoreXL SND feature. Part of CoreXL that distributes packets between CoreXL Firewall instances. Traffic distribution between CoreXL Firewall instances is dynamically based on the utilization of CPU cores, on which the CoreXL Firewall instances are running. The dynamic decision is made for first packets of connections, by assigning each of the CoreXL Firewall instances a rank, and selecting the CoreXL Firewall instance with the lowest rank. The rank for each CoreXL Firewall instance is calculated according to its CPU utilization. The higher the CPU utilization, the higher the CoreXL Firewall instance's rank is, hence this CoreXL Firewall instance is less likely to be selected by the CoreXL SND.

CoreXL Firewall Instance
On a Check Point Firewall with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel. Synonym: CoreXL FW Instance.

CoreXL SND
Secure Network Distributor. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

CPHA
General term in Check Point Cluster that stands for Check Point High Availability (historic fact: the first release of ClusterXL supported only the High Availability mode) that is used only for internal references (for example, inside kernel debug) to designate ClusterXL infrastructure.

CPUSE
Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself.

Critical Device
A special software device on each Cluster Member, through which the critical aspects for cluster operation are monitored. When the critical monitored component on a Cluster Member fails to report its state on time, or when its state is reported as problematic, the state of that member is immediately changed to Down. The complete list of the configured critical devices (pnotes) is printed by the 'cphaprob -ia list' command or 'show cluster members pnotes all' command. Synonyms: Pnote, Problem Notification.

Custom Report
User-defined report for a Check Point product, typically based on a predefined report.

D

DAIP Firewall
Check Point Firewall with a Dynamically Assigned IP (DAIP) is a server, on which the IP address of the external interface is assigned dynamically (by a DHCP server, by an ISP).

Data Loss Prevention
Software Blade on a Check Point Firewall that detects and prevents the unauthorized transmission of confidential information outside the organization. Acronym: DLP.

Data Type
Classification of data in a Check Point Security Policy for the Content Awareness Software Blade.

Dead
State reported by a Cluster Member when it goes out of the cluster (due to 'cphastop' command (which is a part of 'cpstop'), or reboot).

Decision Function
A special cluster algorithm applied by each Cluster Member on the incoming traffic in order to decide, which Cluster Member should process the received packet. Each Cluster Member maintains a table of hash values generated based on connections tuple (source and destination IP addresses/Ports, and Protocol number).

Dedicated Management Interface
Separate physical interface on Traditional VSX Gateway or Traditional VSX Cluster Members, through which Check Point Security Management Server or Multi-Domain Security Management Server connects directly to Traditional VSX Gateway or Traditional VSX Cluster Members. DMI is restricted to management traffic, such as provisioning, logging and monitoring. Acronym: DMI.

Delta Sync
Synchronization of kernel tables between all working Cluster Members - exchange of CCP packets that carry pieces of information about different connections and operations that should be performed on these connections in relevant kernel tables. This Delta Sync process is performed directly by Check Point kernel. While performing Full Sync, the Delta Sync updates are not processed and saved in kernel memory. After Full Sync is complete, the Delta Sync packets stored during the Full Sync phase are applied by order of arrival.

Delta Sync Retransmission
It is possible that Delta Sync packets will be lost or corrupted during the Delta Sync operations. In such cases, it is required to make sure the Delta Sync packet is re-sent. The Cluster Member requests the sending Cluster Member to retransmit the lost/corrupted Delta Sync packet. Each Delta Sync packet has a sequence number. The sending member has a queue of sent Delta Sync packets. Each Cluster Member has a queue of packets sent from each of the peer Cluster Members. If, for any reason, a Delta Sync packet was not received by a Cluster Member, it can ask for a retransmission of this packet from the sending member. The Delta Sync retransmission mechanism is somewhat similar to a TCP Window and TCP retransmission mechanism. When a member requests retransmission of Delta Sync packet, which no longer exists on the sending member, the member prints a console messages that the sync is not complete.

Detect
UserCheck rule action that allows traffic and files to enter the internal network and logs them.

Directory Sync
A solution that holds static Directory information regarding users, groups, devices, and memberships. .

Distributed Deployment
Configuration in which the Check Point Firewall and the Security Management Server products are installed on different servers.

Domain Dedicated Log Server
Dedicated Log Server (not a Domain Log Server) configured in a specified Domain (in versions R81 and higher). It stores and processes logs from Check Point Firewalls that are managed by the corresponding Domain Management Server. Acronym: DDLS.

Domain Dedicated SmartEvent Server
Dedicated SmartEvent Server configured in a specified Domain (in versions R81 and higher). It hosts the events database for logs from Check Point Firewalls that are managed by the corresponding Domain Management Server.

Domain Management Server
Virtual Security Management Server that manages Check Point Firewalls for one Domain, as part of a Multi-Domain Security Management environment. Acronym: DMS.

Down
State of a Cluster Member during a failure when one of the Critical Devices reports its state as "problem": In ClusterXL, applies to the state of the Check Point Firewall; in 3rd-party / OPSEC cluster, applies to the state of the State Synchronization mechanism. A Cluster Member in this state does not process any traffic passing through cluster.

Dying
State of a Cluster Member as assumed by peer members, if it did not report its state for 0.7 second.

Dynamic Object
Special object type, whose IP address is not known in advance. The Check Point Firewall resolves the IP address of this object in real time.

E

Encryption Domain
The networks that a Check Point Firewall protects and for which it encrypts and decrypts VPN traffic.

Endpoint Policy Management
Software Blade on a Management Server to manage an on-premises Endpoint Security environment.

Event
Record of a security or network incident that is based on one or more logs, and on a customizable set of rules that are defined in the Event Policy.

Event Correlation
Procedure that extracts, aggregates, correlates, and analyzes events from the logs.

Event Policy
Set of rules that define the behavior of SmartEvent.

