QUANTUM

07 January 2026

MULTI-DOMAIN SECURITY MANAGEMENT

R82

Administration Guide

Check Point Copyright Notice

© 2024 - 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 R82

For more about this release, see the R82 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
07 January 2026	Updated: ■ *"Global Management" on page 63* (added SmartTasks)
9 December 2025	Updated: ■ *"migrate_server" on page 525*
3 September 2025	Updated *"Failure Recovery" on page 126*
10 May 2025	Updated *"mds_backup" on page 495*
12 November 2024	Updated: ■ *"Migrating a Domain Management Server between R82 Multi-Domain Servers" on page 58* ■ *"Backing Up and Restoring a Domain" on page 55*
21 October 2024	First release of this document

Table of Contents

Introduction to Multi-Domain Security Management ... *18*
Basic Multi-Domain Security Management Components ... *19*
The Multi-Domain Server ... *19*
Domain Management Servers ... *19*
Domain Log Servers ... *20*
SmartConsole ... *22*
Multi-Domain View ... *22*
Connecting to SmartConsole ... *24*
Gateways & Servers View ... *26*
Server Processes ... *27*
Multi-Domain Server Processes ... *27*
Domain Management Server Processes ... *27*
Automatic Start of Multi-Domain Server Processes ... *28*
Environment Variables ... *29*
Standard Check Point Environment Variables ... *29*
Deploying Multi-Domain Security Management ... *31*
Planning your Deployment ... *31*
Multi-Site High Availability Deployment ... *31*
Single Site Deployments ... *31*
Platform & Performance Issues ... *33*
Topology, IP Addresses, and Routing ... *33*
Configuring an IPv6 Address on a Multi-Domain Server ... *33*
Using More than one Interface on a Multi-Domain Server ... *40*
Changing the Leading Interface ... *40*
Synchronizing Clocks ... *41*
Protecting the Multi-Domain Security Management Deployment ... *42*
Security Gateway Managed by a Domain Management Server ... *43*

Defining an Access Control Policy for Multi-Domain Server Components 43
Using External Authentication Servers 44
Configuring External Authentication 44
Managing Domains 46
Creating a New Domain 46
Assigning Trusted Clients to Domains 47
Configuring Automatic Domain IP Address Assignment 49
Changing an Existing Domain Configuration 50
Deleting a Domain Management Server or Domain 50
Connecting to a Domain Management Server 51
Working with Cross-Domain Management 52
Changing an Existing Multi-Domain Server 53
Setting the Domain Management Server Display Format 54
Backing Up and Restoring a Domain 55
Migrating a Domain Management Server between R82 Multi-Domain Servers 58
Database Revisions 60
Cross-Domain Search 61
Global Management 63
The Global Domain 63
Connecting to the Global Domain 63
Changing the Global Domain 63
Working with Global Objects 64
Working with Global Configuration Rules 65
Policy Presets 66
Sample Access Control Policy Layer 70
Sample Threat Prevention Policy Layer 72
Using Layers with the Global Domain 74
Upgrade Issues 74
Policy Layers and Administrator Permissions 75
Dynamic Objects and Dynamic Global Objects 75

Defining Rules with Dynamic Objects ... 75
Applying Global Rules to Security Gateways by Function ... 76
Creating a Global Policy in the Global SmartConsole ... 78
Global Assignments ... 80
Configuring an Assignment ... 80
Reassigning ... 81
Handling Assignment Errors ... 82
Deleting a Global Assignment ... 82
Global Assignment Status ... 83
Updating IPS Protections ... 84
Updating the Application & URL Filtering Database ... 86
SmartTasks ... 86
Exceptions ... **87**
Exception Rules ... 87
Disabling a Protection on One Server ... 88
Creating an Exception for a Specific Protection, Site, File or Blade ... 89
Creating Exceptions from Logs or Events ... 93
Exception Groups ... 94
Creating Exception Groups ... 95
Exceptions in a Multi-Domain Environment ... 96
Managing Administrators and Permissions ... **98**
Configuring Administrators ... 98
Administrator - General ... 99
Contact Options ... 100
Creating a Certificate for Logging in to SmartConsole ... 101
Working with Permission Profiles ... 102
Predefined Multi-Domain Permission Profiles ... 102
Working with Multi-Domain Permission Profiles ... 103
Multi-Domain Permission Profile Parameters ... 104
Creating Custom Domain Permissions ... 105

VPN and Multi-Domain Security Management ... ***107***
Global VPN Communities ... *107*
VPN Connectivity ... *108*
Configuring Global VPN Communities ... *109*
Step 1 - Configuring a VPN Domain on each Security Gateway ... *109*
Step 2 - Enabling Gateways for Global Use ... *109*
Step 3 - Creating the VPN Global Community ... *110*
Step 4 - Defining a Security Policy ... *111*
Step 5 - Assigning the Global Configuration to the Local Domains ... *111*
Reassigning the Global Configuration to One or More Local Domains ... *111*
Working with High Availability ... ***113***
Overview of High Availability ... *113*
Multi-Site High Availability Deployment Example ... *114*
Creating a Secondary Multi-Domain Server ... *117*
Limitations ... *117*
Domain Management Server High Availability and Load Sharing ... *119*
Creating a Secondary Domain Management Server ... *119*
Creating a High Availability Environment with a Security Management Server ... *121*
Synchronization ... *123*
How Synchronization Works ... *123*
Initial Synchronization ... *123*
Periodic Synchronization ... *124*
Manual Synchronization ... *124*
Manually Synchronizing a Multi-Domain Server ... *124*
Manually Synchronizing Domain Management Servers ... *125*
Multi-Domain Server ICA Database Synchronization ... *125*
Failure Recovery ... *126*
Deleting a Secondary Multi-Domain Server or Multi-Domain Log Server ... *131*
Re-Establishing SIC Trust for a Secondary Multi-Domain Server ... *132*
Logging and Monitoring ... ***133***

Working with Log Servers ... 134
Configuring Logging ... 135
Creating a Multi-Domain Log Server with Domain Log Servers ... 135
Configuring Security Gateways to Send Logs to a Log Servers ... 136
Deleting a Domain Log Server ... 137
Configuring Log Settings ... 137
Log Server Deployment Scenarios ... 139
Deploying a Domain Dedicated Log Server ... 140
Introduction ... 140
Procedure for an R82 Multi-Domain Environment ... 140
Procedure for an R77.x Multi-Domain Environment ... 141
Using the Log View ... 145
Monitoring Multi-Domain Security Management ... 146
Monitoring Multi-Domain Server Status ... 146
Monitoring Domain Management Server Status ... 146
Monitoring Security Gateway Status ... 147
Creating and Changing an Administrator Account ... 149
Managing Security through API ... 152
API ... 152
API Tools ... 153
Configuring the API Server ... 153
Configuring Implied Rules or Kernel Tables for Security Gateways ... 157
Introduction ... 157
Configuration files ... 157
Configuration Procedure ... 159
Location of 'user.def' Files on the Management Server ... 160
Location of 'table.def' Files on the Management Server ... 161
Location of 'crypt.def' Files on the Management Server ... 163
Location of 'vpn_table.def' Files on the Management Server ... 165
Location of 'vpn_route.conf' Files on the Management Server ... 167

Location of 'communities.def' Files on the Management Server ... 169
Location of 'base.def' Files on the Management Server ... 171
Location of 'dhcp.def' Files on the Management Server ... 173
Location of 'gtp.def' Files on the Management Server ... 175
Location of 'implied_rules.def' Files on the Management Server ... 177
Command Line Reference ... ***179***
Syntax Legend for CLI Commands ... 179
cma_migrate ... 181
contract_util ... 182
contract_util check ... 184
contract_util cpmacro ... 185
contract_util download ... 186
contract_util mgmt ... 188
contract_util print ... 189
contract_util summary ... 190
contract_util update ... 191
contract_util verify ... 192
cp_conf ... 193
cp_conf admin ... 195
cp_conf auto ... 198
cp_conf ca ... 199
cp_conf client ... 201
cp_conf finger ... 205
cp_conf lic ... 206
cp_log_export ... 209
cpca_client ... 230
cpca_client create_cert ... 232
cpca_client double_sign ... 234
cpca_client get_crldp ... 236
cpca_client get_pubkey ... 238

cpca_client init_certs ... 239
cpca_client lscert ... 240
cpca_client revoke_cert ... 243
cpca_client revoke_non_exist_cert ... 246
cpca_client search ... 247
cpca_client set_ca_services ... 250
cpca_client set_cert_validity ... 252
cpca_client set_mgmt_tool ... 253
cpca_client set_sign_hash ... 258
cpca_create ... 260
cpinfo ... 261
cplic ... 262
cplic check ... 265
cplic contract ... 267
cplic db_add ... 269
cplic db_print ... 271
cplic db_rm ... 273
cplic del ... 274
cplic del <object name> ... 275
cplic get ... 276
cplic print ... 278
cplic put ... 280
cplic put <object name> ... 283
cplic upgrade ... 286
cppkg ... 288
cppkg add ... 290
ppkg delete ... 291
cppkg get ... 293
cppkg getroot ... 294
cppkg print ... 295

cppkg setroot ... 296
cpprod_util ... 297
cpmiquerybin ... 302
cprid ... 304
cpstat ... 305
cprinstall ... 313
cprinstall boot ... 316
cprinstall cprestart ... 317
cprinstall cpstart ... 318
cprinstall cpstop ... 319
cprinstall delete ... 320
cprinstall get ... 321
cprinstall install ... 322
cprinstall revert ... 325
cprinstall show ... 326
cprinstall snapshot ... 327
cprinstall transfer ... 328
cprinstall uninstall ... 330
cprinstall verify ... 332
cpview ... 334
Overview of CPView ... 334
CPView User Interface ... 334
Using CPView ... 335
cpwd_admin ... 336
cpwd_admin config ... 339
cpwd_admin del ... 342
cpwd_admin detach ... 343
cpwd_admin exist ... 344
cpwd_admin flist ... 345
cpwd_admin getpid ... 347

cpwd_admin kill ... 348
cpwd_admin list ... 349
cpwd_admin monitor_list ... 352
cpwd_admin start ... 353
cpwd_admin start_monitor ... 355
cpwd_admin stop ... 356
cpwd_admin stop_monitor ... 358
dbedit ... 359
fw ... 372
fw fetchlogs ... 374
fw hastat ... 378
fw kill ... 379
fw log ... 380
fw logswitch ... 390
fw lslogs ... 394
fw mergefiles ... 397
fw repairlog ... 400
fw sam ... 401
fw sam_policy ... 409
fw sam_policy add ... 412
fw sam_policy batch ... 425
fw sam_policy del ... 427
fw sam_policy get ... 430
fwm ... 436
fwm dbload ... 439
fwm exportcert ... 440
fwm fetchfile ... 441
fwm fingerprint ... 443
fwm getpcap ... 445
fwm ikecrypt ... 447

fwm load ... 448
fwm logexport ... 449
fwm mds ... 454
fwm printcert ... 456
fwm sic_reset ... 462
fwm snmp_trap ... 463
fwm unload ... 466
fwm ver ... 470
fwm verify ... 471
inet_alert ... 472
ldapcmd ... 475
ldapcompare ... 477
ldapmemberconvert ... 481
ldapmodify ... 487
ldapsearch ... 489
mcd ... 492
mds_backup ... 495
mds_restore ... 498
mdscmd ... 499
mdsconfig ... 501
mdsenv ... 504
mdsquerydb ... 506
mdsstart ... 508
mdsstart_customer ... 512
mdsstat ... 513
mdsstop ... 515
mdsstop_customer ... 519
mgmt_cli ... 520
migrate ... 521
migrate_server ... 525

migrate_global_policies ... 534
queryDB_util ... 535
rs_db_tool ... 536
sam_alert ... 538
stattest ... 542
threshold_config ... 545
$MDSVERUTIL ... 551
$MDSVERUTIL AllCMAs ... 562
$MDSVERUTIL AllVersions ... 563
$MDSVERUTIL CMAAddonDir ... 566
$MDSVERUTIL CMACompDir ... 567
$MDSVERUTIL CMAFgDir ... 568
$MDSVERUTIL CMAFw40Dir ... 569
$MDSVERUTIL CMAFw41Dir ... 570
$MDSVERUTIL CMAFwConfDir ... 571
$MDSVERUTIL CMAFwDir ... 572
$MDSVERUTIL CMAIp ... 573
$MDSVERUTIL CMAIp6 ... 574
$MDSVERUTIL CMALogExporterDir ... 575
$MDSVERUTIL CMALogIndexerDir ... 576
$MDSVERUTIL CMANameByFwDir ... 577
$MDSVERUTIL CMANameByIp ... 578
$MDSVERUTIL CMARegistryDir ... 579
$MDSVERUTIL CMAReporterDir ... 580
$MDSVERUTIL CMASmartLogDir ... 581
$MDSVERUTIL CMASvnConfDir ... 582
$MDSVERUTIL CMASvnDir ... 583
$MDSVERUTIL ConfDirVersion ... 584
$MDSVERUTIL CpdbUpParam ... 585
$MDSVERUTIL CPprofileDir ... 586

$MDSVERUTIL CPVer ... 587
$MDSVERUTIL CustomersBaseDir ... 588
$MDSVERUTIL DiskSpaceFactor ... 589
$MDSVERUTIL InstallationLogDir ... 590
$MDSVERUTIL IsIPv6Enabled ... 591
$MDSVERUTIL IsLegalVersion ... 592
$MDSVERUTIL IsOsSupportsIPv6 ... 593
$MDSVERUTIL LatestVersion ... 594
$MDSVERUTIL MDSAddonDir ... 595
$MDSVERUTIL MDSCompDir ... 596
$MDSVERUTIL MDSDir ... 597
$MDSVERUTIL MDSFgDir ... 598
$MDSVERUTIL MDSFwbcDir ... 599
$MDSVERUTIL MDSFwDir ... 600
$MDSVERUTIL MDSIp ... 601
$MDSVERUTIL MDSIp6 ... 602
$MDSVERUTIL MDSLogExporterDir ... 603
$MDSVERUTIL MDSLogIndexerDir ... 604
$MDSVERUTIL MDSPkgName ... 605
$MDSVERUTIL MDSRegistryDir ... 606
$MDSVERUTIL MDSReporterDir ... 607
$MDSVERUTIL MDSSmartLogDir ... 608
$MDSVERUTIL MDSSvnDir ... 609
$MDSVERUTIL MDSVarCompDir ... 610
$MDSVERUTIL MDSVarDir ... 611
$MDSVERUTIL MDSVarFwbcDir ... 612
$MDSVERUTIL MDSVarFwDir ... 613
$MDSVERUTIL MDSVarSvnDir ... 614
$MDSVERUTIL MSP ... 615
$MDSVERUTIL OfficialName ... 616

$MDSVERUTIL OptionPack ... 617
$MDSVERUTIL ProductName ... 618
$MDSVERUTIL RegistryCurrentVer ... 619
$MDSVERUTIL ShortOfficialName ... 620
$MDSVERUTIL SmartCenterPuvUpgradeParam ... 621
$MDSVERUTIL SP ... 622
$MDSVERUTIL SVNPkgName ... 623
$MDSVERUTIL SvrDirectory ... 624
$MDSVERUTIL SvrParam ... 625
Creating a Domain Management Server with the 'mgmt_cli' Command ... 626
Glossary ... 627

Introduction to Multi-Domain Security Management

Check Point Multi-Domain Security Management is a centralized management solution for large-scale, distributed environments with many discrete network segments, each with different security requirements. This solution lets administrators create Domains based on geography, business units or security functions to strengthen security and simplify management.

Each Domain has its own Security Policies, network objects and other configuration settings. You use the Global Domain for common security Policies that apply to all or to specified Domains. The Global Domain also includes network objects and other configuration settings that are common to all or to specified Domains.

About this Guide

This *Administration Guide* includes conceptual information and procedures for working with Check Point Multi-Domain Security Management features only.

- To learn how to use SmartConsole to work with Security Policies, the Rule Base, network objects, and security configuration, see the *R82 Security Management Administration Guide*.
- To learn how to work with logs, monitoring, and reports, see the *R82 Logging and Monitoring Administration Guide*.
- To learn how to work with Software Blades and their features, see the applicable *Administration Guides*.

Basic Multi-Domain Security Management Components

This section is a brief introduction to the main components of the Multi-Domain Security Management environment.

The Multi-Domain Server

A **Multi-Domain Server** is a physical server that contains the Domain Management Servers, Security Policies, system data, and Multi-Domain Security Management system software. You connect to a Multi-Domain Server to work with Multi-Domain Security Management features, objects, and configuration settings. This includes:

- Domain Management Servers and their configuration settings
- Global Policies and objects
- Administrators and permission profiles
- Logs and monitoring features
- System configuration settings

You can create a High Availability and/or Load Sharing deployment with two or more, synchronized Multi-Domain Servers.

Domain Management Servers

A *Domain* is a virtual object that defines a network or a collection of networks related to an entity. You can define a Domain for a company, business unit, department, branch or geographical location. For example, a cloud service provider typically has one Domain for each customer. A bank can have one Domain for each geographical region, state, or country.

A *Domain Management Server* is the functional equivalent of a Security Management Server in a single-domain environment. You connect directly to a Domain Management Server with SmartConsole to manage a Domain and its components:

- Domain Security Gateways
- Domain Security Policies, rules, and other Domain level security settings
- Domain system objects, such as services, users, and VPN Communities.
- Domain Software Blades and their related configuration settings

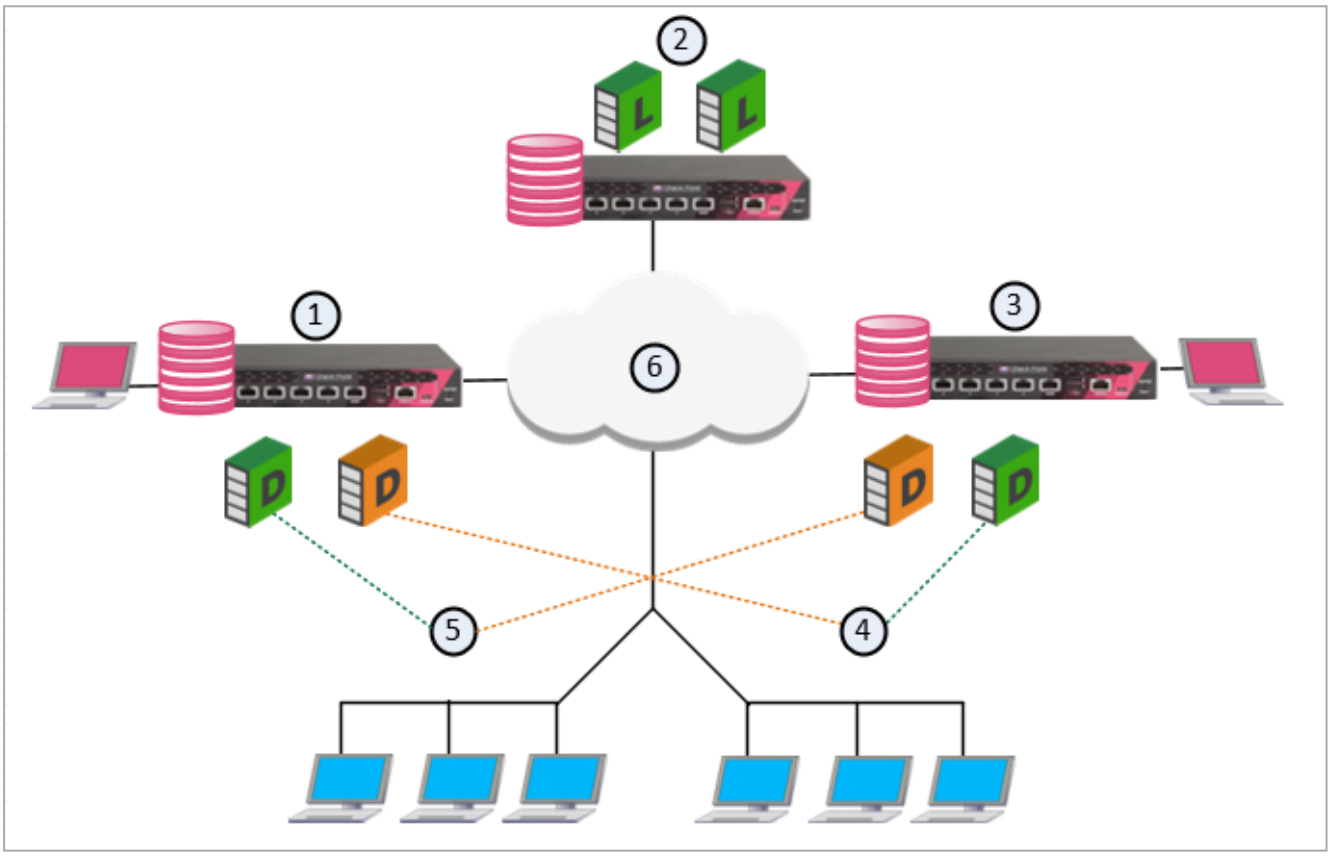
To learn more about working with SmartConsole to manage Domains, see the *R82 Security Management Administration Guide*.

There can be more than one Domain Management Server for a Domain in a High Availability deployment, each on a different Multi-Domain Server. One Domain Management Server is *Active*, and the other, fully synchronized Domain Management Servers are *Standby*.

Domain Log Servers

A typical Multi-Domain Security Management deployment includes, at least one Multi-Domain Log Server to hold log files generated by Domain Security Gateways. Each Domain can have its own Domain Log Server on the Multi-Domain Log Server. This deployment strategy keeps log traffic isolated from other network traffic for better throughput.

This illustration shows a sample deployment with two Multi-Domain Servers and two Domains. The Multi-Domain Log Server contains two Domain Log Servers, one for each Domain.