Expert Mode
The name of the elevated command line shell that gives full system root permissions in the Check Point Gaia operating system.

F

F2F
Denotes non-VPN connections that SecureXL forwarded to firewall. See "Firewall Path".

Failback
Recovery of a Cluster Member that suffered from a failure. The state of a recovered Cluster Member is changed from Down to either Active, or Standby (depending on the Cluster Mode). Synonym: Fallback.

Failed Member
A Cluster Member that cannot send or accept traffic because of a hardware or software problem.

Failover
Transferring of a control over traffic (packet filtering) from a Cluster Member that suffered a failure to another Cluster Member (based on internal cluster algorithms). Synonym: Fail-over.

Failure
A hardware or software problem that causes a Check Point Firewall to be unable to serve as a Cluster Member (for example, one of cluster interface has failed, or one of the monitored daemon has crashed). Cluster Member that suffered from a failure is declared as failed, and its state is changed to Down (a physical interface is considered Down only if all configured VLANs on that physical interface are Down).

Firewall Path
Packet flow on the Host Security Appliance, when the SecureXL device is unable to process the packet. The packet is passed to the CoreXL layer and then to one of the CoreXL Firewall instances for full processing. This path also processes all packets when SecureXL is disabled. Synonym: Slow Path.

Flapping
Consequent changes in the state of either cluster interfaces (cluster interface flapping), or Cluster Members (Cluster Member flapping). Such consequent changes in the state are seen in the 'Logs & Monitor' > 'Logs' (if in SmartConsole > cluster object, the cluster administrator set the 'Track changes in the status of cluster members' to 'Log').

Flush and ACK

Cluster Member forces the Delta Sync packet about the incoming packet and waiting for acknowledgments from all other Active members and only then allows the incoming packet to pass through. In some scenarios, it is required that some information, written into the kernel tables, will be Sync-ed promptly, or else a race condition can occur. The race condition may occur if a packet that caused a certain change in kernel tables left Member_A toward its destination and then the return packet tries to go through Member_B. In general, this kind of situation is called asymmetric routing. What may happen in this scenario is that the return packet arrives at Member_B before the changes induced by this packet were Sync-ed to this Member_B. Example of such a case is when a SYN packet goes through Member_A, causing multiple changes in the kernel tables and then leaves to a server. The SYN-ACK packet from a server arrives at Member_B, but the connection itself was not Sync-ed yet. In this condition, the Member_B will drop the packet as an Out-of-State packet (First packet isn't SYN). In order to prevent such conditions, it is possible to use the "Flush and ACK" (F&A) mechanism. This mechanism can send the Delta Sync packets with all the changes accumulated so far in the Sync buffer to the other Cluster Members, hold the original packet that induced these changes and wait for acknowledgment from all other (Active) Cluster Members that they received the information in the Delta Sync packet. When all acknowledgments arrived, the mechanism will release the held original packet. This ensures that by the time the return packet arrived from a server at the cluster, all the Cluster Members are aware of the connection. F&A is being operated at the end of the Inbound chain and at the end of the Outbound chain (it is more common at the Outbound). Synonyms: FnA, F&A.

Forwarding

Process of transferring of an incoming traffic from one Cluster Member to another Cluster Member for processing. There are two types of forwarding the incoming traffic between Cluster Members - Packet forwarding and Chain forwarding. For more information, see "Forwarding Layer in Cluster" and "ARP Forwarding".

Forwarding Layer

The Forwarding Layer is a ClusterXL mechanism that allows a Cluster Member to pass packets to peer Cluster Members, after they have been locally inspected by the firewall. This feature allows connections to be opened from a Cluster Member to an external host. Packets originated by Cluster Members are hidden behind the Cluster Virtual IP address. Thus, a reply from an external host is sent to the cluster, and not directly to the source Cluster Member. This can pose problems in the following situations: (1) The cluster is working in High Availability mode, and the connection is opened from the Standby Cluster Member. All packets from the external host are handled by the Active Cluster Member, instead. (2) The cluster is working in a Load Sharing mode, and the decision function has selected another Cluster Member to handle this connection. This can happen since packets directed at a Cluster IP address are distributed between Cluster Members as with any other connection. If a Cluster Member decides, upon the completion of the firewall inspection process, that a packet is intended for another Cluster Member, it can use the Forwarding Layer to hand the packet over to that Cluster Member. In the High Availability mode, packets are forwarded over a Synchronization network directly to peer Cluster Members. It is important to use secured networks only, as encrypted packets are decrypted during the inspection process, and are forwarded as clear-text (unencrypted) data. In the Load Sharing mode, packets are forwarded over a regular traffic network. Packets that are sent on the Forwarding Layer use a special source MAC address to inform the receiving Cluster Member that they have already been inspected by another Cluster Member. Thus, the receiving Cluster Member can safely hand over these packets to the local Operating System, without further inspection.

Full High Availability

A special Cluster Mode supported only on Check Point appliances running Gaia OS (R75.40 and higher) or SecurePlatform OS (R77.30 and lower), where each Cluster Member also runs as a Security Management Server. This provides redundancy both between Check Point Firewalls (only the High Availability mode is supported) and between Security Management Servers (only the High Availability mode is supported). Synonyms: Full HA Cluster Mode, Full HA, FullHA.

Full Sync
Process of full synchronization of applicable kernel tables by a Cluster Member from the working Cluster Member(s) when it tries to join the existing cluster. This process is meant to fetch a "snapshot" of the applicable kernel tables of already Active Cluster Member(s). Full Sync is performed during the initialization of Check Point software (during boot process, the first time the Cluster Member runs policy installation, during 'cpstart', during 'cphastart'). Until the Full Sync process completes successfully, this Cluster Member remains in the Down state, because until it is fully synchronized with other Cluster Members, it cannot function as a Cluster Member. Meanwhile, the Delta Sync packets continue to arrive, and the Cluster Member that tries to join the existing cluster, stores them in the kernel memory until the Full Sync completes. The whole Full Sync process is performed by fwd daemons on TCP port 256 over the Sync network (if it fails over the Sync network, it tries the other cluster interfaces). The information is sent by fwd daemons in chunks, while making sure they confirm getting the information before sending the next chunk. Also see "Delta Sync".

G

Gaia
Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

Gaia Clish
The name of the default command line shell in Check Point Gaia operating system. This is a restricted shell (role-based administration controls the number of commands available in the shell).

Gaia Portal
Web interface for the Check Point Gaia operating system.

Geo Cluster
A High Availability cluster mode (in versions R81.20 and higher), where Cluster Members are located in different cloud availability zones. This mode supports the configuration of IP addresses from different subnets on all cluster interfaces, including the Sync interfaces. The Active Cluster Member inspects all traffic routed to the cluster and synchronizes the recorded connections to its peer Cluster Members. The traffic is not balanced between the Cluster Members. See "High Availability".

Global Domain
Domain on a Multi-Domain Security Management Server, on which the Multi-Domain Security Management Server administrator creates and manages objects, security policies and settings that apply to the entire Multi-Domain Security Management environment.

Global Objects
On a Multi-Domain Security Management Server, all objects defined in the Global Domain. You can use this objects in a Global Policy or Local Policies on Domains.

Global Policy
On a Multi-Domain Security Management Server, a policy defined in the Global Domain. You can assigns this Global Policy to Domains.

H

HA not started
Output of the 'cphaprob <flag>' command or 'show cluster <option>' command on the Cluster Member. This output means that Check Point clustering software is not started on this Check Point Firewall (for example, this machine is not a part of a cluster, or 'cphastop' command was run, or some failure occurred that prevented the ClusterXL product from starting correctly).

High Availability
A redundant cluster mode, where only one Cluster Member (Active member) processes all the traffic, while other Cluster Members (Standby members) are ready to be promoted to Active state if the current Active member fails. In the High Availability mode, the Cluster Virtual IP address (that represents the cluster on that network) is associated: (1) With physical MAC Address of Active member (2) With virtual MAC Address. Synonym: Active/Standby. Acronym: HA.

Hotfix
Software package installed on top of the current software version to fix a wrong or undesired behavior, and to add a new behavior.

HTTPS Inspection
Feature on a Check Point Firewall that inspects traffic encrypted by the Secure Sockets Layer (SSL) protocol for malware or suspicious patterns. Synonym: SSL Inspection. Acronyms: HTTPSI, HTTPSi.

HTU
Stands for "HA Time Unit". All internal time in ClusterXL is measured in HTUs (the times in cluster debug also appear in HTUs). Formula in the Check Point software: 1 HTU = 10 x fwha_timer_base_res = 10 x 10 milliseconds = 100 ms.

Hybrid
Starting in R80.20, on Check Point Firewalls with 40 or more CPU cores, Software Blades run in the user space (as 'fwk' processes). The Hybrid Mode refers to the state when you upgrade Cluster Members from R80.10 (or lower) to R80.20 (or higher). The Hybrid Mode is the state, in which the upgraded Cluster Members already run their Software Blades in the user space (as "fwk" processes), while other Cluster Members still run their Software Blades in the kernel space (represented by the fw_worker processes). In the Hybrid Mode, Cluster Members are able to synchronize the required information.

I

ICA
Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

ICAP Client
The ICAP Client functionality in a Check Point Firewall that enables it to interact with an ICAP Server responses (see RFC 3507), modify their content, and block the matched HTTP connections.

ICAP Server
The ICAP Server functionality in a Check Point Firewall that enables it to interact with an ICAP Client requests, send the files for inspection, and return the verdict.

Identity Agent
Check Point dedicated client agent installed on Windows-based user endpoint computers. This Identity Agent acquires and reports identities to the Check Point Firewall with Identity Awareness enabled. The administrator configures the Identity Agents (not the end users). There are two types of Identity Agents - Full and Light. You can download the Full and Light Identity Agent package from the Captive Portal - 'https://<Gateway_IP_Address>/connect' or from Support Center.

Identity Agent Configuration Utility
Check Point utility that creates custom Identity Agent installation packages. This utility is installed as a part of the Identity Agent: go to the Windows Start menu > All Programs > Check Point > Identity Agent > open the 'Identity Agent' shortcut > select 'Properties' > click 'Open File Location' ('Find Target' in some Windows versions > double-click 'IAConfigTool.exe').

Identity Agent Distributed Configuration Tool
Check Point Identity Agent control tool for Windows-based client computers that are members of an Active Directory domain. The Distributed Configuration tool lets you configure connectivity and trust rules for Identity Agents - to which [[[Undefined variable Vars_BladesFeatures.tp_cpfws]]] the Identity Agent should connect, depending on its IPv4 / IPv6 address, or Active Directory Site. This tool is installed a part of the Identity Agent: go to the Windows Start menu > All Programs > Check Point > Identity Agent > open 'Distributed Configuration'. Note - You must have administrative access to this Active Directory domain to allow automatic creation of new LDAP keys and writing.

Identity Awareness
Software Blade on a Check Point Firewall that enforces network access and audits data based on network location, the identity of the user, and the identity of the computer. Acronym: IDA.

Identity Broker
Identity Sharing mechanism between Identity Servers (PDP): (1) Communication channel between PDPs based on Web-API (2) Identity Sharing capabilities between PDPs - ability to add, remove, and update the identity session.

Identity Collector
Check Point dedicated client agent installed on Windows Servers in your network. Identity Collector collects information about identities and their associated IP addresses and sends it to the Check Point Firewalls for identity enforcement, you can download the Identity Collector package from the Support Center.