Item	Description
1	London Multi-Domain Server with an Active Domain Management Server for London and a Standby Domain Management Server for Tokyo
2	Multi-Domain Log Server with Domain Log Servers for London and Tokyo
3	Tokyo Multi-Domain Server with an Active Domain Management Server for Tokyo and a Standby Domain Management Server for London
4	Tokyo network

Item	Description
5	London network
6	Internet
	Active Domain Management Server
	Standby Domain Management Server
	Domain Log Server

SmartConsole

SmartConsole is the unified application of Check Point R80.x Security Management.

SmartConsole provides a consolidated solution for everything that is necessary for the security of your organization:

- Security Policy Management
- Log Analysis
- System Health Monitoring
- Multi-Domain Security Management

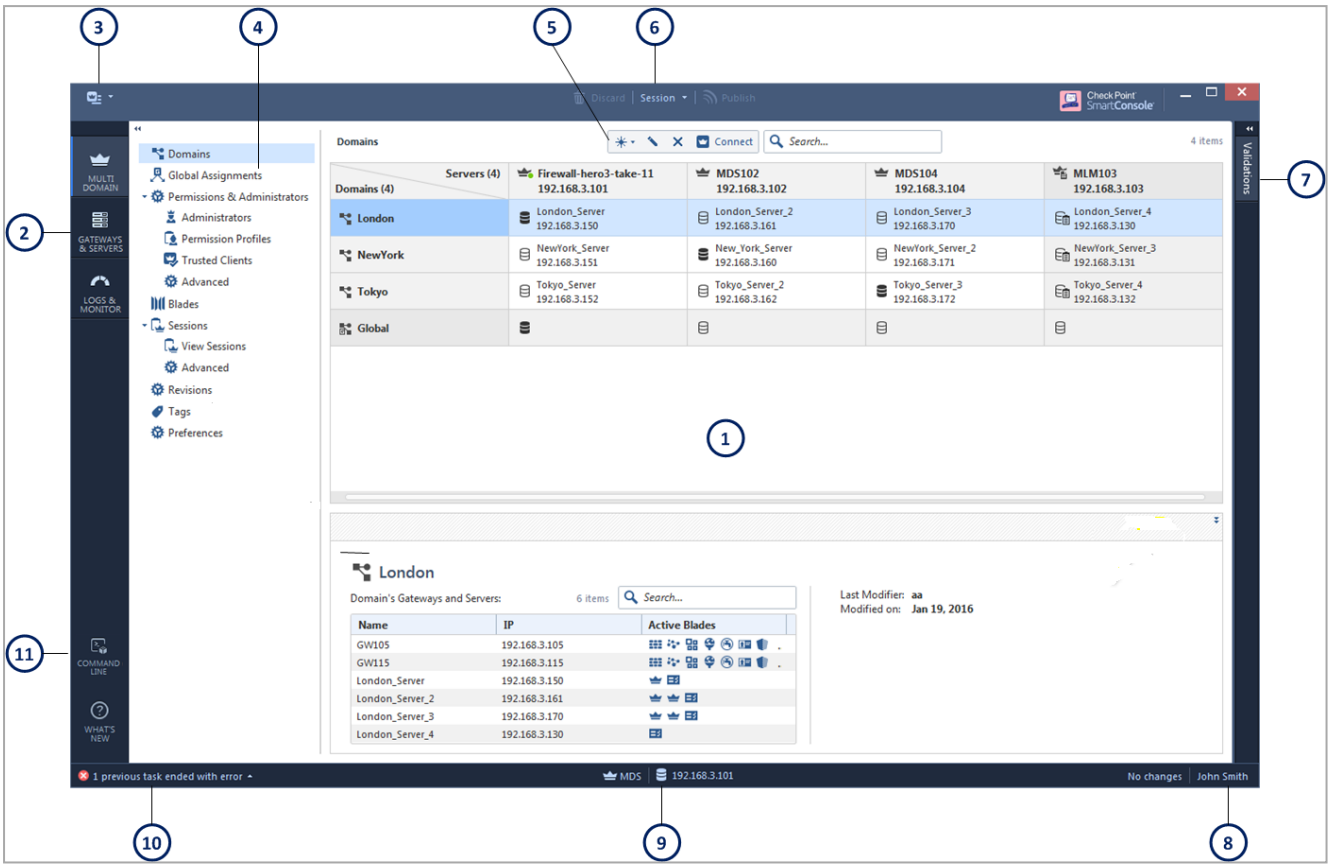
SmartConsole makes it easy to manage your Multi-Domain Security Management environment. Before you start to configure your cyber security environment and Policies, we recommend that you know the SmartConsole application.

Multi-Domain View

Use the *Multi-Domain view* to manage Multi-Domain Servers, Domains, system objects, configuration settings and other features. You must log into a Multi-Domain Server to see the Multi-Domain view.

For a guided tour of **Multi-Domain** view, click the **What's New** button at the bottom left of the window. Click the **<** and **>** icons to scroll between the different What's New screens.

Multi-Domain view elements



Item	Description
1	View, as selected from the **Navigation Toolbar** and **View** tree (This example shows the **Multi-Domain** > **Domains** view)
2	Navigation toolbar
3	Menu
4	View tree
5	Actions toolbar
6	Session Management toolbar
7	Validation tab
8	Logged in administrator
9	Server details area
10	Task information area

Item	Description
11	Management script commands and API

Connecting to SmartConsole

Use SmartConsole to connect to a Multi-Domain Server when you work with Multi-Domain Security Management objects and settings. Use SmartConsole to connect to a Domain Management Server when you work with Domain Security Policies, rules, objects and configuration settings. You can also connect to Domains or specified Domain Management Servers from within the Multi-Domain view.

To connect to the Multi-Domain Server to the "MDS" context:

1. Open the SmartConsole application.
2. Enter the applicable username and password.
3. Enter the IP address of the Multi-Domain Server, and then click **Login**.
4. In the **Welcome** screen, select **MDS** from the list, and then click **Proceed**.

   SmartConsole opens in the **Domains** view.

To connect to the Global Domain Management Server:

1. Open the SmartConsole application.
2. Enter the applicable username and password.
3. Enter the IP address of the Multi-Domain Server, and then click **Login**.
4. In the **Welcome** screen, select **Global** from the list, and then click **Proceed**.

   SmartConsole opens in the **Security Policies** view.

To connect to a Domain:

1. Open the SmartConsole application.
2. Enter the applicable username and password.
3. Enter the IP address of the Multi-Domain Server, and then click **Login**.
4. In the **Welcome** screen, select the required Domain from the list, and then click **Proceed**.

   SmartConsole opens with the selected Domain Management Server.

To connect to a Domain Management Server from the SmartConsole Multi-Domain view:

1. Open the SmartConsole application.
2. Enter the applicable username and password.
3. Enter the IP address of the Multi-Domain Server, and then click **Login**.
4. In the **Welcome** screen, select **MDS** from the list, and then click **Proceed**.

   SmartConsole opens in the **Domains** view.
5. In the **Multi-Domain** > **Domains** view, right-click the required Domain Management Server in the grid and select **Connect to Domain Server**.

Note - In a Management High Availability deployment, you can only make changes to a Domain from the Active Domain Management Server. The Active Domain Management Server object appears with a black icon. If you connect to a Standby Domain Management Server (appears with the white icon), SmartConsole opens in the Read Only mode. See *"Working with High Availability" on page 113*.

Gateways & Servers View

The **Gateways & Servers** view shows all Security Gateway, Domain Management Server, and Domain Log Server objects in the Multi-Domain Security Management environment. This feature lets administrators, with applicable permissions, see and work with them in one convenient location.

You can double-click an object in this view to open its configuration window in the Domain's SmartConsole.

For example, if you double-click, **GW105** on the example below, the **London_Server** Domain Management Server opens in SmartConsole and shows the **GW105** configuration window.

Example - the Gateways & Servers view

Status	Name	Domain	IP	Version	Active Blades	Hardware
–	GW105	London	192.168.3.105	R77.20	...	4000 Appliances
–	GW106	NewYork	192.168.3.106	R77.20	...	12000 Appliances
–	GW107	Tokyo	192.168.3.107	R77.20	...	13000 Appliances
–	GW115	London	192.168.3.115	R77.30	...	21000 Appliances
–	GW116	NewYork	192.168.3.116	R77.30	...	13000 Appliances
–	GW117	Tokyo	192.168.3.117	R77.30	...	61000 Appliances
–	London_Server	London	192.168.3.150	R80		Open server
–	London_Server_2	London	192.168.3.161	R80		Open server
–	London_Server_3	London	192.168.3.170	R80		Open server
–	London_Server_4	London	192.168.3.130	R80		Open server
–	New_York_Server	NewYork	192.168.3.160	R80		Open server
–	NewYork_Server	NewYork	192.168.3.151	R80		Open server
–	NewYork_Serve...	NewYork	192.168.3.171	R80		Open server
–	NewYork_Serve...	NewYork	192.168.3.131	R80		Open server
–	Tokyo_Server	Tokyo	192.168.3.152	R80		Open server
–	Tokyo_Server_2	Tokyo	192.168.3.162	R80		Open server
–	Tokyo_Server_3	Tokyo	192.168.3.172	R80		Open server
–	Tokyo_Server_4	Tokyo	192.168.3.132	R80		Open server

Server Processes

Multi-Domain Server Processes

Each Multi-Domain Server Level process has one instance on every Multi-Domain Server/Multi-Domain Log Server machine, when it is running. These processes run on the Multi-Domain Server.

Process	Description
`cpd`	Check Point daemon - A generic process for many Check Point services, such as installing and fetching policy, online updates, and pushing the SIC certificates.
`cpca`	The Certificate Authority management process
`fwd`	Audit Log server process
`fwm`	Legacy Check Point management server main process (R77.x and earlier)

For proper operation of the Multi-Domain Server, these processes must run together with `CPM`, `postgres`, and `solr`. An exception to this rule is instances where `cpca` cannot run, such as for Domain Log Servers. `cpca` must always run for Domain Management Servers.

Domain Management Server Processes

Each one of these processes runs a different instance for each Domain Management Server:

Process	Description
`cpd`	Check Point daemon - A generic process for many Check Point services, such as installing and fetching policy, online updates, and pushing the SIC certificates.
`cpca`	The Certificate Authority manager process (Domain Servers only)
`fwd`	Log server process
`fwm`	Legacy Check Point management server main process (R77.x and earlier)
`status_proxy`	Status collection of SmartLSM Security Gateways

For proper operation of the Domain Management Server, `cpca`, `fwd` and `fwm` must always run, except for specified configurations where `cpca` cannot run. Other processes are required only as necessary for applicable functionality.

For more information, see sk97638: Check Point Processes and Daemons.

Automatic Start of Multi-Domain Server Processes

The script for the automatic start of Multi-Domain Server processes upon boot is at `/etc/init.d`. The name of the file is `firewall1`. A link to this file appears in `/etc/rc3.d` directory under the name `S95firewall1`.

Environment Variables

Different Multi-Domain Server processes require standard environment variables that:

- Point to the installation directories of different components
- Contain management IP addresses
- Hold data important for correct initialization and operation of the processes

Additionally, specific environment variables control certain parameters of different functions of Multi-Domain Server.

Multi-Domain Server installation contains shell scripts for *Bourne Shell* and for *C-Shell*, which define the necessary environment variables:

- The Bourne Shell version is:

  `/opt/CPshrd-R82/tmp/.CPprofile.sh`

- The C-Shell version is:

  `/opt/CPshrd-R82/tmp/.CPprofile.csh`

Calling these script files from other shell script files (using the " . " command or the "`source`" command) will define the environment necessary for the Multi-Domain Server processes to run.

Standard Check Point Environment Variables

Variable	Description
`FWDIR` `MSDIR`	Location of Check Point files ■ In the Multi-Domain Server environment, this environment variable is equal to `$MDSDIR` ■ In Domain Management Server environment, it contains `/opt/CPmds-R82/customers/<`*`Name of Domain Management Server`*`>/CPsuite-R82/fw1`
`PGDIR`	Location of the PostgreSQL database - `$CPDIR/database/postgresql`
`MDS_` `TEMPLATE`	Location of log files and Java archives
`CPDIR`	Location of Check Point SVN Foundation files that point to different directories in Multi-Domain Server and Domain Management Server environments

Variable	Description
MDSDIR	Location of the Multi-Domain Server installation (/opt/CPmds-R82)
SUROOT	Points to the location of SmartUpdate packages

Deploying Multi-Domain Security Management

This chapter includes information to help you plan your deployment and gives a general overview of the deployment process.

Planning your Deployment

This section includes best practices and other suggestions to help make your Multi-Domain Security Management deployment work efficiently.

Multi-Site High Availability Deployment

Large enterprises use Multi-Domain Security Management in a multi-site, High Availability deployment, with many Multi-Domain Servers located at remote sites, often in different countries. Each Multi-Domain Server and Multi-Domain Log Server continuously synchronizes with its remote peers.

The advantages of this type of deployment are:

- Full Multi-Domain Server, Multi-Domain Log Server, and Domain Management Server redundancy
- Domain Management Server load sharing that can balance traffic based on geographic location
- Many administrators can connect to different Multi-Domain Servers to manage Security Policies and system configuration from different locations

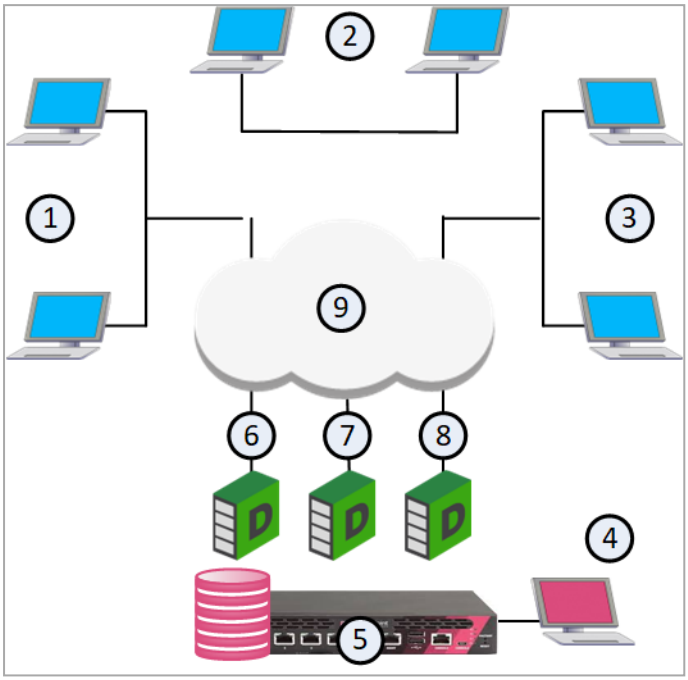
Note - The system automatically creates the Global Domain when you install Multi-Domain Security Management.

Single Site Deployments

Small organizations, with moderate traffic volumes can use a single-site deployment, with one Multi-Domain Server that manages a set of Domains.

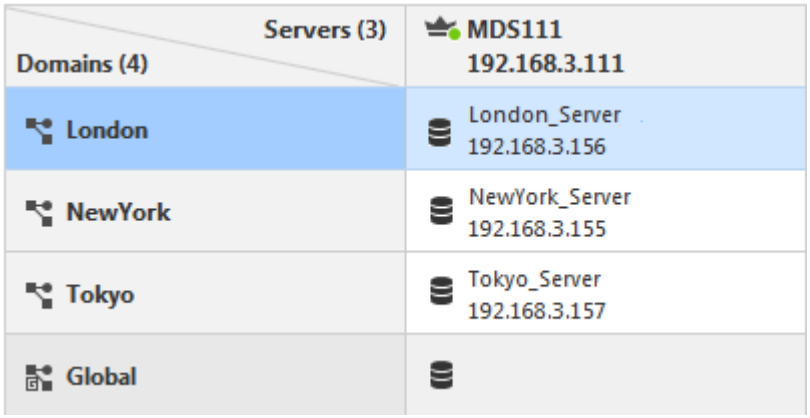
Best Practice - For this type of deployment, use a backup solution that periodically saves the system databases and settings to another device.

This example shows a single-site Multi-Domain Server deployment with three Domains at remote locations. Each Domain has many Security Gateways to protect the internal networks and resources. This example has only one Multi-Domain Server and does not use High Availability.



Item	Description
1	London Domain and networks
2	New York (Headquarters) Domain and networks
3	Tokyo Domain and networks
4	SmartConsole clients, typically at a network control center.
5	Multi-Domain Server
6	London Domain Management Server
7	New York Domain Management Server
8	Tokyo Domain Management Server
9	Internet

This illustration shows the configuration grid in the SmartConsole **Multi Domain** view for the example deployment:



Platform & Performance Issues

Make sure that your Multi-Domain Security Management system hardware is compliant with the system requirements for this release. If your Multi-Domain Server has more than one interface, make sure that the total traffic load complies with the performance load recommendations for that Multi-Domain Server.

Topology, IP Addresses, and Routing

All Multi-Domain Servers must have at least one interface with a routable IP address.

You must configure these Multi-Domain Servers to run DNS server queries and to resolve the IP addresses and host names.

Configure your network routing for IP communication between:

- All Multi-Domain Servers, Domain Management Servers, and Multi-Domain Log Servers
- Different Domains, if necessary
- Domain Management Servers, Domain Log Servers, and Security Gateways in a Domain
- A Domain Management Server and its Domain High Availability peers
- SmartConsole and Multi-Domain Servers, Domain Management Servers and Domain Log Servers

Make sure that IP addresses and routing configuration can handle special issues, such as Multi-Domain Servers in different physical locations.

Configuring an IPv6 Address on a Multi-Domain Server

Starting in R82, it is possible to use IPv6 addresses for the internal Check Point communication:

- Between a Multi-Domain Security Management Server, its Domain Management Servers, and their managed Security Gateways.

  This internal Check Point communication includes Secure Internal Communication (SIC), policy installation, and logging.

- Between a Multi-Domain Log Server, its Domain Log Servers, and the managed Security Gateways.

  This internal Check Point communication includes Secure Internal Communication (SIC) and logging.

- Between a Multi-Domain Security Management Server and a Multi-Domain Log Server.

  This internal Check Point communication includes Secure Internal Communication (SIC) and logging.

Procedure to configure a new IPv6 Address on a Multi-Domain Server

Part 1 - Configuring the Multi-Domain Server

1. Enable IPv6 support in the Gaia OS on the Multi-Domain Server.

   See the *R82 Gaia Administration Guide* > Chapter **System Management** > Section **System Configuration**.

2. Reboot the Multi-Domain Server.

   See the *R82 Gaia Administration Guide* > Chapter **Maintenance** > Section **Shut Down**.

3. On the **Leading Interface** of the Multi-Domain Server, configure the required IPv6 address.

   See the *R82 Gaia Administration Guide* > Chapter **Network Management** > Section **Network Interfaces** > Section **Physical Interfaces**.

4. Configure the applicable IPv6 static routes on the Multi-Domain Server.

   See the *R82 Gaia Administration Guide* > Chapter **Network Management** > Section **IPv6 Static Routes**.

5. Add the same IPv6 address you configured on the **Leading Interface** to the Multi-Domain Server database with the API command "`set-mds`":

a. In the Management API Reference:

   a. Open the chapter "**Multi-Domain**".

   b. Open the section "**Multi-Domain Server (MDS)**".

   See one of these Management API references:

   - The online *Check Point Management API Reference* (at the top, select the correct version) .
   - The local *Management API Reference* (first, you must follow sk174606 to allow access to this local Management API reference):

     ```
     https://<IP Address or Gaia Management Interface>/api_docs/#introduction
     ```

b. Run the API command "`set-mds`":

   (The syntax below is for the CLI command "`mgmt_cli`".)

   ```
   mgmt_cli --domain 'System Data' set-mds name <Name of Multi-Domain Server Object> ipv6-address "IPv6 Address Configured on Leading Interface>"
   ```

   Notes:
   - In the "`name`" parameter, you must enter the name of the Multi-Domain Server object as it appears in SmartConsole.
   - If you run command in the CLI on the Primary Multi-Domain Server, then in the "`name`" parameter you can specify the name of the Secondary Multi-Domain Server object.

6. Restart the Check Point services on the Multi-Domain Server with these commands in the CLI (Gaia Clish or the Expert mode):

   a. Stop the Check Point services:

   ```
   mdsstop
   ```

   b. Start the Check Point services:

   ```
   mdsstart
   ```

7. Make sure all the required processes are running on the Multi-Domain Server with this command in the CLI (Gaia Clish or the Expert mode):

   ```
   mdsstat
   ```

8. Configure the required IPv6 address in the Domain Management Server / Domain Log Server with the applicable API command.

   You can update and existing object or create a new object.

   (The syntax below is for the CLI command "`mgmt_cli`".)

   - To update an existing Domain Management Server / Domain Log Server object and restart it:

     ```
     mgmt_cli set domain name "<Name of Domain Object>"
     servers.update.multi-domain-server "Name of Multi-
     Domain Server Object" servers.update.name "Name of
     Domain Management Server or Domain Log Server Object"
     servers.update.ipv6-address "<IPv6 Address of Domain
     Management Server or Domain Log Server Object>"
     servers.update.restart-domain-server true
     ```

- To create a new Domain Management Server / Domain Log Server object with both an IPv4 and an IPv6 addresses:
  - To create a new Domain Management Server and start it:

```
mgmt_cli add domain name "Name of Domain Object"
servers.1.multi-domain-server "<Name of Multi-
Domain Security Management Server Object>"
servers.1.name "<Name of Domain Management Server
Object>" servers.1.type "management server"
servers.1.ipv4-address "<IPv4 Address of Domain
Management Server Object>" servers.1.ipv6-address
"<IPv6 Address of Domain Management Server Object>"
```

    Note - Digit "1" in the syntax "servers.1." means the first Domain Management Server on this Multi-Domain Security Management Server. If there are already configured Domain Management Servers, then enter the next subsequent number.