Identity Collector Identity Sources
Identity Sources for Check Point Identity Collector - Microsoft Active Directory Domain Controllers, Cisco [[[Undefined variable Vars_BladesFeatures.tp_cisco_ise_full]]] ([[[Undefined variable Vars_BladesFeatures.tp_cisco_ise]]]) Servers, or NetIQ eDirectory Servers.

Identity Collector Query Pool
A list of Identity Sources for Check Point Identity Collector.

Identity Logging
Software Blade on a Management Server to view Identity Logs from the managed Check Point Firewalls with enabled Identity Awareness Software Blade.

Identity Server
Check Point Firewall with enabled Identity Awareness Software Blade.

Indicator
Pattern of relevant observable malicious activity in an operational cyber domain, with relevant information on how to interpret it and how to handle it.

Init
State of a Cluster Member in the phase after the boot and until the Full Sync completes. A Cluster Member in this state does not process any traffic passing through cluster.

Inline Layer
Set of rules used in another rule in Security Policy.

Intelligent Queuing Engine
A bandwidth allocation algorithm that guarantees high priority traffic takes precedence over low priority traffic.

Internal Network
Computers and resources protected by the Firewall and accessed by authenticated users.

IoC
Indicator of Compromise. Artifact observed on a network or in an operating system that, with high confidence, indicates a computer intrusion. Typical IoCs are virus signatures and IP addresses, MD5 hashes of Malware files, or URLs or domain names of botnet command and control servers. Identified through a process of incident response and computer forensics, intrusion detection systems and anti-virus software can use IoC's to detect future attacks.

IP Tracking
Collecting and saving of Source IP addresses and Source MAC addresses from incoming IP packets during the probing. IP tracking is a useful for Cluster Members to determine whether the network connectivity of the Cluster Member is acceptable.

IP Tracking Policy
Internal setting that controls, which IP addresses should be tracked during IP tracking: (1) Only IP addresses from the subnet of cluster VIP, or from subnet of physical cluster interface (this is the default) (2) All IP addresses, also outside the cluster subnet.

IPS
Software Blade on a Check Point Firewall that inspects and analyzes packets and data for numerous types of risks (Intrusion Prevention System).

IPsec VPN
Software Blade on a Check Point Firewall that provides a Site to Site VPN and Remote Access VPN access.

IRQ Affinity
A state of binding an IRQ to one or more CPU cores.

J

Jitter
Variation in the delay of received packets. On the sending side, packets are spaced evenly apart and sent in a continuous stream. On the receiving side, the delay between each packet can vary according to network congestion, improper queuing or configuration errors.

Jumbo Hotfix Accumulator
Collection of hotfixes combined into a single package. Acronyms: JHA, JHF, JHFA.

K

Kerberos
An authentication server for Microsoft Windows Active Directory Federation Services (ADFS).

L

LLQ
Low Latency Queuing is a feature developed by Cisco to bring strict priority queuing (PQ) to class-based weighted fair queuing (CBWFQ). LLQ allows delay-sensitive data (such as voice) to be given preferential treatment over other traffic by letting the data to be dequeued and sent first.

Load Sharing
A redundant cluster mode, where all Cluster Members process all incoming traffic in parallel. For more information, see "Load Sharing Multicast Mode" and "Load Sharing Unicast Mode". Synonyms: Active/Active, Load Balancing mode. Acronym: LS.

Load Sharing Multicast
Load Sharing Cluster Mode, where all Cluster Members process all traffic in parallel. Each Cluster Member is assigned the equal load of [100% / number_of_members]. The Cluster Virtual IP address (that represents the cluster on that network) is associated with Multicast MAC Address 01:00:5E:X:Y:Z (which is generated based on last 3 bytes of cluster Virtual IP address on that network). A ClusterXL decision algorithm (Decision Function) on all Cluster Members decides, which Cluster Member should process the given packet.

Load Sharing Unicast
Load Sharing Cluster Mode, where one Cluster Member (called Pivot) accepts all traffic. Then, the Pivot member decides to process this traffic, or to forward it to other non-Pivot Cluster Members. The traffic load is assigned to Cluster Members based on the hard-coded formula per the value of "Pivot_overhead" attribute in the cluster object. The Cluster Virtual IP address (that represents the cluster on that network) is associated with: (1) Physical MAC Address of Pivot member (2) Virtual MAC Address.

Log Server
Dedicated Check Point server that runs Check Point software to store and process logs.

Logging & Status
Software Blade on a Management Server to view Security Logs from the managed Check Point Firewalls.

M

Mail Transfer Agent
Feature on a Check Point Firewall that intercepts SMTP traffic and forwards it to the applicable inspection component. Acronym: MTA.

Main Domain Management Server
Domain Management Server on a Multi-Domain Security Management Server, on which you configured the object of your Traditional VSX Gateway or Traditional VSX Cluster. In this case, objects of your Virtual Systems are defined on different Domain Management Servers (Target Domain Management Servers).

Malware Database
The Check Point database of commonly used signatures, URLs, and their related reputations, installed on a Check Point Firewall and used by the ThreatSpect engine.

Management High Availability
Deployment and configuration mode of two Check Point Management Servers, in which they automatically synchronize the management databases with each other. In this mode, one Management Server is Active, and the other is Standby. Acronyms: Management HA, MGMT HA.

Management Interface
(1) Interface on a Gaia Check Point Firewall or Cluster Member, through which Management Server connects to the Check Point Firewall or Cluster Member. (2) Interface on Gaia computer, through which users connect to Gaia Portal or CLI.

Management Server
Check Point Single-Domain Security Management Server or a Multi-Domain Security Management Server.

Manual NAT Rules
Manual configuration of NAT rules by the administrator of the Check Point Management Server.

Master
State of a Cluster Member in a VRRP Cluster that processes all traffic in the cluster.