  - To create a new Domain Log Server and start it:

```
mgmt_cli add domain name "Name of Domain Object"
servers.1.multi-domain-server "<Name of Multi-
Domain Log Server Object>" servers.1.name "<Name of
Domain Log Server Object>" servers.1.type "log
server" servers.1.ipv4-address "<IPv4 Address of
Domain Log Server Object>" servers.1.ipv6-address
"<IPv6 Address of Domain Log Server Object>"
```

    Note - Digit "1" in the syntax "servers.1." means the first Domain Log Server on this Multi-Domain Log Server. If there are already configured Domain Log Servers, then enter the next subsequent number.

9. Make sure all the required processes are running on the Multi-Domain Server with this command in the CLI (Gaia Clish or the Expert mode):

```
mdsstat
```

Part 2 - Configuring the Security Gateways and Cluster Members

1. Enable IPv6 support in the Gaia OS on the applicable Security Gateways and each applicable Cluster Member.

   See the *R82 Gaia Administration Guide* > Chapter **System Management** > Section **System Configuration**.

2. Reboot the Security Gateways and each Cluster Member.

   See the *R82 Gaia Administration Guide* > Chapter **Maintenance** > Section **Shut Down**.

3. Configure IPv6 addresses on the applicable interfaces.

   See the *R82 Gaia Administration Guide* > Chapter **Network Management** > Section **Network Interfaces**.

4. Configure the applicable IPv6 static routes.

   See the *R82 Gaia Administration Guide* > Chapter **Network Management** > Section **IPv6 Static Routes**.

Part 3 - Configuring the Security Gateways and Cluster objects in SmartConsole

Follow the *R82 Security Management Administration Guide*.

Procedure to change an existing IPv6 address on a Multi-Domain Server

1. Connect to the command line on the Multi-Domain Security Management Server.
2. Log in to the Expert mode.
3. Disable the current IPv6 configuration:

   ```
   mdsconfig -n disable_ipv6 <Name of Leading Interface>
   ```

4. Restart the Check Point services on the Multi-Domain Server:
   a. Stop the Check Point services:

      ```
      mdsstop
      ```

   b. Start the Check Point services:

      ```
      mdsstart
      ```

5. Make sure all the required processes are running on the Multi-Domain Server:

   ```
   mdsstat
   ```

6. Configure the new IPv6 address on the Leading Interface.

   Follow steps 3-7 in *"Part 1 - Configuring the Multi-Domain Server" on page 34*.

7. Change the IPv6 addresses assigned Domain Management Servers / Domain Log Servers with the API command "`set domain`":

   (The syntax below is for the CLI command "`mgmt_cli`".)

   ```
   mgmt_cli set domain name "<Name of Domain Object>"
   servers.update.multi-domain-server "<Name of Multi-Domain
   Server Object>" servers.update.name "<Name of Domain
   Management Server or Domain Log Server Object>"
   servers.update.ipv6-address "<IPv6 Address of Domain
   Management Server or Domain Log Server Object>"
   servers.update.restart-domain-server true
   ```

8. Make sure all the required processes are running on the Multi-Domain Server:

   ```
   mdsstat
   ```

Using More than one Interface on a Multi-Domain Server

If there is more than one interface on a Multi-Domain Server, you must configure at least one interface to be the *leading interface*. Multi-Domain Servers (Primary and Secondary) and Multi-Domain Log Servers use the leading interface to communicate with each other for database synchronization.

Make sure that all Multi-Domain Server interfaces are routable. Domain Management Servers must be able to communicate with their Domain Security Gateways. Domain Log Servers must be able to communicate with their Domain Security Gateways.

Changing the Leading Interface

You define the leading interface during the installation procedure, but you can change it later. If you add a new interface to a Multi-Domain Server after installation, define the Leading Interface manually.

To add a New Leading Interface

1. From the Multi-Domain Server command line, run: `mdsconfig`
2. Select **Leading VIP Interfaces**, and then select **Add external IPv4 interface**.
3. Enter the interface name and press **Enter**.

Changing the Leading Interface

1. From the Multi-Domain Server command line, run: `mdsconfig`
2. Do steps 2-3, in the above procedure, to add new interface.
3. Select **Leading VIP Interfaces**.
4. Select **Remove External IPv4 interface**.
5. Enter the interface name to remove and press **Enter**.

Synchronizing Clocks

All Multi-Domain Server system clocks must synchronize to approximately one second. Before you create a new Multi-Domain Server or Multi-Domain Log Server, you must synchronize its clock with other system components.

Clock synchronization is important for these reasons:

- SIC trust can fail if devices are not synchronized correctly
- SmartEvent Correlation Unit uses time stamps, which must be accurate
- Make sure that cron jobs run at the correct time
- Certificate validation is based on the correct time

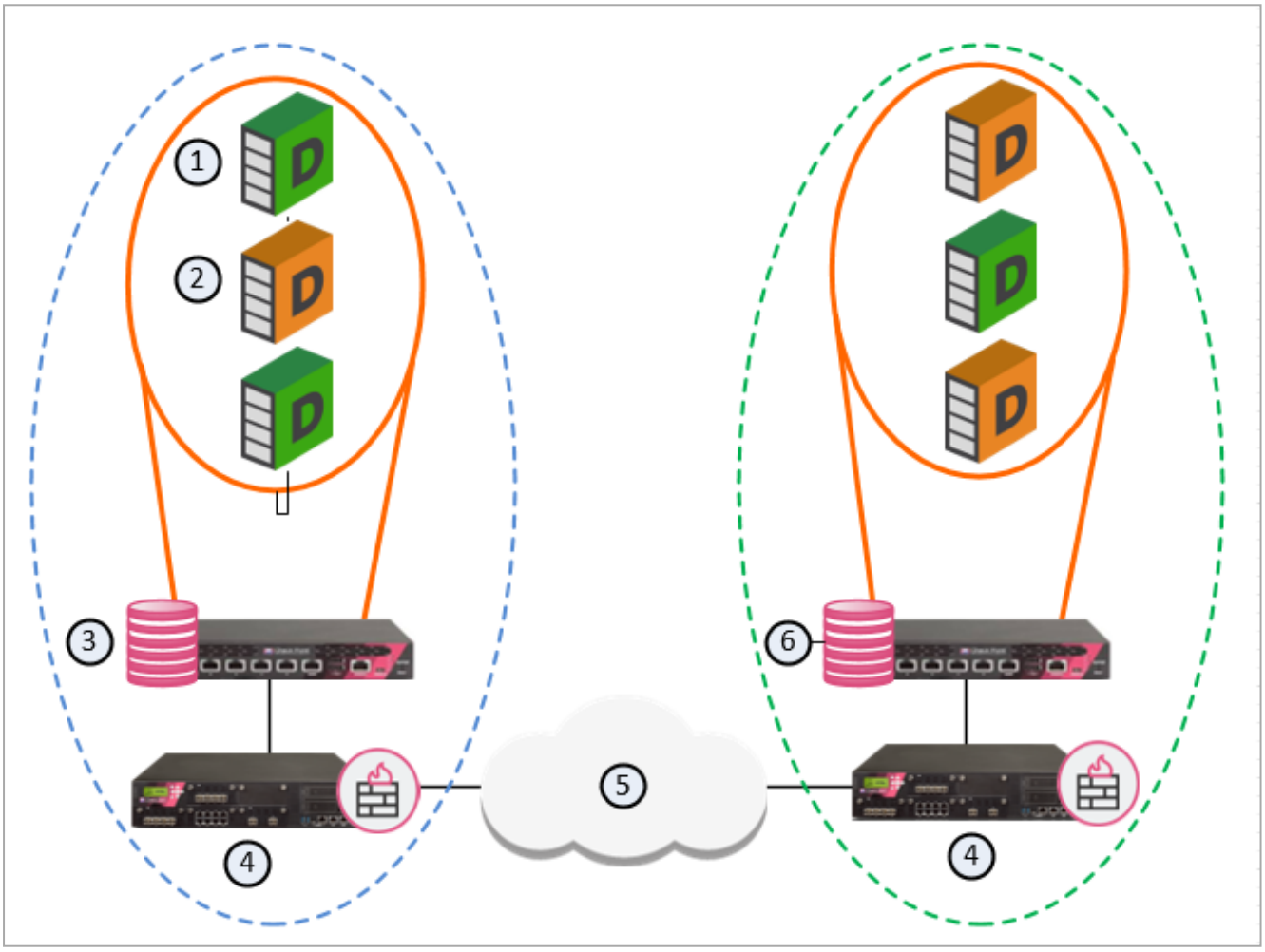
Use these resources to synchronize component system clocks:

- Manually, using Gaia Portal or Gaia Clish
- A third-party synchronization utility

Protecting the Multi-Domain Security Management Deployment

It is a security best practice to deploy a Check Point Security Gateway that protects the Multi-Domain Servers, Multi-Domain Log Server and other components. You can manage this Security Gateway with a Domain Management Server or a Security Management Server that is not part of a Multi-Domain Security Management environment.

This simple use case shows a small High Availability deployment with a Security Gateway protecting each Multi-Domain Server. One of the Domain Management Servers manages these Security Gateways.



Item	Description
1	Active Domain Management Servers
2	Standby Domain Management Servers

Item	Description
3	Primary Multi-Domain Server with Active and Standby Domain Management Servers
4	Security Gateways
5	Internet
6	Secondary Multi-Domain Server with Active and Standby Domain Management Servers

Security Gateway Managed by a Domain Management Server

You can create a Domain and Domain Management Server to manage the Policies for Security Gateways that protect Multi-Domain Servers in your environment.

Workflow for this scenario:

1. Run SmartConsole and log into the Multi-Domain Server.
2. Create a new Domain and Domain Management Server.
3. Connect to the new Domain SmartConsole and create a Security Gateway object.
4. Enable the **Firewall** and other Software Blades on this Security Gateway.
5. Create and install a Security Policy for the Security Gateway.

Defining an Access Control Policy for Multi-Domain Server Components

communication between the different Multi-Domain Security Management components. You can define these rules in global configurations or in local Domain Policies.

Use this table as a guideline to allow connections between specified components:

Activity	Source	Destination
Allow connections between SmartConsole and the Multi-Domain Server	SmartConsole Multi-Domain Server	Multi-Domain Server SmartConsole
Allow connections between Multi-Domain Servers	Multi-Domain Servers	Multi-Domain Servers

Activity	Source	Destination
Allow connections between Domain Management Servers and Security Gateways	Domain Management Server Security Gateway	Security Gateway Domain Management Server
Allow Domain Management Server status data and certificate exchange between Domain Management Server High Availability peers Allow Domain Management Server synchronization between peers	Domain Management Server peer	Domain Management Server peer

See the *R82 Security Management Administration Guide* to learn how to create a Security Policy.

Using External Authentication Servers

Multi-Domain Security Management supports these external authentication solutions:

- RADIUS
- TACACS
- RSA SecurID Authentication Manager

When an administrator logs in, an authentication requests goes to the external authentication server, which sends a reply to the Multi-Domain Server. TACACS and RADIUS use the Multi-Domain Server as a proxy between the Domain Management Server and the external authentication server. To make this work correctly, you must configure each Multi-Domain Server on the authentication server.

Note - If the Multi-Domain Server is DOWN, the Domain Management Server cannot authenticate administrators.

Configuring External Authentication

To configure External Authentication:

1. Connect to the Multi-Domain Server with SmartConsole.
2. In the **Domains** view, select the Global Domain, and then click **Connect**.
3. Connect to the Global Domain with SmartConsole, and then create a host object for the authentication server.

4. Define the Multi-Domain Security Management administrators in the authentication server.
5. In SmartConsole, select **Administrators**.
6. Select an existing administrator or click **New**.
7. In the **General** tab, select the applicable **Authentication Scheme**.
8. If the selected authentication server is **RADIUS** or **TACACS**, select the server that you configured in the Global Domain SmartConsole.
9. If the authentication server is SecurID:
    a. Close SmartConsole.
    b. Generate the file `sdconf.rec` on the Authentication Manager, and configure the user to use *Tokencode* only.
    c. Copy `sdconf.rec` to `/var/ace/` on each Multi-Domain Server.
    d. Open `/etc/services` in a text editor and add the following lines:

    ```
    securid 5500/udp

    securidprop 5510/tcp
    ```

    e. Reboot the Multi-Domain Server.

Note - The `<authentication_server>` parameter is required for TACACS and RADIUS.

Managing Domains

A *Domain Management Server* is the functional equivalent of a Security Management Server in a single-Domain environment.

You connect with SmartConsole directly to a Domain Management Server to manage the Domain and its components:

- Security Gateways managed by this Domain
- Domain Security Policies, rules, and other Domain-level security settings
- Domain system objects, such as services, users, and VPN Communities.
- Domain Software Blades and their related configuration settings

This chapter contains:

- Instructions to create and manage Domains and Domain Management Servers.
- Instructions to create and configuring a Secondary Multi-Domain Server.

Creating a New Domain

Use this procedure to create a new Domain together with the first Domain Management Server for this Domain.

To create a New Domain

1. Connect to the Multi-Domain Server with SmartConsole.
2. In the **Multi-Domain** > **Domains** view, click **New**.
3. In the **Domain** window, enter a unique Domain name.
4. Click the **+** icon in the **General** > **Domain Servers** section.

   In a Management High Availability deployment, you must select a Multi-Domain Server from the list.

   a. Enter a unique Domain Management Server name or accept the default name.

   b. Enter the Domain Management Server IP address, or click **Resolve IP** to get the IP Address from the Multi-Domain Server address pool.

   c. Accept the default Domain Management Server type and click **OK**.

d. Click **Trusted Clients** and select one or more trusted clients from the list that can connect to this Domain Management Server.

e. Optional: Click **Additional Information** and enter contact information for the person responsible for this Domain Management Server.

5. Click **OK** to save the new Domain and Domain Management Server.

6. After you created the Domain, you can configure administrator access to your Domain using an Identity Provider. In the **Multi-Domain** view > **Domains**, right-click the Domain and select **Edit**. Go to the Identity Provider tab, and select one of these options:

   - **Use the default Identity Provider for Managing Administrator Access to this Domain** - Use the Identity Provider selected in the **Manage & Settings** view > **Permissions & Administrators** > **Advanced** > **Identity Provider**.
   - **Use the Domain Identity Provider for Managing Administrator Access to this Domain** - Select this option if there is an identity provider which is configured in the **Multi-Domain** view, but you would like to use a different Identity Provider for the specific Domain.

   For more information on how to create and configure an Identity Provider, see *Creating an Administrator Account with SAML Authentication Login*.

7. Click **OK**.

Notes:

- When you create a new Domain, you must always create at least one new Domain Management Server with it.
- You can also use this procedure to create Standby Domains and Domain Management Servers for Domain Management Server for redundancy and Load Sharing. To do this, there must be at least one Secondary Multi-Domain Server in the deployment.
- To create a Log Server, you must have a Multi-Domain Log Server or a Secondary Multi-Domain Server in your environment.
- To add a license for a Domain, go to the main Menu > **Manage licenses and packages**.
- You cannot add additional information fields to the Domain object.

Assigning Trusted Clients to Domains

You must assign one or more trusted SmartConsole clients to Domains before you can connect to them. If you do not do this, an error message shows when you try to connect.

Each Domain assignment identifies trusted SmartConsole clients based on one of these criteria:

- An IP address
- A host name

- A range of IP addresses
- Net mask
- IP addresses with wildcard characters
- **Any** - All SmartConsole clients can connect

Assigning a new trusted client to a Domain

1. Connect to the Multi-Domain Server with SmartConsole
2. From the tree, click **Multi-Domain**.
3. From the tree, click **Permissions & Administrators** > **Trusted Clients**.
4. Click **New**.
5. In the **New Trusted Client** window, enter a unique name for this Domain assignment.
6. Select an identification criterion from the **Type** list and enter the applicable information.
7. In the **Domains Assignment** section, add one or more Domains.
8. Optional: Select **Multi-Domain Server Trusted Client** to apply this assignment to Multi-Domain Servers in addition to the specified Domains.
9. Click **OK**.

Adding an existing trusted client to a Domain

1. Connect to the Multi-Domain Server with SmartConsole
2. From the tree, click **Multi-Domain**.
3. From the tree, click **Permissions & Administrators > Trusted Clients**.
4. Double-click the trusted client name.
5. In the **Domains Assignment** section, add one or more Domains.
6. Optional: Select **Multi-Domain Server Trusted Client** to apply this assignment to Multi-Domain Servers in addition to the specified Domains.
7. Click **OK**.

Changing a Domain assignment

1. Connect to the Multi-Domain Server with SmartConsole
2. From the tree, click **Multi-Domain**.
3. From the tree, click **Permissions & Administrators > Trusted Clients**.

4. Double-click the trusted client name.
5. Select an identification criterion from the **Type** list and enter or change the applicable information.
6. In the **Domains Assignment** section, add or delete one or more Domains.
7. Optional: Select **Multi-Domain Server Trusted Client** to apply this assignment to Multi-Domain Servers in addition to the specified Domains.
8. Click **OK**.

To clone an existing Domain:

1. Connect to the Multi-Domain Server with SmartConsole.
2. Go to the **Multi-Domain** view > **Domains**.
3. Right-click the required Domain, and select **Clone**.
4. In the window that opens, click **Continue**.
5. Configure the cloned Domain.
6. Click **OK**.

You can see the progress of cloning at the bottom left corner of SmartConsole.

Configuring Automatic Domain IP Address Assignment

You can configure a Multi-Domain Server to assign an IP address to Domain Management Servers managed by this Multi-Domain Server from a predefined pool of IP addresses. This makes sure that the assigned IP address is not in use by other Multi-Domain Servers or Domain Management Servers.

To configure a Multi-Domain Server to assign IP addresses to Domain Management Servers

1. Connect to the Multi-Domain Server with SmartConsole
2. From the left tree, click **Multi-Domain** > **Domains**.
3. Right-click a Multi-Domain Server and select **Edit**.

   The **Multi-Domain Server** window opens.
4. From the left tree, click **Multi-Domain**.
5. In the **IP Range** section, enter the first and last IP address in the range.
6. Click **OK**.

Changing an Existing Domain Configuration

1. Connect to the Multi-Domain Server with SmartConsole.
2. From the left tree, click **Multi-Domain** > **Domains**.
3. Right-click a Domain in the grid, and then select **Edit**.

   The **Domain** window opens.
4. From the left tree, click **General**.
5. In the **Domain Servers** section, select the Domain Management Server and click the **pencil icon** (**Edit/View Domain Server**).

   Note - You cannot change the Domain name.
6. Add, delete, or change the other Domain definitions as necessary.
7. Click **OK**.

Deleting a Domain Management Server or Domain

Deleting a Domain Management Server

1. Connect with SmartConsole to the Multi-Domain Server.
2. From the left tree, click **Multi-Domain** > **Domains**.
3. Right-click a Domain Management Server in the grid, and then select **Delete**.

Deleting a Domain

1. Connect with SmartConsole to the Multi-Domain Server.
2. From the left tree, click **Multi-Domain** > **Domains**.
3. In the **Domains** column, right-click a Domain, and then select **Delete**.

Note - This action automatically deletes the Active and Secondary Domain Management Servers, Domain Log Servers, and the Domain object.

Connecting to a Domain Management Server

Connecting directly to a Domain Management Server

1. Connect with SmartConsole to the Multi-Domain Server.
2. In the **Welcome** screen, select a Domain from the list, and then click **Proceed**.
3. SmartConsole opens with the active Domain Management Server in the **Gateways & Servers** view.

Connecting from the SmartConsole Multi-Domain view

1. Connect with SmartConsole to the Multi-Domain Server.
2. From the left tree, click **Multi-Domain** > **Domains**.
3. Right-click the Active Domain Management Server in the grid, and then select **Connect to Domain Server**.

Note - In a Management High Availability deployment, you can only make changes to a Domain from the active Domain Management Server. The active Domain Management Server shows with a black icon. If you connect to a standby Domain Management Server (white icon), SmartConsole opens in the Read Only mode.

Working with Cross-Domain Management

The Multi-Domain Security Management **Gateways & Servers** view lets administrators see and work with Domain Management Servers, Security Gateways, and other objects for all Domains in one convenient window.

You must have the applicable permissions to see and work with these objects.

To open the Gateways & Servers view

1. Connect with SmartConsole to the Multi-Domain Server.
2. From the left tree, click **Gateways & Servers**.

   This view shows all Security Gateways and Clusters managed by all Domain Management Servers.

   Example:

Status	Name	Domain	IP	Version	Active Blades	Hardware
–	GW105	London	192.168.3.105	R77.20	...	4000 Appliances
–	GW106	NewYork	192.168.3.106	R77.20	...	12000 Appliances
–	GW107	Tokyo	192.168.3.107	R77.20	...	13000 Appliances
–	GW115	London	192.168.3.115	R77.30	...	21000 Appliances
–	GW116	NewYork	192.168.3.116	R77.30	...	13000 Appliances
–	GW117	Tokyo	192.168.3.117	R77.30	...	61000 Appliances
–	London_Server	London	192.168.3.150	R80		Open server
–	London_Server_2	London	192.168.3.161	R80		Open server
–	London_Server_3	London	192.168.3.170	R80		Open server
–	London_Server_4	London	192.168.3.130	R80		Open server
–	New_York_Server	NewYork	192.168.3.160	R80		Open server
–	NewYork_Server	NewYork	192.168.3.151	R80		Open server
–	NewYork_Serve...	NewYork	192.168.3.171	R80		Open server
–	NewYork_Serve...	NewYork	192.168.3.131	R80		Open server
–	Tokyo_Server	Tokyo	192.168.3.152	R80		Open server
–	Tokyo_Server_2	Tokyo	192.168.3.162	R80		Open server
–	Tokyo_Server_3	Tokyo	192.168.3.172	R80		Open server
–	Tokyo_Server_4	Tokyo	192.168.3.132	R80		Open server

To work with a Security Gateway, double-click the Security Gateway object. A SmartConsole instance for the applicable Domain Management Server opens and automatically shows the **Gateway** window for the selected Security Gateway. In a Management High Availability environment, SmartConsole opens for the Active Domain Management Server.

To work with a Domain, double-click its Domain Management Server object. A SmartConsole instance for the applicable opens and automatically shows the **Host** window for the selected Domain Management Server. In a Management High Availability environment, make sure that you select the Active Domain Management Server, which opens in the Read/Write mode. Standby Domain Management Servers open as Read-Only, and you cannot make any changes to Domain objects.

Changing an Existing Multi-Domain Server

You can change the settings for an existing Multi-Domain Server or Multi-Domain Log Server.

To change the settings for an existing Multi-Domain Server:

1. Connect with SmartConsole to the Multi-Domain Server.
2. From the left tree, click **Multi-Domain** > **Domains**.
3. In the top row of the **Domains** grid, double-click the Multi-Domain Server or Multi-Domain Log Server object.
4. In the **Multi-Domain Server** window, change the parameters in these views:
   - **General**
   - **Configuring Automatic Domain IP Address Assignment**

Notes:

- You cannot change the name of the Multi-Domain Server object.
- Configuring only IPv6 address without IPv4 address on the Multi-Domain Security Management Server is not supported.

Setting the Domain Management Server Display Format

You can change how Domain Management Servers show in the **Domains** grid.

To set the Domain Management Servers display format

1. Connect with SmartConsole to the Multi-Domain Server.
2. From the left tree, click **Multi-Domain** > **Preferences**.
3. Select a **Domain Server Display Format**:
   - **Domain Server Name and IP** (default)
   - **Domain Server IP**
   - **Domain Server Name**

Backing Up and Restoring a Domain

You can back up a Domain and later restore it on the same Multi-Domain Server.

Important:

- You can restore a Domain *only* on the same Multi-Domain Server, on which you backed it up.
- You can restore a Domain, to which a Global Policy is assigned, *only* if during the Domain backup you did **not** purge the assigned Global Domain Revision.

Backing Up a Domain

Run this API:

```
export-management
```

For API documentation, see the *Check Point Management API Reference* (at the top, select the correct version) - search for `export-management`.

Restoring a Domain

1. **Make sure it is possible to restore the Domain**

   Before you can restore a Domain, you must delete the current Domain.

   Before you delete the current Domain, make sure it is possible to restore it.

   Run this API with the "`verify-domain-restore`" flag:

   For API documentation, see the *Check Point Management API Reference* (at the top, select the correct version) - search for `import-management`.

2. **Delete the current Domain**

   Before you can restore a Domain, you must delete the current Domain.

   You can perform this step in one of these ways:

   - In SmartConsole connected to the **MDS** context
   - With the API *delete domain* (see the *Check Point Management API Reference* (at the top, select the correct version))

3. **Restore the Active Domain Management Server**

   Run this API:

   ```
   import-management
   ```

For API documentation, see the *Check Point Management API Reference* (at the top, select the correct version) - search for `import-management`.

4. **Restore the Standby Domain Management Servers and Domain Log Servers**

   When you restore the Standby Domain Management Servers and Domain Log Servers, they must have the same IP addresses that were used when you collected the Domain backup.

   For API documentation, see the *Check Point Management API Reference* (at the top, select the correct version) - search for *set domain*

   For each Standby Domain Management Server, run this API:

   ```
   set-domain name <Name or UID of Domain> servers.add.ip-
   address <IP Address of Domain Management Server>
   servers.add.name <Name of Domain Management Server>
   servers.add.multi-domain-server <Name of Multi-Domain
   Server> servers.add.backup-file-path <Full Path to Domain
   Backup File>.tgz --format json
   ```

   For each Domain Log Server, run this API:

   ```
   set-domain name <Name or UID of Domain> servers.add.ip-
   address <IP Address of Domain Log Server> servers.add.name
   <Name of Domain Log Server> servers.add.multi-domain-
   server <Name of Multi-Domain Server> servers.add.backup-
   file-path <Full Path to Domain Backup File>.tgz --format
   json servers.add.type "log server"
   ```

5. **Configure and assign the Administrators and GUI clients**

   You must again configure the Multi-Domain Server Administrators and GUI clients and assign them to the Domains.

   a. Configure the Multi-Domain Server Administrators and GUI clients:

      i. Run the `mdsconfig` command

      ii. Configure the **Administrators**

      iii. Configure the **GUI clients**

   b. Assign the Administrators and GUI clients to the Domains:

      See *"Backing Up and Restoring a Domain" on the previous page* and *"Backing Up and Restoring a Domain" on the previous page*.

6. **Install policy on all managed Security Gateways and Clusters**

    a. Connect with SmartConsole to the restored Active Domain.

    b. Install the applicable policies on all managed Security Gateways and Clusters.

Migrating a Domain Management Server between R82 Multi-Domain Servers

This procedure lets you export the entire management database from a Domain Management Server on one R82 Multi-Domain Server and import it on another R82 Multi-Domain Server.

For the list of known limitations, see sk156072.

Procedure:

1. **On the source Multi-Domain Server, export the Domain Management Server**

   a. Run this API:

   ```
   export-management
   ```

   For API documentation, see the *Check Point Management API Reference* (at the top, select the correct version) - search for `export-management`.

   b. Calculate the MD5 of the export file:

   ```
   md5sum <Full Path to Export File>
   ```

2. **Transfer the export file to the target Multi-Domain Server**

   a. Transfer the export file from the source Multi-Domain Server to the target Multi-Domain Server, to some directory.

   Note - Make sure to transfer the file in the binary mode.

   b. Make sure the transferred file is not corrupted.

   Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the source Multi-Domain Server:

   ```
   md5sum <Full Path to Export File>
   ```

3. **On the target Multi-Domain Server, import the Domain Management Server**

   a. Run this API:

   ```
   import-management
   ```

   For API documentation, see the *Check Point Management API Reference* (at the top, select the correct version) - search for `import-management`.

b. Make sure that all the required daemons (FWM, FWD, CPD, and CPCA) are in the state "`up`" and show their PID (the "`pnd`" state is also acceptable):

```
mdsstat
```

If some of the required daemons on a Domain Management Server are in the state "`down`", then wait for 5-10 minutes, restart that Domain Management Server and check again. Run these three commands:

```
mdsstop_customer <IP Address or Name of Domain
Management Server>
mdsstart_customer <IP Address or Name of Domain
Management Server>
mdsstat
```

4. **Configure and assign the Administrators and GUI clients**

You must again configure the Multi-Domain Server Administrators and GUI clients and assign them to the Domains.

a. Configure the Multi-Domain Server Administrators and GUI clients:

i. Run the `mdsconfig` command

ii. Configure the **Administrators**

iii. Configure the **GUI clients**

iv. Exit the `mdsconfig` menu

b. Assign the Administrators and GUI clients to the Domains:

See *"Migrating a Domain Management Server between R82 Multi-Domain Servers" on the previous page* and *"Migrating a Domain Management Server between R82 Multi-Domain Servers" on the previous page*.

5. **Install policy on all managed Security Gateways and Clusters**

a. Connect with SmartConsole to the Active Domain (to which this Domain Management Server belongs).

b. Install the applicable policies on all managed Security Gateways and Clusters.

Database Revisions

You can revert to previous versions of the database on your domains. Revert to revision is supported on the Global and Local Domains but not on the Multi-Domain Management Server view. Note that the Global Domain supports revisions only if the corresponding revision was not purged. For more information on how to use the database revision feature, see the *R82 Security Management Administration Guide*

Cross-Domain Search

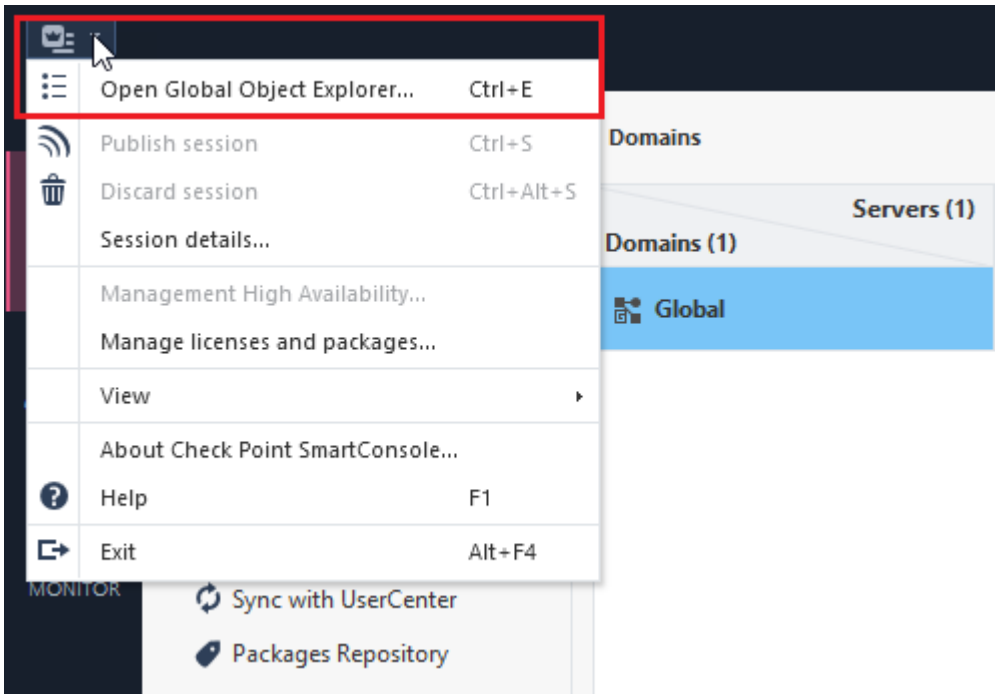
Starting from R81, you can do these actions from the Multi-Domain view across all Domains, without logging into each Domain:

- Search an object
- View unused objects
- See where an object is used

For information on how to do these actions in a specific domain, see the *R82 Security Management Administration Guide*.

To do a cross-domain search:

1. In the Multi-Domain view, click the drop-down arrow in the main menu and select **Open Global Object Explorer**.



   The **Global Object Explorer** window opens.

2. In the search box, enter what you are searching. A list appears which shows all the applicable objects which fit your search in all the Domains.

You can select to see all search results or only results of unused objects.

To view unused objects:

1. In the Multi-Domain view, click the drop-down arrow in the main menu and select **Open Global Object Explorer**.

   The **Global Object Explorer** window opens.

2. In the upper left corner, select **Unused Objects**.

A list appears with all the unused object in all the Domains..

To see where an object is used

1. In the Multi-Domain view, click the drop-down arrow in the main menu and select **Open Global Object Explorer**.

   The **Global Object Explorer** window opens.

2. Navigate to the applicable object.

3. Right-click the object and select **Where Used**.

A list appears with all the places where the object appears in all the Domains.

Notes:

- Cross-Domain Search is supported only on Domains defined on a Multi-Domain Server, to which the user is connected with SmartConsole.
- Cross-Domain Search is supported only on Domains, for which the connected user has Read or Read/Write permissions.

Global Management

This section describes how to connect to the Global Domain, create a Global Policy, create Global Assignments, update IPS Protections and the Application & URL Filtering Database.

The Global Domain

The **Global Domain** is a collection of rules, objects and settings shared with all Domains or with specific Domains. The system automatically creates the Global Domain when you install Multi-Domain Security Management. You cannot delete the Global Domain. You cannot create additional Global Domains.

You organize global rules, objects and settings into *global configurations*. Each global configuration can include one or more of these components:

- One **Global Access Control Policy** - Global rules that control access to network resources. This includes rules for Firewall, Application Control, URL Filtering, and IPsec VPN. The **Network** Policy Layer is created automatically after installation or upgrade. You can manually create an Application or other Global Policy Layers as necessary.
- One **Global Threat Prevention Policy** - Global rules that prevent malware, intrusions and other threats. This includes rules for IPS, Anti-Bot, Anti-Virus, and other Threat Prevention features. The Threat Prevention Policy Layer is created automatically after installation or upgrade.
- **Global Objects** - System objects and configuration settings that are common to all or to specific Domains. Connect to the Global Domain with SmartConsole to create and configure global objects.

Connecting to the Global Domain

To connect to the Global Domain:

1. Connect to the Multi-Domain Server with SmartConsole.
2. In the **Domains** view, right-click the Global Domain, and then click **Connect to Domain**.

   A SmartConsole instance opens for the Global Domain.

Changing the Global Domain

This section includes basic procedures for working the contents of the Global Domain.

When connected to the Global Domain you can:

- Create, delete or change Global Access Control and Threat Prevention Policies.
- Create, delete or change rules in Global Policies.
- Create, delete or change global objects.

This activity is not supported in this release:

- Defining Security Gateways as installation targets in global configuration rules. You must use local Policies to do this.

Working with Global Objects

Use global objects in global configuration rules. Global objects work much in the same way as objects in local Policy rules.

The Global Domain includes many, predefined global objects for your convenience. These default global objects are visible (read only), in the Global Domain. You cannot delete or change them.

You can create, change or delete user-defined global objects in the Global Domain only. Global objects are visible in local Domains in the read-only mode.

Important:

- Before you delete a global object, make sure that no global or local policy rules use this global object. This can cause errors when you reassign global configurations.
- It is supported to add a global Host object only to a global Group object.
- It is supported to add a global Network object only to a global Network Group object.

To add a new global object:

1. Connect to the Global Domain with SmartConsole.
2. Click the **Objects** menu, and then select an object type from the menu.

   You can also create a new global object with the **Object Explorer**.
3. Configure the required parameters.
4. Click **OK** to save the new object.

To change a user-defined global object, select it in the **Object Explorer**, and then change the applicable settings.

To delete a user-defined object, select it in the **Object Explorer** and click **Delete**.

Important - After you complete the global object task, assign or reassign the global configuration to the applicable Domains. This action automatically:

- Publishes the changes that were done on the Multi-Domain Server
- Updates the local Domain and its Rule Base

Working with Global Configuration Rules

This section is a general overview of the procedure for defining rules in the Global Policies. To learn more about Policy rules and their configuration procedures, see the *R82 Security Management Administration Guide*.

Global Policy Layers have one placeholder for local Domain rules. You can create global rules above and below this placeholder. In the local Domain Policy Layer, you define local rules in the placeholder. If there are no local Domain rules, the placeholder can be empty.

The position of rules in Domain Policy Layers defines the order in which they are enforced. It is important to put rules in the correct sequence. Global Policy Layers do not have implied rules, but implied rules can be inherited from global properties in local Domains.

Best Practice - Define a global cleanup rule in each Policy Layer.

There is no NAT Rule Base in the Global Domain and you cannot define NAT settings there. You must define NAT rules manually in Domain Policy Layers.

Workflow for global Domain Policy Layers:

1. Connect to the Multi-Domain Server with SmartConsole.
2. In the **Domains** view, right-click the Global Domain, and then click **Connect to Domain**.

   A SmartConsole instance opens for the Global Domain.
3. Select **Access Control** and **Threat Prevention** Policy Layers and configure their rules.
4. Publish the SmartConsole session.
5. Go to **Multi-Domain** > **Global Assignments**, and assign the configuration to the local Domains. If you assigned the configuration before, and made changes to the Global Domain Policy, reassign the global domain configuration to the local Domains.

   The system creates a task, during which these actions occur:

   - Makes sure that all Global and local Domain Layer rules are consistent and work together correctly. For example, it makes sure that new local Policy Layers are connected to existing local Domain Policy Layers.
   - Updates the local Domain and its Rule Base.

- Publishes the changes again.
- Changes the assignment status to **Up to Date**.

6. Install Policies on the local Domains.

Policy Presets

SmartConsole lets you create Policy Presets for better policy installation planning. A Policy Preset is a collection of Security Gateways or Policy Packages for policy installation purposes. After you define a Preset, you can install policy on all the items which are included in the Preset at the same time. You also have the option to define a policy installation schedule for a specific Preset. In a large deployment Multi-Domain Server environment, Policy Presets help you save time and manage the policy installation process more efficiently.

You can create 2 types of Policy Presets:

- **By Gateways** - Policies are installed on all Security Gateways in the Preset. The applicable policy is installed on each Security Gateway in the Preset. A Preset can include Security Gateways from different Domains, from the same Domain, Security Gateways with different policies or identical policies.
- **By Policy Packages** - All Policy Packages included in the Preset are installed on the Security Gateways that enforce it at the same time.

Note - A Preset by Policy Packages installs policy only on Security Gateways which enforce the selected Policy Packages included in the Preset. It does not necessarily install policy on all Security Gateways in a Domain.

You can use Presets for policy installation only after you installed policy on the installation targets for the first time. Security Gateways with no policy installed on them are skipped during the installation process.

To create a Policy Preset:

1. In the Multi-Domain view, go to **Multi-Domain** > **Install Policy Presets** > **New**.
2. In **Installation Targets**, select one of these options:
   - **By Gateways** - This Policy preset is installed on the Security Gateways that you select.
   - **By Policy Packages** - This Policy preset is installed on the Security Gateways which enforce the selected Policy Packages.
3. In **Policy Types**, select which policy to install: Access Control policy, Threat Prevention policy, or both.
4. In **Scheduling**:

   You can schedule the policy installation to specific days and hours.

The hour of the policy installation is set to the time zone of:

- The SmartConsole client - for a one-time installation.
- The Multi-Domain Management Server - for a recurring installation.

Use Case - Time Set for a Recurring Installation

In a one time installation, the installation time is according to the SmartConsole client. In a recurring installation, the installation time is according to the Multi-Domain Server. This affects how you set both the hour and the day on your local SmartConsole client.

Example 1:

Your SmartConsole client is in Israel, and your Multi-Domain Server is in New York.

- You want to schedule a recurring installation on Saturday 2 PM Israel time (14:00):

  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select:

  Install policy at 14:00

  Recurrence > **Configure** > **Days in week** > **Saturday**

- You want to schedule a recurring installation on Saturday 2 PM New York time (14:00):

  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select: **Install policy at 21:00**

  Recurrence > **Configure** > **Days in week** > **Saturday**

Example 2:

Your SmartConsole client is in Israel, and your Multi-Domain Server is in New York.

- You want to schedule a recurring installation on Saturday 6 PM Israel time (18:00):

  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select:

  Install policy at 18:00

  Recurrence > **Configure** > **Days in week** > **Saturday**

- You want to schedule a recurring installation on Saturday 6 PM New York time (18:00):

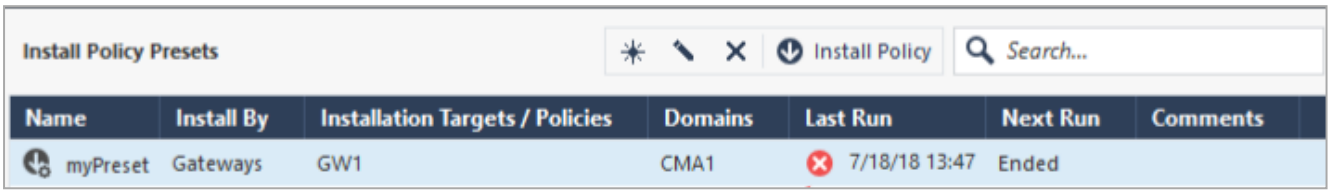
  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select: **Install policy at 01:00**

  Recurrence > **Configure** > **Days in week** > **Sunday**

Note - The hour of the policy installation is set to the time zone of:
- The SmartConsole client - for a one-time installation.
- The Multi-Domain Management Server - for a recurring installation.

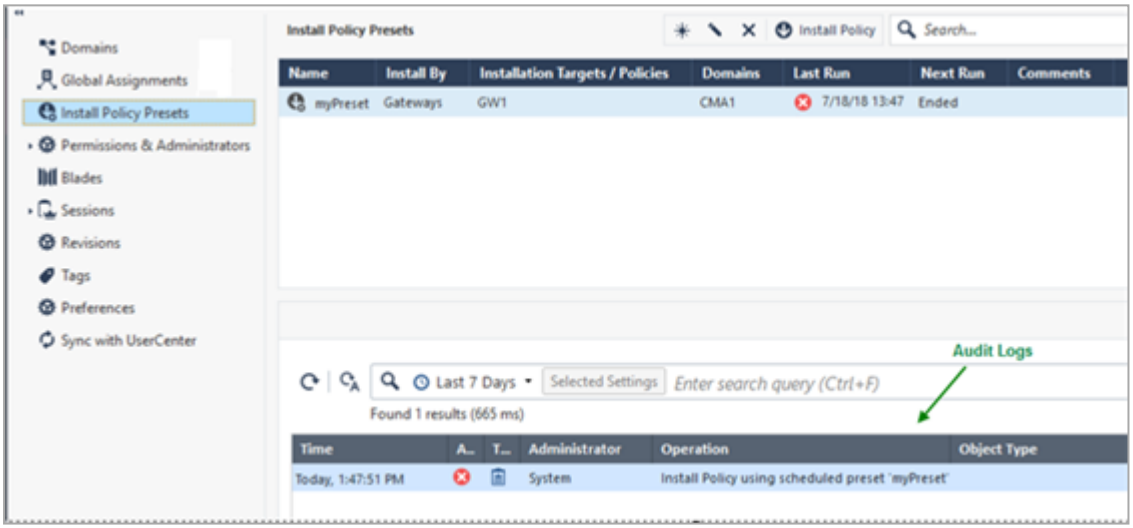
5. Publish the SmartConsole session.