Medium Path
Packet flow on the Host Security Appliance, when the packet is handled by the SecureXL device. The CoreXL layer passes the packet to one of the CoreXL Firewall instances to process it. Even when CoreXL is disabled, the SecureXL uses the CoreXL infrastructure to send the packet to the single CoreXL Firewall instance that still functions. When the Medium Path is available, the SecureXL fully accelerates the TCP handshake. Rule Base match is achieved for the first packet through an existing connection acceleration template. The SecureXL also fully accelerates the TCP [SYN-ACK] and TCP [ACK] packets. However, once data starts to flow, to stream it for Content Inspection, an FWK instance now handles the packets. The SecureXL sends all packets that contain data to FWK for data extraction in order to build the data stream. Only the SecureXL handles the TCP [RST], TCP [FIN] and TCP [FIN-ACK] packets, because they do not contain data that needs to be streamed. The Medium Path is available only when CoreXL is enabled. Exceptions are: IPS (some protections); VPN (in some configurations); Application Control; Content Awareness; Anti-Virus; Anti-Bot; HTTPS Inspection; Proxy mode; Mobile Access; VoIP; Web Portals. Synonym: PXL.

Mirror and Decrypt
The Mirror and Decrypt feature on a Check Point Firewall that performs these actions: (1) Mirror only of all traffic - Clones all traffic (including HTTPS without decryption) that passes through, and sends it out of the designated physical interface. (2) Mirror and Decrypt of HTTPS traffic - Clones all HTTPS traffic that passes through, decrypts it, and sends it in clear-text out of the designated physical interface. Acronym: M&D.

Mobile Access
Software Blade on a Check Point Firewall that provides a Remote Access VPN access for managed and unmanaged clients. Acronym: MAB.

Multi-Domain Log Server
Dedicated Check Point server that runs Check Point software to store and process logs in a Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from [[[Undefined variable tp_cpfws]]] that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

Multi-Domain Security Management Server
Dedicated Check Point server that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Synonym: Multi-Domain Security Management Server. Acronym: MDS.

Multi-Queue
Performance-enhancing technology on Check Point Firewall that configures more than one traffic queue for each network interface. Multi-Queue assigns more than one receive packet queue (RX Queue) and more than one transmit packet queue (TX Queue) to an interface. Multi-Queue is applicable only if SecureXL is enabled (this is the default). Acronym: MQ.

Multi-Version Cluster
The Multi-Version Cluster mechanism lets you synchronize connections between Cluster Members that run different versions. This lets you upgrade to a newer version without a loss in connectivity and lets you test the new version on some of the Cluster Members before you decide to upgrade the rest of the Cluster Members. Acronym: MVC.

N

NAC
Network Access Control. This is an approach to computer security that attempts to unify endpoint security technology (such as Anti-Virus, Intrusion Prevention, and Vulnerability Assessment), user or system authentication and network security enforcement. Check Point's Network Access Control solution is called Identity Awareness Software Blade.

Network Object
Logical object that represents different parts of corporate topology - computers, IP addresses, traffic protocols, and so on. Administrators use these objects in Security Policies.

Network Objective
Defines how the cluster will configure and monitor an interface - Cluster, Sync, Cluster+Sync, Monitored Private, Non-Monitored Private. Configured in SmartConsole > cluster object > 'Topology' pane > 'Network Objective'.

Network Policy Management
Software Blade on a Management Server to manage an on-premises environment with an Access Control and Threat Prevention policies.

Non-Blocking Mode
Cluster operation mode, in which Cluster Member keeps forwarding all traffic.

Non-Dedicated Management Interface
Shared physical interface on Traditional VSX Gateway or Traditional VSX Cluster Members (supported only in versions R80.40 and lower), which carries user "production" traffic and through which Check Point Security Management Server or Multi-Domain Security Management Server connects to Traditional VSX Gateway or Traditional VSX Cluster Members. Non-DMI configuration requires the use of a Virtual Router or Virtual Switch. Acronym: Non-DMI.

Non-Monitored Interface
An interface on a Cluster Member, whose Network Type was set as Private in SmartConsole, in cluster object.

Non-Pivot
A Cluster Member in the Unicast Load Sharing cluster that receives all packets from the Pivot Cluster Member.

Non-Sticky Connection
A connection is called non-sticky, if the reply packet returns via a different Cluster Member, than the original packet (for example, if network administrator has configured asymmetric routing). In the Load Sharing mode, all Cluster Members are Active, and in Static NAT and encrypted connections, the Source and Destination IP addresses change. Therefore, Static NAT and encrypted connections through a Load Sharing cluster may be non-sticky.

O

Observable
Event or stateful property that can be observed in an operational cyber domain.

Open Server
Physical computer manufactured and distributed by a company, other than Check Point.

P

Package Repository
Collection of software packages that were uploaded to the Management Server. You can easily install these packages in SmartConsole on the managed Check Point Firewalls.

Packet Selection
Distinguishing between different kinds of packets coming from the network, and selecting, which member should handle a specific packet (Decision Function mechanism): CCP packet from another member of this cluster; CCP packet from another cluster or from a Cluster; Member with another version (usually older version of CCP); Packet is destined directly to this member; Packet is destined to another member of this cluster; Packet is intended to pass through this Cluster Member; ARP packets.

PDP
Check Point Firewall with Identity Awareness enabled that acts as Policy Decision Point: acquires identities from identity sources; shares identities with other gateways.

PEP
Check Point Firewall with Identity Awareness enabled that acts as Policy Enforcement Point: receives identities via identity sharing; redirects users to Captive Portal.

Permission Profile
Predefined group of SmartConsole access permissions assigned to Domains and administrators. With this feature you can configure complex permissions for many administrators with one definition.

Pingable Host
Some host (that is, some IP address) that Cluster Members can ping during probing mechanism. Pinging hosts in an interface's subnet is one of the health checks that ClusterXL mechanism performs. This pingable host will allow the Cluster Members to determine with more precision what has failed (which interface on which member). On Sync network, usually, there are no hosts. In such case, if switch supports this, an IP address should be assigned on the switch (for example, in the relevant VLAN). The IP address of such pingable host should be assigned per this formula: IP_of_pingable_host = IP_of_physical_interface_on_member + ~10. Assigning the IP address to pingable host that is higher than the IP addresses of physical interfaces on the Cluster Members will give some time to Cluster Members to perform the default health checks. Example: IP address of physical interface on a given subnet on Member_A is 10.20.30.41; IP address of physical interface on a given subnet on Member_B is 10.20.30.42; IP address of pingable host should be at least 10.20.30.5

Pivot
A Cluster Member in the Unicast Load Sharing cluster that receives all packets. Cluster Virtual IP addresses are associated with Physical MAC Addresses of this Cluster Member. This Pivot Cluster Member distributes the traffic between other Non-Pivot Cluster Members.

Policy Layer
Layer (set of rules) in a Security Policy.

Policy Package
Collection of different types of Security Policies, such as Access Control, Threat Prevention, QoS, and Desktop Security. After installation, Check Point Firewalls enforce all Policies in the Policy Package.

Preconfigured Mode
Cluster Mode, where cluster membership is enabled on all Cluster Members to be. However, no policy had been yet installed on any of the Cluster Members - none of them is actually configured to be primary, secondary, and so on. The cluster cannot function, if one Cluster Member fails. In this scenario, the "preconfigured mode" takes place. The preconfigured mode also comes into effect when no policy is yet installed, right after the Cluster Members came up after boot, or when running the 'cphaconf init' command.

Predefined Report
Default report included in a Check Point product that you can run right out of the box.

Prevent
UserCheck rule action that blocks traffic and files and can show a UserCheck message.

Primary Multi-Domain Security Management Server
The Multi-Domain Security Management Server in Management High Availability that you install as Primary.

Primary Security Management Server
The Security Management Server in Management High Availability that you install as Primary.

Primary Up
ClusterXL in High Availability mode that was configured as Switch to higher priority Cluster Member in the cluster object in SmartConsole: (1) Each Cluster Member is given a priority (in the cluster object). Cluster Member with the highest priority appears at the top of the table, and Cluster Member with the lowest priority appears at the bottom of the table. (2) The Cluster Member with the highest priority will assume the Active state. (3) If the current Active Cluster Member with the highest priority (for example, Member_A), fails for some reason, or is rebooted, then failover occurs between Cluster Members. The Cluster Member with the next highest priority will be promoted to be Active (for example, Member_B). (4) When the Cluster Member with the highest priority (Member_A) recovers from a failure, or boots, then additional failover occurs between Cluster Members. The Cluster Member with the highest priority (Member_A) will be promoted to Active state (and Member_B will return to Standby state).

Private Interface
An interface on a Cluster Member, whose Network Type was set as 'Private' in SmartConsole in cluster object. This interface is not monitored by cluster, and failure on this interface will not cause any changes in Cluster Member's state.

Probing
If a Cluster Member fails to receive status for another member (does not receive CCP packets from that member) on a given segment, Cluster Member will probe that segment in an attempt to illicit a response. The purpose of such probes is to detect the nature of possible interface failures, and to determine which module has the problem. The outcome of this probe will determine what action is taken next (change the state of an interface, or of a Cluster Member).

Provisioning
Software Blade on a Management Server that manages large-scale deployments of Check Point Firewalls using configuration profiles. Synonyms: SmartProvisioning, SmartLSM, Large-Scale Management, LSM.

PSL
Passive Streaming Library. Packets may arrive at Check Point Firewall out of order, or may be legitimate retransmissions of packets that have not yet received an acknowledgment. In some cases, a retransmission may also be a deliberate attempt to evade IPS detection by sending the malicious payload in the retransmission. Check Point Firewall ensures that only valid packets are allowed to proceed to destinations. It does this with the Passive Streaming Library (PSL) technology. (1) The PSL is an infrastructure layer, which provides stream reassembly for TCP connections. (2) The Check Point Firewall makes sure that TCP data seen by the destination system is the same as seen by code above PSL. (3) The PSL handles packet reordering, congestion, and is responsible for various security aspects of the TCP layer, such as handling payload overlaps, some DoS attacks, and others. (4) The PSL is capable of receiving packets from the Firewall chain and from the SecureXL. (5) The PSL serves as a middleman between the various security applications and the network packets. It provides the applications with a coherent stream of data to work with, free of various network problems or attacks. (6) The PSL infrastructure is wrapped with well-defined APIs called the Unified Streaming APIs, which are used by the applications to register and access streamed data.

PSLXL
Technology name for combination of SecureXL and PSL (Passive Streaming Library) in versions R80.20 and higher. In versions R80.10 and lower, this technology was called PXL (PacketXL).

Publisher PDP
Check Point Firewall with Identity Awareness enabled that gets identities from an identity source/remote PDP and shares identities to a remote PDP. The Publisher PDP: (1) Initiates an HTTPS connection to the Subscriber PDP for each Identity to be shared (2) Verifies the CN and OU present in the subject field of the certificate presented (3) Verifies that the CA's certificate matches the certificate that was approved in advance by the administrator (4) Checks if the certificate presented is revoked (5) Shares identities including the information about user(s), machine(s) and Access Roles in the form of HTTP POST requests.

Q

QoS
Software Blade on a Check Point Firewall that provides policy-based traffic bandwidth management to prioritize business-critical traffic and guarantee bandwidth and control latency.

QoS Action Properties
Properties that define bandwidth allocation, limits, and guarantees for a security rule.

R

RDED
Retransmit Detect Early Drop. The bottleneck that results from the connection of a LAN to the WAN causes TCP to retransmit packets. RDED prevents inefficiencies by detecting retransmits in TCP streams and preventing the transmission of redundant packets when multiple copies of a packet are concurrently queued on the same flow.