You can see the next policy installation schedule in the **Next Run** column:



At any time, you can select a Preset and click **Install Policy**, regardless of the preset schedule.

The audit logs of your Preset activity show at the bottom of the **Install Policy Presets** page and in the Logs & Events view.



Note - The policy preset is installed on the Multi-Domain Server with the active global Domain. If a domain has no domain server on the Multi-Domain Server with the active global Domain, then the policy preset is not installed on this Domain.

Use Case - Installation on multiple Multi-Domain Servers

In this example, the Global policy will not be installed on Domain 2, because Domain 2 has no server in Multi-Domain Server2.

Servers Domains	Multi-Domain Server 1	Multi-Domain Server 2
Domain1	Domain1_Server (Active)	Domain1_Server_2 (Standby)
Domain2	Domain2_Server (Active)	No Server

Servers Domains	Multi-Domain Server 1	Multi-Domain Server 2
Global	Standby	Active

Use Case - Time Set for a Recurring Installation

In a one time installation, the installation time is according to the SmartConsole client. In a recurring installation, the installation time is according to the Multi-Domain Server. This affects how you set both the hour and the day on your local SmartConsole client.

Example 1:

Your SmartConsole client is in Israel, and your Multi-Domain Server is in New York.

- You want to schedule a recurring installation on Saturday 2 PM Israel time (14:00):

  In your SmartConsole client > **New Install Policy Preset**> **Scheduling**, select:

  Install policy at 14:00

  Recurrence > **Configure** > **Days in week** > **Saturday**

- You want to schedule a recurring installation on Saturday 2 PM New York time (14:00):

  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select: **Install policy at 21:00**

  Recurrence > **Configure** > **Days in week** > **Saturday**

Example 2:

Your SmartConsole client is in Israel, and your Multi-Domain Server is in New York.

- You want to schedule a recurring installation on Saturday 6 PM Israel time (18:00):

  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select:

  Install policy at 18:00

  Recurrence > **Configure** > **Days in week** > **Saturday**

- You want to schedule a recurring installation on Saturday 6 PM New York time (18:00):

  In your SmartConsole client > **New Install Policy Preset** > **Scheduling**, select: **Install policy at 01:00**

  Recurrence > **Configure** > **Days in week** > **Sunday**

Use Case - Mail Security Servers

You are the administrator for a corporation that has five branches, each branch in a different city. You manage the Security Gateways from a Multi-Domain console. In the Multi-Domain console, each branch is represented by a Domain. Each Domain has a mail security server. When there is a mail-related update, you must update the policy on all mail security servers (no update is required for the other Security Gateways in each Domain). How can you make the policy installation process more efficient?

Create a Preset which includes the mail security server in each Domain. After you create this Preset, each time it is necessary to update the Policy on the mail security servers, you can select this preset for installation. This way, you do not need to search and filter for each mail security server separately.

You can also schedule the policy installation for specific days and hours, for example, in the evening hours, when there are fewer employees at work.

Sample Access Control Policy Layer

Global Access Control rules use a placeholder for local Domain rules. The position of this placeholder in the Rule Base controls the order that Security Gateways handle global and local Policy rules. For simplicity of presentation, this example shows one Global Policy Layer that has both Network and Application rules. In the real world, there are different Policy Layers for these two rule types.

Sample Global Policy Layer

No.	Name	Source	Destination	VPN	Services & Applications	Action
1	Traffic from Management Server to Security Gateway	Security Gateway objects Management Server	Management Server Security Gateway objects	Any	Any	Accept
2	FB & Twitter	Internal Net	Any	Any	Facebook Twitter	Drop
3	Placeholder for Domain Rules					Domain Layer
4	DMZ Notify	Internal Net	DMZ Net	Any	Any	Inform
5	Cleanup	Any	Any	Any	Any	Drop

In this example, the placeholder for local Domain rules is rule number 3. Global Domain rules 1 and 2 run before the local Domain rules. Global rule 4 and the cleanup rule run after the local Domain rules.

Each local Domain Policy includes both Global Domain Policy rules and local Domain rules that apply to its Security Gateways. Local Domain Policy rules show in a Domain Layer under a parent rule.

Sample Domain Policy Layer with Global and Local Domain Rules

No.	Name	Source	Destination	VPN	Services & Applications	Action
1	Traffic from Management Server to Security Gateway	Security Gateway objects Management Server	Management Server Security Gateway objects	Any	Any	Accept
2	FB & Twitter	Internal Net	Any	Any	Facebook Twitter	Drop
3	Parent Rule for Local Domain Policy					
3.1	External to SD server	External Net	Host_ 10.10.10.11	Any	Any	Accept
3.2	Finance	Finance Top Mgmt.	Finance Dept	Any	Any	Accept
3.3	File Sharing Allowed	Any	Any	Any	Dropbox Google Docs CP Threat Cloud	Accept
4	DMZ Notify	Internal Net	DMZ Net	Any	Any	Inform
5	Cleanup	Any	Any	Any	Any	Drop

In this example, the Security Gateways handle the global configuration rules (1 and 2) and then the local Domain rules. If there is still no match in the local rules, the Security Gateways handle the last two global rules, including the cleanup rule..

Although a local Domain can define implied rules, it is a best practice to put critical global rules at the beginning of the Rule Base. Put the global cleanup rule at the end. This overrides the implicit cleanup rule and gives you flexibility to define an effective sequence for local Domain rules. .

Sample Threat Prevention Policy Layer

Global Threat Prevention rules use a placeholder for local Domain rules. The position of this placeholder in the Rule Base controls the order that Security Gateways handle global and local Policy rules. The first rule that matches traffic generates the specified action.

Sample global Policy Rule Base

No.	Name	Protected Scope	Protection Site	Action	Track	Install On
1	Max Security	Portal Server Finance Server	N/A	Strict	Alert Packet Capture	Policy Targets
Global Exceptions (No Rules)						
E-1.1	MS Office False Positives	Any	MS Word MS Publisher MS Excel	Detect	Log Packet Capture	Policy Targets
2	Printers & Other Devices	Peripheral Net	N/A	Basic	Log Packet Capture	Policy Targets
Global Exceptions (No Rules)						
3	Parent Rule for Domain Policy			Domain Layer		
4	Cleanup	Any	N/A	Optimized	Log Packet Capture	Policy Targets
Global Exceptions (No Rules)						

In this example, the local Domain placeholder is rule number 3. Global Domain rules 1 and 2 run before the local Domain rules. Global Domain rule 4 is the default rule that runs after the local Domain rules.

Each Domain Policy includes both global rules and local rules that apply to its Security Gateways. Local Domain Policy rules show in a local Domain Layer under a parent rule.

Sample Domain Rule Base with global and local Domain Rules

No.	Name	Protected Scope	Protection Site	Action	Track	Install On
1	Max Security	Portal Server Finance Server	N/A	Strict	Alert Packet Capture	Policy Targets
Global Exceptions (No Rules)						
E-1.1	MS Office False Positives	Any	MS Word MS Publisher MS Excel	Detect	Facebook Twitter	Policy Targets
2	Printers & Other Devices	Peripheral Net	N/A	Basic	Log Packet Capture	Policy Targets
Global Exceptions (No Rules)						
3	Placeholder for Domain Policy			Domain Layer		
3.1	Management Threats	Management	N/A	Optimized	Log Packet Capture	Policy Targets
3.2	Guests	Guest	N/A	Strict	Log Packet Capture	Policy Targets
4	Cleanup	Any	N/A	Optimized	Log Packet Capture	Policy Targets

This example shows Policy Layer with Global Domain rules together with the local Domain rules.

Using Layers with the Global Domain

- You create Global Access Control and Threat Prevention Policy Layers in the Global Domain. You configure Local Domain Policy Layers in the applicable local Domains.
- The Global **Network** Policy Layer is created automatically, but you can manually create a Global **Application** Layer. The Global Threat Prevention Layer is created automatically. If your policy installation targets contain Security Gateways R77.30 or lower, the Network and Application layers are the only supported layers. Do not create more Policy Layers.
- In each Policy Layer, the position of the local Domain Policy Layer is defined by the position of its placeholder in the Rule Base. You can add global rules above or below the placeholder. You can define Threat Prevention rule exceptions for Global and local Domain Policy Layers.
- You can temporarily disable the local Domain Policy Layer.

  In SmartConsole for the applicable local Domain, right-click in the **No** column of the placeholder, and then select **Disable**. The Domain Policy shows as grayed-out.

  To re-enable it, right-click the same cell, and select **Disable** again. Publish the SmartConsole session.

  Note - You cannot disable local Policy Layers in the Global Domain. This option is not available.
- To delete the rules from a local Domain Layer, click the pencil icon in the **Action** column, and select **No domain rules** in the local Domain. Publish the SmartConsole session.
- To use a different Domain Policy Layer, click the pencil icon in the **Action** column, and select a different Domain Policy Layer from the list. Publish the SmartConsole session.

Upgrade Issues

When you upgrade an R77.X or earlier Multi-Domain Server, existing Policies are converted in this manner:

- If a pre-R80.x Policy has a Global Access Control Policy with no defined rules (placeholder only), its mode is automatically set to **no global Policy** after an upgrade to R80.x. You can change the mode as necessary for both R80.x and pre-R80.x Policies.
- The **Firewall** Policy is converted into an R80.10 **Network** Policy Layer. Its implicit cleanup rule is set to **Drop**.
- The **Application & URL Filtering** Policy is converted to the **Application** Policy Layer. The implicit cleanup rule for it is set to **Accept**.
- If a Domain contains **IPS** rules, an IPS Layer is automatically created in the R80.x Threat Prevention Policy for the applicable Domain.

Policy Layers and Administrator Permissions

The use of Policy Layers lets you define granular permissions for different aspects of security management. In a typical organization, only administrators with **Global Management** or **Superuser** privileges can work with Global Policy Layers. **Domain Managers** or **Domain Level Only** administrators typically have permissions to work with specified Policy Layers in their local Domains.

Dynamic Objects and Dynamic Global Objects

Dynamic objects are "logical" network objects for which IP addresses or address ranges are not explicitly defined. You define dynamic objects in the Global Domain and use them in global configuration rules. The dynamic objects are resolved to local objects when you assign the global policy to the local Domains.

You can create dynamic objects for most object types, including Security Gateways, hosts, services, networks and groups. Use the standard global objects available in SmartConsole or create your own global objects. All dynamic objects must have the `_global` suffix, which identifies the objects as global.

There are two types of dynamic objects:

- **Dynamic Global Network Objects** - In each Domain, you define a host object with the same name as the global dynamic object. During the assignment of the global policy, the references to the global dynamic object in different rules are replaced by the reference to the local host object with the same name. The *_global* syntax triggers the reference replacement mechanism.
- **Dynamic Objects** - The dynamic object is assigned an IP at the Security Gateway level, when you assign the global configuration to a Domain and install Policies on the Security Gateways. There is no need to create a corresponding local object.

The use of dynamic objects makes it possible to create global rules with no specified network objects. This lets you create rules that are templates.

Defining Rules with Dynamic Objects

To create a new global dynamic object:

1. Connect to Global Domain SmartConsole.
2. In the **Object Explorer**, select **New** > **Network Objects** > **Dynamic Object**.
3. Select:
   - **Dynamic Global Network Object** - The dynamic global object is replaced by a matching Domain object,

   Or

- **Dynamic Object** -The dynamic object is assigned an IP at the Security Gateway level.

4. In the **New Dynamic Object** window, enter a name.

   For the Dynamic Global Network Object, the name must have the suffix `_global`. For example, `FTP_Server_global`.

5. Drag the dynamic object to the applicable cells in the global Rule Base.
6. Publish the SmartConsole session.
7. Assign the Global Policy to all the applicable Domains.

To use a dynamic global network object in a local Domain rule:

1. Connect to SmartConsole for each applicable Domain.
2. In each Domain, create a local object with the same name as the Dynamic Global Network Object, with the `_global` suffix.

   The local object must include the applicable local parameters, such as the IP address.

When you assign the global policy to the local Domain, the local object replaces this Dynamic Global Network Object.

For Dynamic Objects, there is no need to create an equivalent local object.

Applying Global Rules to Security Gateways by Function

You can create Security Rules in Global Domain that are installed on some Security Gateways or groups of Security Gateways and not others. This way, Security Gateways with different functions on one Domain can receive different security rules for a specified function or environment. When you install global policy to a number of similarly configured Domains, the related global rules are installed to all of the related Security Gateways on each Domain.

This feature is particularly useful for enterprise deployments of Multi-Domain Security Management, where Domains typically represent geographic subdivisions of an enterprise. For example, an enterprise deployment may have Domains for business units in New York, Boston, and London, and each Domain is similarly configured, with a Security Gateway (or Security Gateways) to protect a DMZ, and others to protect the perimeter. This capability lets you configure the global policy so that some global security rules are installed to DMZ Security Gateways, and different rules are installed to the perimeter Security Gateways.

Note - Global security rules can be installed on Security Gateways, and Open Security Extension (OSE) devices.

To install a specified security rule on a specified Security Gateway or types of Security Gateways:

1. Connect to the Global Domain for the related Global Policy.
2. In the **Objects Categories** tree, go to **New** > **Network Object** > **Dynamic Objects** and select **Dynamic Global Network Object**.
3. Name the dynamic object, and add the suffix `_global` to the end of the name.
4. Create rules to be installed on Security Gateways with this function, and drag the dynamic object you created into the **Install On** column for each rule.
5. Launch SmartConsole for each related Domain.
6. Create a group object with the name of the dynamic object you created, including the suffix `_global`.

   Best Practice - While you can give a Security Gateway a name of the global dynamic object, we recommend to create a group to preserve future scalability (for instance, to include another Security Gateway with this function). We do not recommend changing the name of an existing Security Gateway to the dynamic object name.
7. Add to the group all the Security Gateways on the Domain that you want to receive these global security rules.
8. From the Multi-Domain Security Management view, re-assign the global policy to the related Domains.

Creating a Global Policy in the Global SmartConsole

You create Global Policies in the Global SmartConsole. You create Domain policies in the SmartConsole launched using the Domain Management Server. Let us consider an MSP that wants to implement a rule which blocks unwanted services at Domain sites. The Multi-Domain Security Management Superuser, Carol, wants to set up a rule which lets the Domain administrators decide which computers are allowed to access the Internet.

Source	Destination	VPN	Service	Action
MyRule	Any	Any	Any	Accept

After she created a Global Policy which includes this rule, she assigns and installs it to specific Domains and their Security Gateways. Each Domain administrator must create a group object with the same name as in the Domain Management Server database. This is done in SmartConsole. This way, local administrators translate the dynamic global object into sets of network object from the local database.

For details about how to use the SmartConsole, see the *R82 Security Management Administration Guide*.

These are the differences between the Domain SmartConsole and the Global SmartConsole:

Feature	Domain SmartConsole	Global SmartConsole
Rule Base	Local, applying to the Domain network only.	Global, applying to multiple networks of all Domains assigned this Global Policy.
	Domain Security Rules and Global Rules (in Read Only mode) if the Global Policy is assigned to the Domain.	Global Rules and a place holder for Domain rules.
	Not associated with the Domain other security policies.	Automatically added to all of the assigned security policies of Domains.
	Each Domain policy is independent, with its own rules.	All the assigned Domain policies share the global rules.
Network Objects	Local to this network only.	Global to multiple networks of all Domains assigned this Global Policy.
Global Properties	Enabled.	Disabled (manipulations is through the Domain SmartConsole).
Saving a Security Policy	Adds the security policy to the list of Domain security policies.	Adds the Global Policy to the Global Policies database (and displays it in the **Global Policies** Tree of SmartConsole).

Note - You cannot use the Global SmartConsole to create Security Gateway objects. Instead, use a SmartConsole connected to a specific Domain Management Server to create these objects.

Global Assignments

A *global assignment* is a Multi-Domain Security Management system object that assigns a global configuration to one specified Domain. You create global assignments to assign different combinations of Global Access Control Policies, Global Threat Prevention Policies, and global object definitions to different Domains.

When you create a new global assignment, it automatically assigns the specified global configuration to the specified Domain. It also publishes the assignment and updates local Domain Policies.

Best Practice - When you create a new Domain, create a global assignment for that Domain at the same time.

When you do one or more of these actions, you must publish the Global Domain session and *reassign* the global configuration:

- Add, delete, or change rules in a global configuration
- Add, delete, or change user-defined objects in a global configuration
- Define the SmartEvent object in the global database
- Change the definition of a global assignment

The assign/reassign action does not automatically install Policies.

Best Practice - Install Policies after you assign or reassign a global assignment.

Configuring an Assignment

To create a new global assignment:

1. Connect to the Multi-Domain Server with SmartConsole.
2. Go to **Multi-Domain** > **Global Assignments**.
3. Click **Assign** > **New Assignment**.
4. In the **New Assignment** window, select a **Local Domain**.
5. Optional: Select a Global **Access Control Policy** for this local Domain.

   You can click **Advanced** to open the **Advanced Assignment** window to assign the selected Policy:

   - Only to the specified, local Domain Policies
   - To all local Domain Policies, except for those explicitly specified
6. Optional: Select a Global **Threat Prevention Policy** for this local Domain.

You can click **Advanced** to open the **Advanced Assignment** window to assign the selected Policy:

- Only to the specified, local Domain Policies
- To all local Domain Policies, except for those explicitly specified

7. Optional: Enable **Manage protection actions**.

   This option lets you change IPS protection actions for Security Gateways on the local Domain.

8. Click **Assign**.
9. In the confirmation window, click **Publish & Assign**.

   The system creates a task, which:

   - Updates the local Domain and its Rule Base
   - Publishes the changes
   - Changes the assignment status to **Up to Date**

To change an existing global assignment:

1. Connect to the Multi-Domain Server with SmartConsole.
2. In the **Global Assignments** view, double-click a Domain.
3. In the **Assignment** window, follow steps 4-6 above.
4. Click **Assign**.
5. In the confirmation window, click **Publish & Assign**.

   The system creates a task which:

   - Updates the local Domain and its Rule Base
   - Publish the changes
   - Changes the assignment status to **Up to Date**

Important - You can create a global assignment that does not include a Global Access Control and Threat Prevention Policy. To do this, select the **None** value to both Policy types. The global configuration assigns only the defined global objects and settings to Domains.

Reassigning

When you make changes to the global configuration items, the assignment status changes to **Not up to date**. The assignment status does not change if you make changes to the local Domain Policies.

To reassign global configurations:

1. Connect to the Multi-Domain Server with SmartConsole, and then click **Global Assignments**.
2. In the **Global Assignments** window, right-click one or more Domains.

   You can reassign to more than one Domain at the same time.
3. Click **Reassign**.

   The system creates a task which:

   - Updates the local Domain and its Rule Base
   - Publishes the changes
   - Changes the assignment status to **Up to Date**.

Handling Assignment Errors

Global assignments run as a task that you can monitor while you work on other tasks.

To monitor assignment/reassignment tasks:

1. In the **Multi-Domain** view, click the task information area.

   The **Recent Tasks** window opens.
2. Find the assignment task.

   If your task does not show, click **Show More**.
3. Click **Details**.

   The **Assignment Task Details** window shows the task progress and details.
4. If the task fails and returns an error message, correct the error, and then try to assign/reassign the global configuration again.

Some common errors include:

- Global objects with duplicate or illegal names
- Deleted global objects used in a rule
- Global rule validation errors

Deleting a Global Assignment

When you delete a global assignment, the global configuration rules and objects no longer apply to its Domain.

Best Practice - Immediately create a new global assignment so that Domain Security Gateways continue to enforce global configuration rules.

Important - You must remove global objects from all local Domain rules before you can delete a global assignment. If there is a rule that uses a global object when you try to delete a global assignment, the delete operation fails.

To delete a global assignment:

1. In the **Global Assignments** view, select a Domain.
2. Click the **Delete** icon on the **Actions** toolbar.
3. In the **Remove** window, select an assignment, and then click **Remove**.

Global Assignment Status

You can see the global assignment status in the **Assignment Up to Date** column, in the **Multi-Domain** > **Global Assignments** view. For each Domain, the date of the last assignment shows together with a status icon:

- Assignment is up to date - no action necessary.
- The global configuration is not assigned or the assignment is not up to date. Assign or update the global configuration as soon as possible.

Updating IPS Protections

Check Point continuously develops and improves its protections against emerging threats. You can manually update the database with latest IPS protections. You must also configure the Global Domain to automatically download contracts and other important data.

Note - Security Gateways with IPS enabled only get the updates after you install Policy.

For troubleshooting or for performance tuning, you can revert to an earlier IPS protection package.

To manually update the IPS protections:

1. Connect to the Global Domain with SmartConsole >
2. Go to **Security Policies > Threat Prevention**>
   - **Custom Policy** > **Custom Policy Tools**

     or (depending on your Threat Prevention policy)
   - **Autonomous Policy** > **Autonomous Policy Tools**
3. Go to **Updates** > **IPS**, and click **Update Now**.
4. Connect to the Multi-Domain Server with SmartConsole.
5. Reassign the global configuration.

To revert to an earlier protection package:

1. Connect to the Global Domain with SmartConsole.
2. Go to **Security Policies > Threat Prevention** >
   - **Custom Policy** > **Custom Policy Tools**

     or (depending on your Threat Prevention policy)
   - **Autonomous Policy** > **Autonomous Policy Tools**
3. Go to **Updates** > **IPS** > **Update Now**, click the drop-down menu and select **Switch to version**
4. In the window that opens, select an **IPS Package Version**, and click **Switch**.
5. Connect to the Multi-Domain Server with SmartConsole.
6. Reassign the global configuration.

To make sure that Contract Downloads is enabled:

1. In each Domain, go to the main menu > **Global Properties**.
2. From the navigation tree, select **Security Management**.
3. Make sure that **Automatically download contracts and other important data** is selected.

   This parameter is enabled by default. If it is not enabled, select it.

Updating the Application & URL Filtering Database

Check Point constantly develops and improves its protections against the latest threats. You can manually update the Application & URL Filtering database with the latest applications and URLs.

To manually update the Application & URL Filtering protections:

1. Connect to the Global Domain with SmartConsole.
2. Click **Security Policies > Access Control**.
3. In the **Access Tools** section, click **Updates**.
4. In the **Application & URL Filtering** section, click **Management Update**.
5. Connect to the Multi-Domain Server with SmartConsole.
6. Assign or reassign the global configuration.

SmartTasks

Management SmartTasks let you configure automatic actions according to different triggers in the system. A SmartTask is a combination of trigger and action.

- Triggers are events – currently defined in terms of existing management operations, such as installing a policy or publishing a session.
- Actions are automatic responses that take place after the trigger event , such as running a script, posting a web request or sending email.

Starting from R82 Jumbo Hotfix Accumulator Take 60, the Global Domain in Multi-Domain Security Management supports SmartTasks. The process to enable, configure, and monitor SmartTasks in the Global Domain is the same as the workflow for SmartTasks in a regular domain. See the *R82 Security Management Administration Guide*.

Exceptions

This chapter explains exceptions and exception groups, how to create them, and the difference between global exceptions and local exceptions.

Exception Rules

If necessary, you can add an **exception** directly to a rule.

An exception sets a different **Action** to an object in the **Protected Scope** from the Action specified Threat Prevention rule.

In general, exceptions are designed to give you the option to reduce the level of enforcement of a specific protection and not to increase it.

Example

The Research and Development (R&D) network protections are included in a profile with the **Prevent** action.

You can define an exception which sets the specific R&D network to **Detect**.

For some Anti-Bot and IPS signatures only, you can define exceptions which are stricter than the profile action.

You can add one or more exceptions to a rule. The exception is added as a shaded row below the rule in the Rule Base.

It is identified in the **No** column with the rule's number plus the letter E and a digit that represents the exception number.

For example, if you add two exceptions to rule number 1, two lines will be added and show in the Rule Base as E-1.1 and E-1.2.

You can use exception groups to group exceptions that you want to use in more than one rule. See the **Exceptions Groups** Pane.

You can expand or collapse the rule exceptions by clicking on the minus or plus sign next to the rule number in the **No**. column.

To add an exception to a rule

Step	Instructions
1	In the **Policy** pane, select the rule to which you want to add an exception.
2	Click **Add Exception**.

Step	Instructions
3	Select the **Above**, **Below**, or **Bottom** option according to where you want to place the exception.
4	Enter values for the columns. Including these: ■ **Protected Scope** - Change it to reflect the relevant objects. ■ **Protection** - Click the plus sign in the cell to open the Protections viewer. Select the protection(s). Click **OK**.
5	Install the Threat Prevention Policy.

Note - You cannot set an exception rule to an inactive protection or an inactive blade.

Disabling a Protection on One Server

*Scenario: The protection Backdoor.Win32.Agent.AH blocks malware on windows servers. How can I change this protection to **detect** for one server only?*

In this example, create this Threat Prevention rule, and install the Threat Prevention policy:

Name	Protected Scope	Protection/Site	Action
Monitor Bot Activity	* Any	- N/A	A profile based on the **Optimized** profile. Edit this profile > go to the **General Policy** pane> in the **Activation Mode** section, set every **Confidence** to **Prevent**.
Exclude	Server_1	Backdoor.Win32.Agent.AH	**Detect**

To add an exception to a rule

Step	Instructions
1	In SmartConsole, go to Security Policies > **Threat Prevention > Custom Policy**.
2	Click the rule that contains the scope of **Server_1**.

Step	Instructions
4	Right-click the rule and select **New Exception**.
5	Configure these settings: ■ **Name** - Give the exception a name such as **Exclude**. ■ **Protected Scope** - Change it to **Server_1** so that it applies to all detections on the server. ■ **Protection/Site** - Click **+** in the cell. From the drop-down menu, click the category and select one or more of the items to exclude. **Note** - To add EICAR files as exceptions, you must add them as Allow List files. When you add EICAR files through Exceptions in Policy rules, the gateway still blocks them, if archive scanning is enabled. ■ **Action** - Keep it as **Detect**. ■ **Track** - Keep it as **Log**. ■ **Install On** - Keep it as **Policy Targets** or select specified gateways, on which to install the rule.
6	Install the Threat Prevention Policy.

Creating an Exception for a Specific Protection, Site, File or Blade

To add a protection to an exception

Step	Instructions
1	In SmartConsole, select **Security Policies > Threat Prevention**.
2	From the navigation tree, select a **Policy Layer**.
3	Right-click the rule and select **New Exception**. An exception sub-rule is added to the policy.
4	Right-click the **Protection/Site/File/Blade** cell and select **Add new items**.

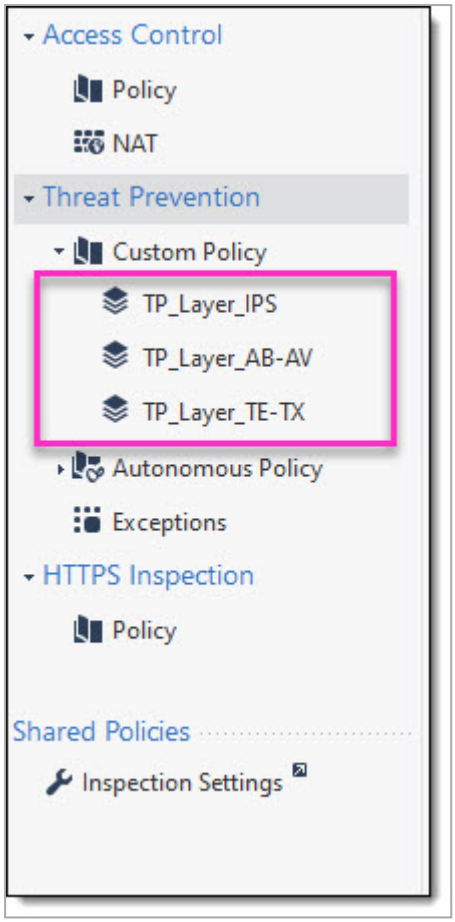
Step	Instructions
5	From the drop-down list, select the relevant category (**IPS Protections, Anti-Bot & Anti-Virus Protections, User Applications, Whitelist Files, Blades**) and then select the required item. The protections are added to the exception sub-rule. **Notes**: ■ There are no DNS protections in this drop-down menu. To add an exception to a DNS protection, you must go to the relevant log and add it from there. ■ To add an exception for an IPS protection, you can also go to **Security Policies > Threat Prevention > Custom Policy > IPS Protections**, right-click a protection and select **Add Exception**.
6	Install Policy.

You can create a rule or exception for a specific blade for a specific website/URL because the Security Gateway is always the destination in non-transparent proxy mode.

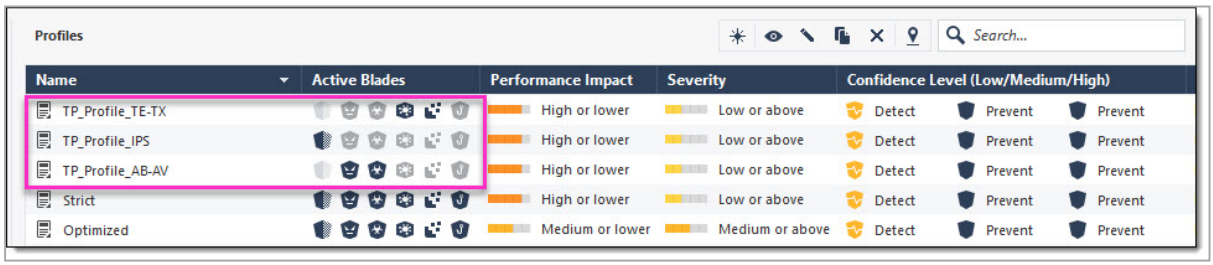
In a transparent proxy mode, or while the traffic is inspected by a Security Gateway, this setup is not a challenge because the destination is configured in the Destination column, and the excluded blade is configured in the Protection/Site/File/Blade column. This is not possible in non-transparent mode because the destination is always the Security Gateway itself.

To create an exception for a specific Threat Prevention blade for a specific website in non-transparent proxy mode

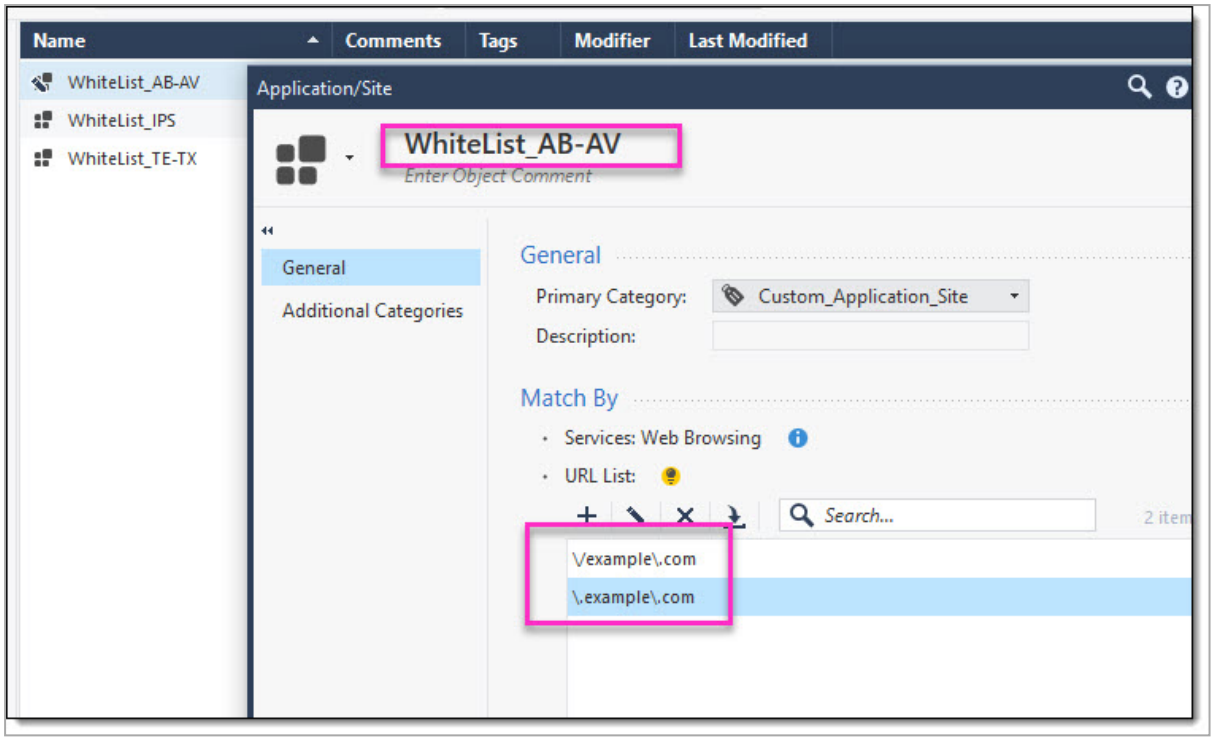
1. Create a separate layer with a separate profile for each blade or a pair of blades (for example: Anti-Virus and Anti-Bot & Advanced DNS, or Threat Emulation and Threat Extraction):



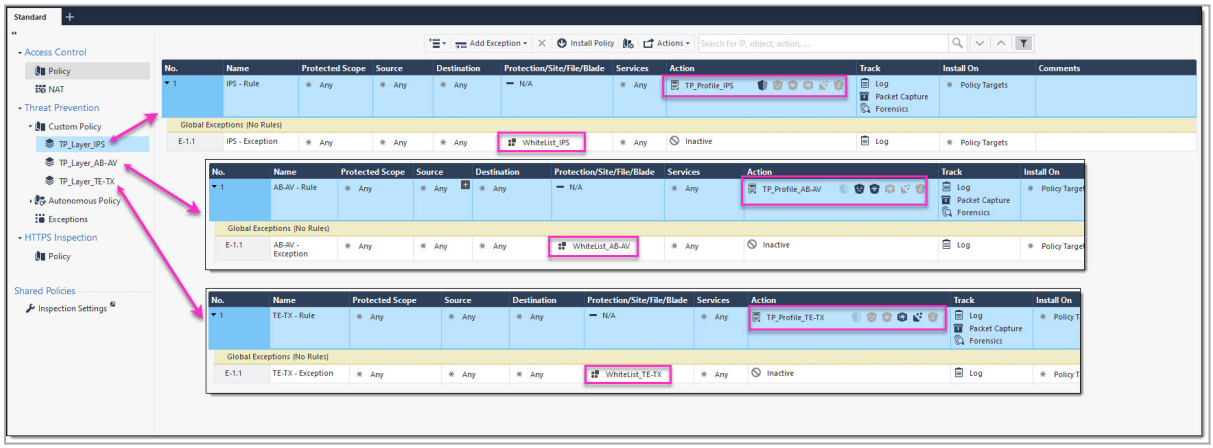
2. Create a separate profile for each layer and enable only the specific blade:



3. Create a custom Application/Site for each layer. For instructions, refer to [sk165094:]



4. Create a Rule Base for each layer, and a different exception rule with the created Custom Application/Site in Protection/Site/File/Blade:



5. In the **Action** column, select **Detect** or **Inactive** to disable the applicable Threat Prevention Blade for the applicable websites/URLs.

Notes:

- You must make changes to a Threat Prevention profile on all applicable profiles. For example: if you change the action for medium confidence protections on Threat Prevention blades, you must make the change in all profiles.
- We recommend to have as few layers as possible.
- When HTTPS Inspection and non-transparent proxy are enabled, the proxy IP address of the Security Gateway is matched as the destination in the HTTPS Inspection Rule Base.
- For a detailed explanation of the enforcement in Multiple-Layered Security Policies, see the *R82 Threat Prevention Administration Guide*.
- For information on how to configure a Security Gateway as HTTP/HTTPS proxy, see sk110013.

Creating Exceptions from Logs or Events

In some cases, after evaluating a log or an event in the **Logs & Events** view, it may be necessary to update a rule exception in the SmartConsole Rule Base.

You can do this directly from within the **Logs & Events** view.

You can apply the exception to a specified rule or apply the exception to all rules that appear below **Global Exceptions**.

To update a rule exception or global exception from a log

Step	Instructions
1	Click **Logs & Events** > **Logs** tab.
2	Right-click the log and select **Add Exception**.
3	Configure the settings for the exception.
4	In the **New Exception Rule** window: ■ To show the exception in the policy, click **Go to**. ■ Otherwise, click **Close**.
5	Install the Threat Prevention Policy.

Exception Groups

An exception group is a container for one or more exceptions. You can attach an exception group to all rules or only to selected rules. Exception groups simplify exception management, by allowing you to reuse the same exception group across multiple rules, instead of defining exceptions manually for each individual rule.

The **Exception Groups** pane shows a list of existing exception groups, the rules that use them, and any related comments.

The Exception Groups pane contains these options

Option	Meaning
New	Creates a new exception group.
Edit	Modifies an existing exception group.
Delete	Deletes an exception group.
Search	Searches for an exception group.

Global Exceptions

The system includes a predefined group named **Global Exceptions**. The system automatically adds exceptions that you define in the **Global Exceptions** group to every rule in the Rule Base. When you create a new exception group, you select which rule to attach it to.

Exception Groups in the Rule Base

Global exceptions and other exception groups are added as shaded rows below the applicable rule in the Rule Base. Each exception group is labeled with a tab that shows its name. Exceptions within a group are identified in the **No** column using this syntax:
`E - <rule number>.<exception number>`, where `E` identifies the line as an exception.

For example

In a **Global Exceptions** group that contains two exceptions, all rules show the exception rows in the Rule Base **No** column as E-1.1 and E-1.2.

Note - The numbering of exceptions varies when you move the exceptions within a rule.

To view exception groups in the Rule Base:

Click the plus or minus sign next to the rule number in the **No**. column to expand or collapse the rule exceptions and exception groups.

Creating Exception Groups

When you create an exception group, you create a container for one or more exceptions. After you create the group, add the exception rules to it. You can then attach the group to the applicable rules in the Threat Prevention Rule Base.

To create an exception group

Step	Instructions
1	In SmartConsole, select **Security Policies > Threat Prevention > Exceptions**.
2	In the **Exceptions** section, click **New**.
3	In **Apply On**, configure how the exception group is used in the Threat Prevention policy. ■ **Manually attach to a rule** - This exception group applies only when you add it to Threat Prevention rules. ■ **Automatically attached to each rule with profile** - This exception group applies to all Threat Prevention rules in the specified profile. ■ **Automatically attached to all rules** - This exception group applies to all Threat Prevention rules.
4	Click **OK**.
5	Install the Threat Prevention policy.

To add exceptions to an exception group

Step	Instructions
1	In SmartConsole, go to **Security Policies > Threat Prevention > Exceptions**.
2	In the **Exceptions** section, select the exception group to which you want to add an exception.
3	In the bottom pane of this page, click **Add Exception**.
4	Configure the new exception rule.
5	Install the Threat Prevention policy.

To add an exception group to a Rule Base

You can add exception groups to Threat Prevention rules.

This only applies to exception groups with **Manually attach to a rule** selected.

Step	Instructions
1	Click **Security Policies > Threat Prevention > Custom Policy**.
2	Right-click the rule and select **Add Exception Group**.
3	Select the applicable exception group from the list.
4	Install the Threat Prevention policy.

To create an exception for a specific file type, limited to a specific source and destination

Step	Instructions
1	In SmartConsole > go to **Security Policies** > **Threat Prevention** > **Custom Policy** > **Custom Policy Tools** > **Profiles**.
2	Click the icon to create a new profile.
3	In the **Threat Emulation** or **Threat Extraction** pages, select **General** > **File Types** > **Process specific file type families** > **Configure**.
4	Right-click the applicable file type and select **Bypass**.
5	Go to the **Exceptions** tab, and in the top pane, click the icon to create a new exception group.
6	In the **Exception Group** window that opens, select **Automatically attached to each group with profile**, and from the drop-down menu, select the newly created profile.
7	In the **Security Policies** view > **Threat Prevention** > **Exceptions** > select the newly created exception group.
8	At the bottom pane, create the required exception rule and define its **Source** and **Destination**.
9	Install the Threat Prevention policy.

Exceptions in a Multi-Domain Environment

In a Multi-Domain environment, there are 2 types of Global Exceptions:

- Global exceptions for the Global Domain
- Global Exceptions for each Local Domain

A Global Exception group for Threat Prevention is created automatically on the Global Domain and on each local Domain. You cannot delete these exception groups. The Global Exception group is empty by default and you can create exceptions manually for it. If you need additional Global Exception groups, you can create them manually.

In the Domain Rule Base for Threat Prevention, the Global Exceptions for the Global Domain appear under the Global rules, and the Global exception for the local Domain appear under the local rules.

Managing Administrators and Permissions

In a Multi-Domain Security Management environment, administrators manage system objects and settings, such as:

- Multi-Domain Servers and Multi-Domain Log Servers
- Domains and Domain Management Servers
- High Availability configuration and synchronization
- Domain Security Gateways, networks and other objects
- Domain Security Policies and rules
- Global Domain

Permission profiles let you assign permissions to Multi-Domain Security Management administrators, based on their area of responsibility. You can assign granular permissions to administrators that manage different elements of the Multi-Domain Security Management environment.

Configuring Administrators

To configure an administrator:

1. Connect to the Multi-Domain Server with SmartConsole, and go to **Permissions & Administrators** > **Administrators**.
2. Click **New**, or select an existing administrator and then click **Edit**.
3. In the **Administrator** view, configure the settings described in the next sections.

Notes:

- You cannot add additional information fields to the Administrator object.
- If two administrators create an administrator account with the same name, after the first administrator publishes a session, the second administrator cannot publish or edit their administrator account. To resolve the issue, the second administrator must discard the changes.

Administrator - General

Authentication

- **Name** - Enter a unique administrator name.
- **Authentication Method** - Select an authentication method and enter other authentication parameters as necessary. To learn more about the various authentication methods, see the *R82 Security Management Administration Guide*.

  To set a default value for this parameter, go to **Permissions & Administrators** > **Advanced** > **Administrator Settings** > **Authentication Default Values**. Select a default authentication from the list.
- **Certificate Information** - Optional: Click **Create** to generate a new certificate.
  - You can use a certificate with or without an authentication method.
  - For an existing administrator definition, you can revoke an existing certificate and create a new one.

Permissions

- **Multi-Domain Permission Profile** - Select a Multi-Domain permission profile from the list.

  Accept the default permission profile or select a different one. You can also create a new permission profile to assign. For an existing administrator, the currently selected permission profile shows.

  Click the **View** icon to see details of the currently assigned permission profile.

  If the **Edit** icon shows, you have permissions to see and change the currently selected permission profile. Click the **Edit** icon to change the settings.

  Permission Profiles per Domain -Select one or more Domains, and then select a Domain permission profile for each one.

  + - Click to select a Domain to add to the profile.

  X - Click to remove the selected Domain from the profile.

  Note - The **Permission Profiles per Domain Section** does not show for Superusers, because Read/Write Domain permission profiles are assigned automatically to all Domains.
- **Expiration** -Define when this administrator account expires.
  - **Never** - The administrator account does not expire.
  - **Expire at** - Select an expiration date for this administrator.

To set a default value for this parameter, go to **Permissions & Administrators** > **Advanced** > **Administrator Settings** > **Default Expiration Values**.