Ready
State of a Cluster Member during after initialization and before promotion to the next required state - Active / Standby / VRRP Master / VRRP Backup (depending on the Cluster Mode). A Cluster Member in this state does not process any traffic passing through cluster. A member can be stuck in this state due to several reasons.

Remote Access VPN
An encrypted tunnel between remote access clients (such as Endpoint Security VPN) and a Check Point Firewall.

Report
Summary of network activity and Security Policy enforcement that is generated by Check Point products, such as SmartEvent.

Route-Based VPN
A routing method for participants in a VPN community, defined by network routes.

Rule
Set of traffic parameters and other conditions in a Rule Base (Security Policy) that cause specified actions to be taken for a communication session.

Rule Base
All rules configured in a given Security Policy. Synonym: Rulebase.

S

Same VMAC
Same Virtual MAC Address (see "VMAC"). When this feature is enabled in a ClusterXL (in the High Availability or Load Sharing Unicast mode), the Cluster Members use Virtual MAC (VMAC) addresses on the cluster interfaces instead of the real MAC addresses. Cluster interfaces that belong to the same subnet get the same VMAC address instead of their real MAC address. This feature helps avoid issues during the cluster operation, when switches block ports connected to the Cluster Members.

Secondary Multi-Domain Security Management Server
The Multi-Domain Security Management Server in Management High Availability that you install as Secondary.

Secondary Security Management Server
The Security Management Server in Management High Availability that you install as Secondary.

SecureXL
Performance-enhancing technology on a Check Point Firewall that accelerates IPv4 and IPv6 traffic that passes through the Check Point Firewall.

Security Management Server
Dedicated Check Point server that runs Check Point software to manage the objects and policies in a Check Point environment within a single management Domain. Synonym: Single-Domain Security Management Server.

Security Policy
Collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

Selection
The packet selection mechanism is one of the central and most important components in the ClusterXL product and State Synchronization infrastructure for 3rd-party clustering solutions. Its main purpose is to decide (to select) correctly what has to be done to the incoming and outgoing traffic on the Cluster Member. (1) In ClusterXL, the packet is selected by Cluster Member(s) depending on the cluster mode: In HA modes - by Active member; In LS Unicast mode - by Pivot member; In LS Multicast mode - by all members. Then the Cluster Member applies the Decision Function (and the Cluster Correction Layer). (2) In 3rd-party / OPSEC cluster, the 3rd-party software selects the packet, and Check Point software just inspects it (and performs State Synchronization).

Service Account
In Microsoft Active Directory, a user account created explicitly to provide a security context for services running on Microsoft Windows Server.

SIC
Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

Silent Standby
In the ClusterXL High Availability mode, this feature configures the Standby Cluster Member to communicate only through the Active Cluster Member. This feature is useful when it is necessary to connect from Standby Cluster Members to a host / server on the network.

Site to Site VPN
An encrypted tunnel between two or more Check Point Firewalls. Synonym: Site-to-Site VPN. Contractions: S2S VPN, S-to-S VPN.

SmartConsole
Check Point GUI application used to manage a Check Point environment - configure Security Policies, configure devices, monitor products and events, install updates, and so on.

SmartDashboard
Legacy Check Point GUI client used to create and manage the security settings in versions R77.30 and lower. In versions R80.X and higher is still used to configure specific legacy settings.

SmartEvent Correlation Unit
SmartEvent software component on a SmartEvent Server that analyzes logs and detects events.

SmartEvent Server
Dedicated Check Point server with the enabled SmartEvent Software Blade that hosts the events database.

SmartProvisioning
Software Blade on a Management Server (the actual name is "Provisioning") that manages large-scale deployments of Check Point Firewalls using configuration profiles. Synonyms: Large-Scale Management, SmartLSM, LSM.

SmartUpdate
Legacy Check Point GUI client used to manage licenses and contracts in a Check Point environment.

Software Blade
Specific security solution (module): (1) On a Check Point Firewall, each Software Blade inspects specific characteristics of the traffic (2) On a Management Server, each Software Blade enables different management capabilities.

Standalone
Configuration in which the Check Point Firewall and the Security Management Server products are installed and configured on the same server.

Standby
State of a Cluster Member that is ready to be promoted to Active state (if the current Active Cluster Member fails). Applies only to ClusterXL High Availability Mode.

Standby Domain Server
All Domain Management Servers for a Domain that are not designated as the Active Domain Management Server.

Standby Security Management Server
The Security Management Server in Management High Availability that is currently configured as Standby.

State Synchronization
Technology that synchronizes the relevant information about the current connections (stored in various kernel tables on Check Point Firewalls) among all Cluster Members over Synchronization Network. Due to State Synchronization, the current connections are not cut off during cluster failover.

Sticky Connection
A connection is called sticky, if all packets are handled by a single Cluster Member (in the High Availability mode, all packets reach the Active Cluster Member, so all connections are sticky).

STIX
Structured Threat Information eXpression™. A language that describes cyber threat information in a standardized and structured way.

Subscriber PDP
Check Point Firewall with Identity Awareness enabled that gets identities from a remote PDP. The Subscriber PDP: (1) Presents the configured SSL certificate to the Publisher PDP (2) Receives the information from the Publisher PDP after verifying the pre-shared secret in the POST requests.

Subscribers
User Space processes that are made aware of the current state of the ClusterXL state machine and other clustering configuration parameters. List of such subscribers can be obtained by running the 'cphaconf debug_data' command.

Sync Interface
An interface on a Cluster Member, whose Network Type was set as Sync or Cluster+Sync in SmartConsole in cluster object. This interface is monitored by cluster, and failure on this interface will cause cluster failover. This interface is used for State Synchronization between Cluster Members. The use of more than one Sync Interfaces for redundancy is not supported because the CPU load will increase significantly due to duplicate tasks performed by all configured Synchronization Networks. Synonyms: Secured Interface, Trusted Interface.

Synchronization Network
A set of interfaces on Cluster Members that were configured as interfaces, over which State Synchronization information will be passed (as Delta Sync packets). The use of more than one Synchronization Network for redundancy is not supported because the CPU load will increase significantly due to duplicate tasks performed by all configured Synchronization Networks. Synonyms: Sync Network, Secured Network, Trusted Network.

System Counter
SmartView Monitor data or report on status, activity, and resource usage of Check Point products.

T

Target Domain Management Server
Domain Management Server on a Multi-Domain Security Management Server, on which you configured the objects of your Virtual Systems. In this case, object of your Traditional VSX Gateway or Traditional VSX Cluster are defined on a different Domain Management Server (Main Domain Management Server).

Terminal Servers Identity Agent
Check Point dedicated client agent installed on Microsoft Windows-based application server that hosts Terminal Servers, Citrix XenApp, and Citrix XenDesktop services. This client agent acquires and reports identities to the Check Point Firewall with Identity Awareness enabled. In the past, this client agent was called Multi-User Host (MUH) Agent. You can download the Terminal Servers Identity Agent from Support Center.

Threat Emulation
Software Blade on a Check Point Firewall that monitors the behavior of files in a sandbox to determine whether or not they are malicious. Acronym: TE.

Threat Emulation Private Cloud Appliance
Check Point appliance that is certified to support the Threat Emulation Software Blade.

Threat Extraction
Software Blade on a Check Point Firewall that removes malicious content from files. Acronym: TEX.

ThreatCloud
The cyber intelligence center of all of Check Point products. Dynamically updated based on an innovative global network of threat sensors and invites organizations to share threat data and collaborate in the fight against modern malware.

ThreatCloud Repository
Cloud database with more than 250 million Command and Control (C&C) IP, URL, and DNS addresses and over 2,000 different botnet communication patterns, used by the ThreatSpect engine to classify bots and viruses. See: https://www.checkpoint.com/infinity-vision/threatcloud/

ThreatSpect Engine
Unique multi-tiered engine that analyzes network traffic and correlates data across multiple layers (reputation, signatures, suspicious mail outbreaks, behavior patterns) to detect bots and viruses.

Traditional VSX Firewall
Physical server that hosts Traditional VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

Transactions
In the context of the Identity Collector, involves the aggregation of events from identity sources, the creation of a request, and the sending of this request to a target. The target then replies with a response. A transaction refers to this request-response.

U

Updatable Object
Network object that represents an external service, such as Microsoft 365, AWS, Geo locations, and more.

URL Filtering
Software Blade on a Check Point Firewall that allows granular control over which web sites can be accessed by a given group of users, computers or networks. Acronym: URLF.

User Database
Check Point internal database that contains all users defined and managed in SmartConsole.

User Directory
Software Blade on a Management Server that integrates LDAP and other external user Management Servers with Check Point products and security solutions.

User Group
Named group of users with related responsibilities.

User Template
Property set that defines a type of user on which a security policy will be enforced.

UserCheck
Functionality in a Check Point Firewall and endpoint clients that gives users a warning when there is a potential risk of data loss or security violation. This helps users to prevent security incidents and to learn about the organizational security policy.

V

Virtual Device
Logical object that emulates the functionality of a type of physical network object. Virtual Device can be on of these: Virtual Router, Virtual System, or Virtual Switch.

Virtual Router
Virtual Device on a Traditional VSX Gateway or Traditional VSX Cluster Member that functions as a physical router. Acronym: VR.

Virtual Switch
Virtual Device on a Traditional VSX Gateway or Traditional VSX Cluster Member that functions as a physical switch. Acronym: VSW.

Virtual System
Virtual Device on a Traditional VSX Gateway or Traditional VSX Cluster Member that implements the functionality of a Check Point Firewall. Acronym: VS.

Virtual System Load Sharing
Traditional VSX Cluster technology that assigns Virtual System traffic to different Active Cluster Members. Acronym: VSLS.

VMAC
Virtual MAC Address. When this feature is enabled in a ClusterXL (in the High Availability or Load Sharing Unicast mode), the current Active or Pivot Cluster Member sends Gratuitous ARP Requests (G-ARP) for its Cluster Virtual IP (VIP) addresses and Virtual MAC (VMAC) addresses in G-ARP updates. Cluster Members create a VMAC address for each Cluster VIP address. This feature helps avoid issues during a cluster failover, when switches do not integrate G-ARP updates into their ARP cache table.

VPN Community
A named collection of VPN domains, each protected by a VPN gateway.

VPN Tunnel
An encrypted connection between two hosts using standard protocols (such as L2TP) to encrypt traffic going in and decrypt it coming out, creating an encapsulated network through which data can be safely shared as though on a physical private line.

VSX
Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Firewalls and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

W

Warp Jump
If two Virtual Systems connect to the same Virtual Switch or Virtual Router, then internally traffic that must pass from a network behind one Virtual System to a network behind another Virtual System, "jumps" from one Virtual System to another Virtual System without passing through the Virtual Switch or Virtual Router.

Warp Link
Logical interface that is created automatically: (1) In a VSNext topology, between a Virtual Gateway and a Virtual Switch (2) In a Traditional VSX topology, between a Virtual System and a Virtual Switch (3) In a Traditional VSX topology, between a Virtual System and a Virtual Router. Acronym: WRP.

WFQ
Weighted Fair Queuing. An algorithm to precisely control bandwidth allocation in QoS.

WFRED
Weighted Flow Random Early Drop. A mechanism for managing the packet buffers of QoS. Adjusting automatically and dynamically to the network traffic situation, WFRED remains transparent to the user.

Z

Zero Phishing
Software Blade on a Check Point Firewall (R81.20 and higher) that provides real-time phishing prevention based on URLs. Acronym: ZPH.