Contact Options

- **Email** - Enter the administrator email address.
- **Contact Details** - Enter additional contact information.
- **Phone** - Enter the administrator telephone number.

Note - If you upgraded from an earlier release, the system copies these values into the new release.

Creating a Certificate for Logging in to SmartConsole

When you define an administrator, you must configure the authentication credentials for the administrator.

The authentication credentials for the administrator can be one of the supported authentication methods, or a certificate, or the two of them.

You can create a certificate file in SmartConsole. The administrator can use this file to log in to SmartConsole using the *Certificate File* option. The administrator must provide the password for the certificate file.

You can import the certificate file to the CryptoAPI (CAPI) certificate repository on the Microsoft Windows SmartConsole computer. The administrator can use this stored certificate to log in to SmartConsole using the *CAPI Certificate* option. The SmartConsole administrator does not need to provide a password.

To create a certificate file

1. In the **New Administrator** window, in the **Certificate Information** section, click **Create**.
2. Enter a password.
3. Click **OK**.
4. Save the certificate file to a secure location on the SmartConsole computer.

The certificate file is in the PKCS #12 format, and has a `.p12` extension.

Note - Give the certificate file and the password to the SmartConsole administrators. The administrator must provide this password when logging in to SmartConsole with the **Certificate File** option.

To Import the certificate file to the CAPI repository

1. On the Microsoft Windows SmartConsole computer, double-click the certificate file.
2. Follow the instructions.

Working with Permission Profiles

A permission profile is a predefined set of permissions that you assign to administrators in a Multi-Domain Security Management environment. This lets you manage complex, granular permissions for many different administrators with one definition.

There are two types of permission profiles:

- **Multi-Domain permission profiles** - Defines administrator permissions for the full Multi-Domain Security Management environment.
- **Domain permission profiles** - Defines the permission set per Domain

Predefined Multi-Domain Permission Profiles

Multi-Domain Security Management includes predefined Multi-Domain and Domain permission profiles that are ready to use. You cannot delete or change these profiles. You can create custom permission profiles as necessary for your environment.

These are the predefined Multi-Domain permission profiles available in this release. In the **Permissions Profile** view, double-click each profile to see the permissions it includes:

Permission Profile	Permissions
Multi-Domain Superuser	Manage all elements of the Multi-Domain Security Management environment, including: Multi-Domain Servers, Multi-Domain Log Servers, Domains, Domain Management Servers, Global Policies, administrators and permission profiles. Multi-Domain Superusers manage all Domain objects, including Security Gateways, Policies, rules, networks and other objects.
Domain Superuser	Manage all Domains, Domain Management Servers, Domain networks, global objects, and global configurations. They manage Domain objects, including Security Gateways, Policies, rules, networks and other objects. Domain Superusers can create and manage other administrators, manage other administrators' sessions, and manage permission profiles at the same or lower levels. Domain Superusers cannot create or change the settings for Multi-Domain Servers or Multi-Domain Log Servers.
Global Manager	Manage Global Domains, global configurations, global rules, and global assignments. Global Managers can manage Domains, but not add or delete domains or manage Multi-Domain Servers. Global managers can manage administrators with equal or lower permissions. Global Managers can create new global assignments and can assign Global Policies to Domains that they have permissions to manage. Domain-Level permissions are based on the assigned Domain permission profile.

Permission Profile	Permissions
Domain Manager	Manage Domain Policies, networks and objects based on their permission profile. Domain Managers can manage administrators with equal or lower permissions. Domain Managers can reassign Global Policies to Domains that they have permissions to manage. They cannot create new global assignments. Domain-Level permissions are based on the assigned Domain permission profile.
Domain Level Only	Manage Domain Policies, networks and objects based on their permission profile. These administrators cannot manage the Multi-Domain Security Management system or its configuration settings, or login to the Multi-Domain Servers. Domain-Level permissions are based on the assigned Domain permission profile.

Pre-Defined Domain Permission Profiles

When you assign an administrator to Domain, you must also assign a Domain Permission Profile. You can assign a predefined Permission Profile or a custom Permission Profile for this administrator.

Permission Profile	Permissions
Read/Write	Read and write permissions for all Domain settings and data without session management or DLP confidential data. The **Read/Write** option lets the administrator see and configure an item.
Read Only	Read only permissions for all Domain data. Read Only lets the administrator see an item, but not change it.

Working with Multi-Domain Permission Profiles

Use this procedure to create or change customized Multi-Domain permission profiles. Only administrators with Superuser permissions can do this.

To create a custom permission profile

1. Connect to the Multi-Domain Server with SmartConsole, and go to **Permissions & Administrators** > **Permission Profiles**.
2. In the **Permission Profile** page, click **New**.
3. Select **New Multi-Domain Permission Profile**.

4. In the **New Multi-Domain Permission Profile** window, select an administrator role and configure the permission settings. The next section explains the available settings and parameters.

To change an existing Multi-Domain permission profile

1. Select a permission profile on the **Permission Profiles** page.
2. Click **Edit** and change the administrator role and permission settings as necessary.

To delete an existing Multi-Domain permission profile

1. Select a permission profile on the **Permission Profiles** page.
2. Click **Delete**.

Multi-Domain Permission Profile Parameters

Multi-Domain Levels

Select an administrator role:

- **Superuser** - Manage all aspects of the Multi-Domain Security Management environment.
- **Manager** - Manage Domains as specified in the **Permissions** section of Administrator definition.
- **Domain Level Only** - Same as Manager, but with no Multi-Domain permissions..

The selected role affects the permissions that you can configure in the next parts: **Multi Domain Management**, **Global Management**, and **Domain Management**. For example, Superusers always have Domain Management permissions.

Multi-Domain Security Management Activities

Enable or disable permissions for these activities:

- **MDS Provisioning** - Create and manage Multi-Domain Servers and Multi-Domain Log Servers. Only Superusers can select this option.
- **Manage All Domains** - Create and manage all Domains and Global Domains. This option is enabled by default for Superusers. Managers can select it.
- **Manage Administrators** - Create and manage Multi-Domain Security Management administrators with the same or lower permission level. For example, a Domain manager cannot create Superusers or global managers. This option is enabled automatically for Superusers. Managers can select it.

- **Manage Sessions** - Connect/disconnect Domain sessions, publish changes, and delete other administrator sessions.
- **Management API login** - Lets an administrator log in to the Security Management Server and run API commands using these tools
  - *mgmt_cli* (Linux and Windows binaries)
  - *Gaia CLI* (Gaia Clish)
  - *Web Services* (REST)
- **Global VPN Management** - Lets the administrator select **Enable global use** for a Security Gateway shown in the MDS **Gateways & Servers** view. (To see the option, right-click on the Security Gateway object).

Global Management Activities

All options are enabled automatically for Superusers. Managers can select them.

- **Manage Global Assignments** - Create, update and delete global assignments.
- **Default profile for all Global Domains** - Change the default permission profile for all global Domains.
- **View global objects in Domains** - Lets an administrator with no global objects permissions view the global objects in the domain. This option is required for valid domain management.

Domain Management

This profile defines the default Domain permissions that automatically apply when you create a new administrator account. After you create the administrator account, you can change its Domain profile as necessary.

Select a default profile from the list. This option is enabled automatically for Superusers, and Managers can optionally select it.

Creating Custom Domain Permissions

Customized Domain permission profiles are a set of granular permissions for Domain level activities in SmartConsole.

To configure custom permission profiles:

1. In the **Permission Profiles** window, click **New Domain Permission Profile**.

   The **New Domain Permission Profile** window opens.

2. Configure read/write permissions for each Software Blade, feature, resource, and the API in these categories as necessary:

- **Overview** -Select default or custom permission options
- **Gateways** -Work with Security Gateway management tasks and VSX provisioning
- **Access Control** - Work with Access Control rules and install Access Control Policies
- **Threat Prevention** - Work with Threat Prevention rules, profiles, and protections. Install Threat Prevention Policies
- **Others** -Work with different features not in other categories
- **Monitoring and Logging** -See and manage logs, monitoring features and related reports
- **Events and Reports** -Work with SmartEvent events, policy and reports
- **Management** -Manage sessions and High Availability options

To prevent administrators from working with an item, clear its option.

Notes:

- You cannot prevent administrators from seeing some resources. You cannot change their options.
- Some resources do not have **Read** or **Write** options. You can only select or clear them.

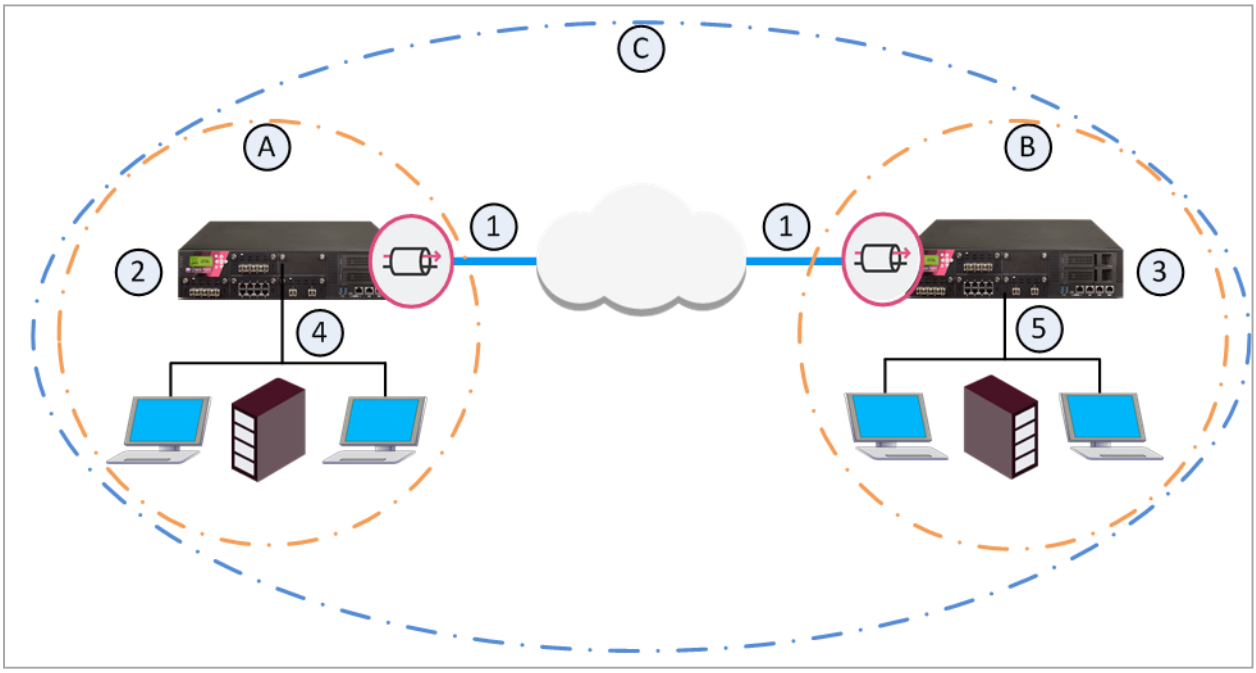
VPN and Multi-Domain Security Management

This chapter describes how to configure and work with the Global VPN communities,

Global VPN Communities

Large enterprises often have branches in different cities or countries. With each branch managed by a different Domain, the enterprise can use a central management system to centrally manage all the various Domains. When connectivity is established, the connections must be secure and have high levels of privacy, authentication, and integrity.

A Global VPN Community connects the enterprise's Security Gateways through VPN and lets the enterprise manage them under one network. You define the Global VPN Community in the Global Domain. The Multi-Domain Server utilizes its knowledge about the different Domain Management Server environments to create a VPN community which can manage them.



Item	Description
A	Domain A on Multi-Domain Server
B	Domain B on Multi-Domain Server
C	Global VPN Community
1	VPN tunnel

Item	Description
2	Security Gateway configured in Domain A
3	Security Gateway configured in Domain B
4	VPN Domain of Security Gateway 2
5	VPN Domain of Security Gateway 3

To learn more about VPN communities, see the *R82 Site to Site VPN Administration Guide*.

VPN Connectivity

When you establish a Global VPN Community, it replaces part of the configuration of Externally Managed Security Gateways and automates the exchange of certificates for each Domain Management Server.

These trusted entities create VPN trust in a Multi-Domain Security Management deployment:

- Certificates issued by a Domain Management Server Internal Certificate Authority (ICA).
- External third party Certificate Authority servers (using OPSEC connectivity).
- Pre-shared secrets.

The ICA of the Domain Management Server issues certificates used by Domain Security Gateways to create SIC trust. Each Security Gateway supports certificates issued by the CAs of the other Domains.

For more information on VPN with Externally Managed Gateways, see the *R82 Site to Site VPN Administration Guide*.

Configuring Global VPN Communities

This is the workflow for Creating a Global VPN Community.

To create a Global VPN Community:

1. Configure a VPN Domain on each participating Security Gateway.
2. Enable each participating Security Gateway for global use.
3. In the Global Domain, define a VPN Community, and add the Global Security Gateway objects to the Global VPN Community. The Global Security Gateway objects represent the participating Domain Security Gateways.
4. Define a Security Policy - You can create a Global policy and assign it to the Local Domains, or you can create the Security Policy rules only in the Local Domains.
5. Assign the Global configuration to the applicable Domains. After assignment, you must also install the policy on the participating Security Gateways.

Step 1 - Configuring a VPN Domain on each Security Gateway

You define the Domain Security Gateways in the Domain SmartConsole.

To define a VPN Domain on a Security Gateway:

In the Security Gateway editor:

1. In **General Properties**, enable **IPSec VPN**.
2. In **Network Management** > **VPN Domain**, configure the settings for the VPN Domain. You must define a VPN Domain and specify if the VPN Domain is based on the network topology or a specific IP address range.

For information on configuration of a VPN Domain, see the *R82 Site to Site VPN Administration Guide*

Multi-Domain Server holds these IP address ranges used by the Security Gateways. During the assignment of the Global configuration, the Multi-Domain Server transfers this information to all the Domains with participating Security Gateways in the Global VPN Community.

Step 2 - Enabling Gateways for Global Use

Repeat this step for all Security Gateways that are to participate in the Global VPN Community:

In the Multi-Domain Server SmartConsole > **Gateways & Servers** view, right-click a Security Gateway and select **Enable Global Use**.

A global Security Gateway object and a VPN Domain object are created for the Security Gateway in the Global Domain. Different Domains can coincidentally contain Security Gateways with the same name. Because each global Security Gateway object must have its own unique **Global Name**, the **Global Names Template** automatically assigns a unique name for each global Security Gateway.

The default global name format is:

<Name of Security Gateway>_of_<Name of Domain>.

For example:

- Security Gateway name = **MyGateway**
- Domain name = **MyDomain**
- Global name = **MyGateway_of_MyDomain**

Notes:

- When the local Domain that manages the gateway to be used globally has the active server on a standby Multi-Domain Server you cannot use the gateway globally.
- When a Security Gateway is enabled for global use, you cannot disable IPsec VPN.To disable IPsec VPN: in the Multi-Domain view, go to Gateways & Servers, right-click the applicable Security Gateway, and clear "**Enable for global use**" checkbox. Publish your changes and reassign them to the applicable Domain using a global assignment.

Enabling clusters for global use

You can enable a cluster for global use in the same way that you enable a Security Gateway. A global cluster object and a VPN Domain object will be created for the cluster in the Global Domain.

Step 3 - Creating the VPN Global Community

After you enabled VPN on the Security Gateways, and enabled the Security Gateways for global use, you can create the Global VPN Community.

To create a Global VPN Community:

1. In the Global Domain, go to **Security Policies** > **Access Control** > **Access Tools** > **VPN Communities** > **New**.
2. Add the global Security Gateway objects, defined in step 1, as participating Security Gateways in the community.

To learn more about VPN communities, see the *R82 Site to Site VPN Administration Guide*.

Step 4 - Defining a Security Policy

The configuration of Security Gateways into a Global VPN Community does not automatically let the Security Gateways access each other. For the Security Gateways to communicate with each other you must define an Access Control Security Policy.

You can define the Access Control Security Policy in the Global Domain or in the Local Domains or both.

To define a Global Security Policy, see *"Global Management" on page 63*. To learn more about the Access Control Security Policy Rule Base, see the *R82 Security Management Administration Guide*.

Step 5 - Assigning the Global Configuration to the Local Domains

After you create the Global VPN Community, and in some case, also the Global Policy, you must assign the Global configuration to the Local Domains. After assignment, install policy on the Local Domains.

To assign the global configuration to the Local Domains:

1. Make sure you published all the changes made in the Global Domain.
2. In the Multi-Domain Server SmartConsole > **Multi-Domain** view > **Global Assignments**, assign the Global objects to the Local Domains (see *"Global Assignments" on page 80*)
3. Install policy on the Security Gateways.

Note - All Security Gateways which participate in the Global VPN Community must use a Simplified VPN Policy.

For each Domain with Security Gateways in the Global VPN Community, a global **CA Server** object is created in the Global Domain. During the assignment process, the Multi-Domain Server automatically exports relevant Domain ICA information (such as the CA certificate) to all the Domain Management Servers with Security Gateways that participate in the community. This way, all the Security Gateways in the community can trust the others' ICAs.

After the assignment, the Global VPN Community object shows in each Domain with Security Gateways in the community. If you assign a Global Policy to a Domain that has no Security Gateways in the community, this Domain does not show the community object and the community Security Gateway objects.

Reassigning the Global Configuration to One or More Local Domains

If you make changes to the global configuration, reassign the configuration to the Domains.

To reassign the Global configuration to the Local Domains:

1. In the Multi-Domain Server SmartConsole > **Multi-Domain** view > **Global Assignments**, select the Domains that have Security Gateways which participate in the Global VPN Community and click **reassign**.
2. In the **Reassign** window, select **Install policy on successful assignment**. This installs the Global Policy on the Security Gateways which participate in the Global VPN Community.

   Note - This operation assigns the Policy to all selected Domains, and then installs the Policy on all Domain Security Gateways, in one step. It does not let you select specific Security Gateways on which to install the Policy. The selected Policy is installed on all Security Gateways in the selected Domains. Assigning the Policy to many Domains and all their Security Gateways can take some time. Use this option with caution.

Working with High Availability

High Availability is redundancy and database backup for management servers. Synchronized servers have the same policies, rules, user definitions, network objects, and system configuration settings.

Overview of High Availability

Multi-Domain Security Management implements High Availability at these levels:

- **Multi-Domain Server High Availability** is an Active/Active redundancy solution that uses two or more fully synchronized Multi-Domain Servers for continuous redundancy. All Multi-Domain Servers are Active. You can log into and work with the primary or secondary Multi-Domain Servers.
- **Domain Management Server High Availability** is both a redundancy and a Load Sharing solution for Domains. You create a Domain Management Server on two or more Multi-Domain Servers. These Domain Management Servers synchronize fully for continuous redundancy.

  One Domain Management Server is Active and the others are Standby. Each Multi-Domain Server can have both Active and Standby Domain Servers. You can configure the Active Domain Management Server on different Multi-Domain Servers for effective load sharing.

All High Availability deployments include one Primary Multi-Domain Server and one or more Secondary servers. Synchronization occurs automatically when administrators publish sessions with changes to Policies, objects or configuration settings.

Primary and Secondary Multi-Domain Servers

The order in which you install Multi-Domain Servers is significant. You must define the first physical server as a Primary Multi-Domain Server in the First Time Wizard. You must define all other Multi-Domain Servers as Secondary in the First Time Wizard.

Active and Standby Domain Management Servers

You can only use the Active Domain Management Server to manage Domain Security Gateways, networks, Security Policies objects and system configuration. Standby Domain Management Servers synchronize fully for redundancy. You can connect to a Standby Domain Management Server in the Read Only mode to look at current object configurations and Rule Base.

In the standard configuration, there is only one Active Domain Management Server for each Domain. All others are Standby Domain Management Servers. If the Active Domain Management Server fails, you must manually change a Standby Domain Management Server to Active.

Important notes about 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.

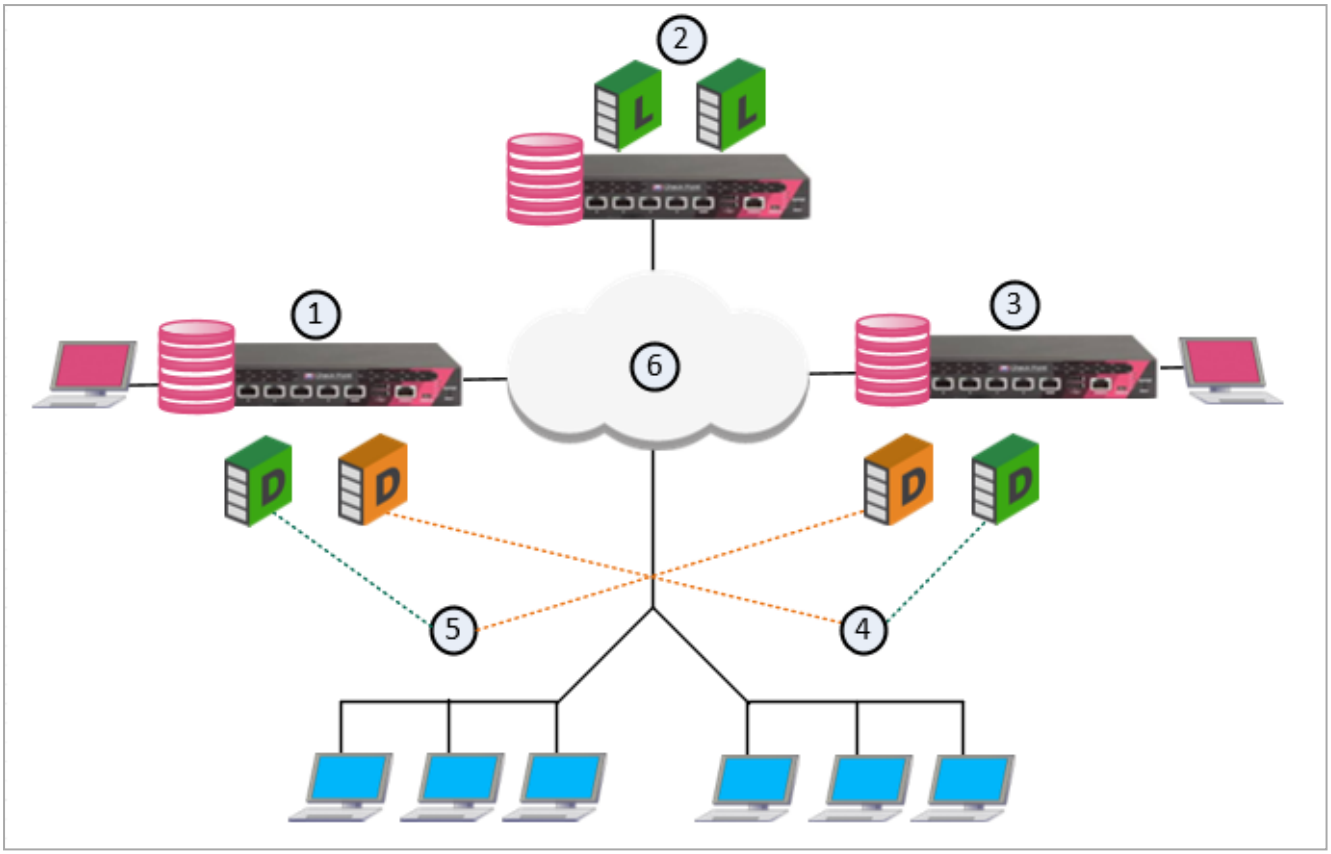
For more information:

- About Gaia Backup and Gaia Snapshot, see the *R82 Gaia Administration Guide*.
- About the "`migrate export`" and "`migrate import`" commands, see the *R82 CLI Reference Guide*.
- About the "`mds_backup`" and "`mds_restore`" commands, see the *R82 CLI Reference Guide*.
- About Virtual Machine Snapshots, see the vendor documentation.

Multi-Site High Availability Deployment Example

This example shows a Multi-Site, High Availability deployment with two Multi-Domain Servers and one Multi-Domain Log Server. A real-life deployment will have many more assets.

Each Multi-Domain Server has two Domains configured for Load Sharing, where a different Domain Management Server is Active at each location. Administrators can connect to all Multi-Domain Servers. For best performance, connect to the Multi-Domain Server nearest to your geographical location.



Item	Description
1	London Multi-Domain Server with an Active Domain Management Server for London and a Standby Domain Management Server for Tokyo
2	Multi-Domain Log Server with Domain Log Servers for London and Tokyo
3	Tokyo Multi-Domain Server with an Active Domain Management Server for Tokyo and a Standby Domain Management Server for London
4	Tokyo network
5	London network
6	Internet
	Active Domain Management Server
	Standby Domain Management Server
	Domain Log Server

This illustration shows the configuration grid in the SmartConsole **Multi Domain** view for the example deployment:

The system automatically creates the Global Domain when you install Multi-Domain Security Management.

Creating a Secondary Multi-Domain Server

This section shows you how to create a new secondary Multi-Domain Server.

Important - Before you start this procedure, make sure to define the physical server as the correct server type (Secondary Multi-Domain Server, or Multi-Domain Log Server) during installation. An incorrect definition can cause deployment failure.

To create a new, Secondary Multi-Domain Server:

1. If you did not do so, install a new Secondary Multi-Domain Server.

   Follow the procedures in the *R82 Installation and Upgrade Guide*. Make sure to define this server as a secondary Multi-Domain Server in the First Time Wizard. Connect to the Primary Multi-Domain Server with SmartConsole and go the **Multi-Domain** > **Domains** view.

2. In the Multi-Domain navigation toolbar, click **New** > **Multi-Domain Server**.
3. Enter a unique name for this Multi-Domain Server.

   To get the IP address automatically, the name must be in the DNS.

4. Enter the IPv4 address or click **Resolve IP** to get the IP address from the DNS.
5. Select the platform operating system, software version, and hardware type.
6. Click **Connect** to establish SIC trust.

The new Multi-Domain Server automatically synchronizes with all existing Multi-Domain Servers and Multi-Domain Log Servers. The synchronization operation can take some time to complete, during which a notification indicator shows in the task information area.

Note - To add a license for a Multi-Domain Server, go to the main Menu > **Manage licenses and packages**.

Limitations

- Private sessions are not synchronized between Multi-Domain Servers.You cannot see a session that is open on one Multi-Domain Server on another Multi-Domain Server or moved it to another Multi-Domain Server.
- You cannot manage the same object (an object that is editable in the Multi-Domain view, for example: an administrator, a domain, a permission profile, a trusted client or a Multi-Domain Server) from multiple Multi-Domain SmartConsoles. It can create synchronization failures between the Multi-Domain Servers. If there is a synchronization failure, make sure that sessions on a different Multi-Domain SmartConsole do not lock the same object.

- Policy installation from the Primary Multi-Domain Server to a Domain fails with an error, if that Domain exists only on the Secondary Multi-Domain Server:
  ```
  Install policy cannot be executed

  Multi-Domain '<Name of Multi-Domain Server Object>' does not
  have domain server for: 'Name of Domain Object'.
  ```
- In a High Availability environment that includes more than two Multi-Domain Security Management Servers, a synchronization problem between 2 specific Multi-Domain Security Management Servers only shows when connected to one of those servers. The problem does not show when connected to a different Multi-Domain Security Management Server in the environment.
- Synchronization on the Multi-Domain Server level fails after creating a new Domain on the secondary Multi-Domain Server, while an initial full synchronization from the new secondary device is performed.
- To move a secondary Multi-Domain Security Management Server from one Multi-Domain Management High Availability environment to another, install the secondary Multi-Domain Security Management Server from scratch in the new environment as a secondary Multi-Domain Security Management Server and synchronize it with the primary Multi-Domain Security Management Server.

Domain Management Server High Availability and Load Sharing

This section includes procedures for configuring the Multi-Domain Security Management environment for secondary Multi-Domain Servers and a Multi-Domain Log Server.

When you install Multi-Domain Security Management for the first time, select **Primary Multi-Domain Server** in the First Time Wizard

For High Availability and Load Sharing, select **Secondary Multi-Domain Server** in the First Time Wizard.

Each Domain has one Active and one or more Standby Domain Management Servers. For example, if a deployment has three Multi-Domain Servers, each Domain can have one Active and two Standby Domain Management Servers. This lets the Domains load be shared between several physical Multi-Domain Servers.

Example of Domain Management Server High Availability with Load Sharing:

Servers (3) / Domains (4)	MDS110 192.168.3.110	MDS104 192.168.3.104	MDS111 192.168.3.111
DOM155	192.168.3.155	192.168.3.176	192.168.3.166
DOM165	192.168.3.156	192.168.3.178	192.168.3.165
DOM175	192.168.3.158	192.168.3.175	192.168.3.167
Global			

By default, the Primary Domain Management Server is Active. All other Domain Management Servers for that Domain are Standbys. You can change a Standby Domain Management Server to Active as necessary.

All Domain management operations, such as working with Security Policies, users, networks and other objects, occur on the Active Domain Management Server. Standby Domain Management Servers automatically synchronize with the Active Domain Management Server. Security Gateways can get a Security Policy and a Certificate Revocation List (CRL) from either the Active or Standby Domain Management Servers.

Creating a Secondary Domain Management Server

When you first create a Domain, you also define the Primary Domain Management Server. Use this procedure to create Secondary Domain Management Servers for existing Domains.

To create a secondary Domain Management Server:

1. Connect to the Multi-Domain Server with SmartConsole.
2. In the Domains view, right-click the empty cell at the intersection of the applicable Multi-Domain Server and Domain in the grid.
3. Select **New Domain Server**.
4. In the **Domain Server** window, configure the Domain Management Server name and IP address.

Domain Management Server synchronization starts automatically and can take some time to complete.

To delete a secondary Domain Management Server configuration, right-click the applicable cell and select **Delete**.

Notes:

- You cannot change settings for an existing Domain Management Server. You must first delete the Domain Management Server and then create a new one.
- In a Multi-Domain Server Management High Availability environment, if the Administrator installs a policy from the Active Domain on the Security Gateway / Cluster object and performs Management High Availability from the Active Domain to the Standby Domain, the Administrator must install a policy from the new Active Domain on the Security Gateway or Cluster object. Otherwise, when upgrading the Multi-Domain Server, SIC communication can be lost with the Security Gateway or Cluster Members.
- Creation of a Security Gateway object on the Domain Management Server that is active on the Secondary Management Server fails. To resolve this issue, run the "`mdsstop; mdsstart`" commands on the Secondary Multi-Domain Server.

Creating a High Availability Environment with a Security Management Server

You can use a Security Management Server to create a High Availability environment with a Domain Management Server. The Security Management Server can operate as an Active or Standby management.

For example:

- The Security Management Server is the Standby Management Server and the Domain Management Server is the Active Management Server.

  If the Domain Management Server is unavailable, the user must activate the Security Management Server so it becomes the Active Management Server.

- The Domain Management Server is the Standby Management Server and the Security Management Server is the Active Management Server.

  If the Security Management Server is unavailable, the Domain Management Server becomes the Active Management Server.

In both cases, the Domain Management Server must be Active to assign a Global Policy.

To create a High Availability environment with multiple Domain Management Servers, you must use a different Security Management Server per each Domain Management Server.

You must define GUI clients and administrators locally on the Security Management Server. The synchronization process cannot export this data from a Domain Management Server to a Security Management Server.

To create a High Availability environment using a Security Management Server

1. Do a Clean Install of a Security Management Server, and define the Security Management Server as a Secondary Security Management Server.
2. Connect to the command line on the Security Management Server.
3. Run: `cpconfig`
4. Configure these items:
   a. Secure Internal Communication - Define an Activation Key to establish SIC trust between the Security Management Server and the Domain Management Server.
   b. Define administrators.
   c. Define GUI clients.

5. In SmartConsole of the Domain Management Server, create a network object of the type **Check Point Host**, which represents the Secondary Security Management Server. Go to the Object Explorer, and click **New** > **More** > **Network Object** > **Gateways & Servers** > **Check Point Host**. The **Check Point Host** window opens.

   In the **General Properties** page:

   a. Enter the object name and IPv4 address.

   b. In the **Management** tab at the bottom of the page, select **Network Policy Management**. The **Secondary Server** is then automatically selected.

      In the **Secure Internal Communication** field, click **Communication** to establish SIC trust between the Security Management Server.

   c. In the **Management** tab at the bottom of the page, select **Network Policy Management**. The **Secondary Server** is then automatically selected.

   d. Click **OK**.

6. Publish the session. Initialization and synchronization between the Domain Management Server and the Security Management Server starts. Wait for the task list to show that a full synchronization completed.

To see the High Availability status of both servers, go to the main Menu and click **High Availability Status**. In this window you can see which server is active and which is standby and the synchronization status.

Notes:

- After you configure a Security Management Server for Management High Availability with a Domain:
  - If you connect with SmartConsole to the Primary Domain server and open the Management High Availability dialog box, it shows the connected peers including the Security Management Server.
  - If you connect with SmartConsole to the Secondary Domain server and open the Management High Availability dialog box, it does not show the Security Management Server.
- If it is necessary to delete a Security Management Server object that was configured for Management High Availability with a Domain and create that object again, you must follow these steps:
  - Delete the Security Management Server object
  - Publish the session
  - Restart the Multi-Domain Server with: `mdsstop ; mdsstart`

Synchronization

In a multi-domain environment, the Multi-Domain Servers work in active-active mode. All Multi-Domain Servers are active and synchronize each other.

The Domains managed by the Multi-Domain Server work in active-standby mode, where the Active Domain Server synchronizes all the standby Domain Servers.

The system automatically synchronizes periodically and when an administrator publishes changes to the configuration.

How Synchronization Works

During synchronization, the system performs these steps without user intervention:

On periodic synchronization:

1. The Active exports the delta data between the Active server and the Standby server to compressed files.
2. The compressed files are transferred to the Standby server.
3. The Standby Server replays the delta data from the uncompressed files.

On manual synchronization:

1. The Active Server exports the public data to compressed files.
2. The compressed files are transferred to the Standby Server.
3. The Standby server overrides the existing data with the uncompressed files.

The data that is transferred during synchronization includes:

- Postgres database
- Solr
- ICA database
- Configuration files
- Domain licenses and contracts. Multi-Domain server licenses and contracts are not transferred.

Initial Synchronization

Initial synchronization occurs automatically when you create a secondary Multi-Domain Server, Multi-Domain Log Server, or Domain Management Server. The system generates a task to copy all databases and system information from the connected server to the new server.

Multi-Domain Server and Multi-Domain Log Server synchronization tasks show in the **Task Information** area, in the Multi-Domain Server SmartConsole. Domain synchronization tasks show in the Domain SmartConsole.

Periodic Synchronization

Multi-Domain Servers synchronize with all other peers and Multi-Domain Log Servers. Periodic synchronization occurs automatically, and when an administrator publishes a session. Private (non-published) sessions do not synchronize.

Periodic synchronizations are incremental. Only database changes synchronize with peers. Active Domain Management Servers synchronize to the standby Domain Management Servers.

Manual Synchronization

Manual synchronization is a full synchronization that overwrites all data on the peers. It disconnects all connected clients and overrides active sessions and running tasks.

When changes made in a session are published on the Active server (made public), the changes are synchronized to the Standby server. Unpublished, private sessions are not synchronized.

Best Practice - Use this option with caution, and only in cases of synchronization error. We recommend that you publish changes before initiating full sync.

For Domain Management Servers, you can only run a manual synchronization from the active Domain Management Server to the standby peers.

Manually Synchronizing a Multi-Domain Server

You can manually synchronize the connected Multi-Domain Server with a peer Multi-Domain Server.

To manually synchronize Multi-Domain Servers:

1. Click the **Synchronization Status** area at the bottom of the SmartConsole window.
2. In the **High Availability Status** window, select a peer Multi-Domain Server to synchronize.
3. Click **Sync Peer**.

Synchronization starts immediately and the status shows in the window. The synchronization operation can take many minutes to complete.

Warning - Use manual synchronization with caution. This can overwrite all data on the peer Multi-Domain Server if they do not synchronize correctly.

Manually Synchronizing Domain Management Servers

You can manually synchronization a Standby Domain Management Server with the Active Domain Management Server on a different Multi-Domain Server.

To manually synchronize Domain Management Servers for a Domain:

1. Open SmartConsole for the active Domain Management Server.
2. Click **Menu** > **High Availability**.
3. In the **High Availability Status** window, click **Actions** > **Sync Peer**..

Synchronization starts immediately and the status shows in the window. The synchronization operation can take many minutes to complete.

Multi-Domain Server ICA Database Synchronization

When you create a new secondary Multi-Domain Server, the Internal Certificate Authority (ICA) on the Primary Multi-Domain Server generates a certificate when you establish SIC trust. The ICA can generate a certificate for a new administrator, if required by the authentication method. In a High Availability deployment with more than one Multi-Domain Server, the system synchronizes the ICA databases as necessary.

Failure Recovery

You can recover a failed **Primary** Multi-Domain Server in a Management High Availability deployment by following the steps provided in this section.

Action Plan:

1. Promote an existing Secondary Multi-Domain Server to become the Multi-Domain Server Primary.
2. Promote each Secondary Domain Management Server to become the Primary Domain Management Server.
3. Install and configure a new Secondary Multi-Domain Server.

Important - Use Domain Management Server promotion only to recover a failed Multi-Domain Server. Do **not** use this procedure to change the Primary and Secondary roles on working servers.

Procedure:

Notes:

- The procedure below assumes that the Primary Multi-Domain Server failed, and the Secondary Multi-Domain Server keeps working.
- There are environments, where a Domain Management Server is primary on a Secondary Multi-Domain Server.
  If the primary Domain Management Server was on the failed Multi-Domain Server, then promote the secondary Domain Management Server.
- This procedure cannot be used to split machines from a single multi-domain environment into multiple separate systems.

1. **Promote the Global Domain Management Server on the Secondary Multi-Domain Server**

Step	Instruction
1	Make sure that all functional, Secondary Multi-Domain Servers and Multi-Domain Log Servers are up and running.
2	Connect with SmartConsole one of the Secondary Multi-Domain Servers you need to promote.
3	If the Global Domain Management Server is not Active, change it to Active: a. In the **Domains** view, right-click the **Global Domain**, and then click **Connect to Domain**. A SmartConsole instance opens for the Global Domain. b. Go to **Menu** > **Management High Availability**. c. In the **High Availability Status** window, click **Actions** > **Set Active** for this Global Domain.
4	Close all SmartConsole windows.

2. **Promote the Secondary Multi-Domain Server to Primary**

This procedure is necessary because there are no automatic steps to promote a Secondary Multi-Domain Server when the Primary Multi-Domain Server fails.

Step	Instruction
1	Connect to the command line on the Secondary Multi-Domain Server you need to promote.
2	Log in to the Expert mode.

3	Run these commands in the order they appear below:
	`cpprod_util FwSetPrimary 1`
	`cpprod_util CPPROD_SetValue PROVIDER-1 Primary 4 1 1`
	`cpprod_util CPPROD_SetValue SIC ICAState 4 3 1`
	`ckp_regedit -d //SOFTWARE//CheckPoint//SIC OTP`
	`ckp_regedit -d //SOFTWARE//CheckPoint//SIC ICAip`
	These commands update the required parameters in the Check Point Registry on the Secondary Multi-Domain Server.

3. **Delete the object of the failed Primary Multi-Domain Server**

   Note - Before deleting the failed Multi-Domain Server, remove all references to all Domain Management Servers running on it. In the SmartConsole **Object Explorer**, go to each Domain Management Server, right-click it and select **Where Used**. Remove all references to the Domain Management Servers from all the objects and rules in which they appear. If needed, adjust the rules accordingly.

Step	Instruction
1	Connect with the *Database Tool (GuiDBEdit Tool)* to the Secondary Multi-Domain Server you need to promote. **Important** - You must start this tool with the "**/mds**" flag.
2	In the top left panel, click **Tables** > **Other** > **mdss**.
3	In the top right panel, locate the object of the **failed Primary** Multi-Domain Server > right-click this object > click **Delete**. **Important** - The Database Tool (GuiDBEdit Tool) deletes this object without asking to confirm.
4	In the top right panel, select the object of the **Secondary** Multi-Domain Server you promoted.
5	In the bottom panel, double-click the **primary** attribute.
6	Select the value **true** > click **OK**.
7	Save the changes: Click the **File** menu > click **Save All**.
8	Close the Database Tool (GuiDBEdit Tool).
9	Connect with SmartConsole one of the Secondary Multi-Domain Servers you promoted.
10	From the left navigation panel, click **Multi Domain**.
11	In the middle panel, click **Domains**.
12	In the right panel, from the top toolbar, right-click the object of the **failed Primary** Multi-Domain Server > click **Delete**.

4. **Promote all the Secondary Domains to Primary**

   Follow these instructions for each Domain on the Secondary Multi-Domain Server.

Important:

- To use this procedure, there must be at least one Active Domain Management Server on a different Multi-Domain Server.
- To make Domain Management Server Active when there is no corresponding peer and the **High Availability Status** window is not available, run these commands:

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

```
mgmt_cli make-server-active force true --domain <Name of Domain Management Server> --user <User Name> --password <Password>
```

These commands set the Domain Management Server to the Active state. Do this for all Domain Management Servers that do not have a High Availability peer.

Step	Instruction
1	In SmartConsole **Domains** view, in the left column, select a Secondary Domain to promote to Primary.
2	If the selected Domain Management Server is Standby, change it to Active: a. Right-click the selected Domain Management Server, and then click **Connect to Domain**. A SmartConsole instance opens for the Domain. b. Go to **Menu** > **Management High Availability**. c. In the **High Availability Status** window, click **Actions** > **Set Active**. d. Close SmartConsole

3	Run these commands on the Multi-Domain Server you promoted to Primary:
	`mdsenv <IP Address or Name of Domain Management Server>`
	`promote_util`

4	Connect with SmartConsole to the Domain Management Server you promoted: Right-click the selected Domain Management Server, and then click **Connect to Domain Server**.
5	From the left navigation panel, click **Gateways & Servers**.

Step	Instruction
6	Right-click the object of the Domain Management Server that failed > click **Where Used**.
7	Delete all instances of the failed Domain Management Server, including the failed Domain Management Server itself.
8	Delete the object of the failed Domain Management Server.
9	Publish the SmartConsole session.
10	Manually synchronize the Domain Management Servers.
11	Close the SmartConsole connected to this Domain Management Server.
12	Assign Global Policies and install Policies on all managed Security Gateways.
13	If the promoted Domain Management Server is using a High Availability Domain Management Server license, replace it with a standard Domain Management Server license.

5. **Restart Check Point Services on the Multi-Domain Server you promoted**

   Run these commands:

   ```
   mdsstop
   mdsstart
   ```

6. **Install and configure a new Secondary Multi-Domain Server**

   See the *R82 Installation and Upgrade Guide*.

Deleting a Secondary Multi-Domain Server or Multi-Domain Log Server

To delete a secondary Multi-Domain Server:

1. Move each Active Domain Management Server on the secondary Multi-Domain Server to another Domain Management Server.
2. Connect to the command line on the Multi-Domain Server to be deleted and run:
   `mdsstop`
3. In SmartConsole, right-click the secondary Multi-Domain Server, and then select **Delete Multi-Domain Server**.
4. Confirm the action and click **OK**.
5. Publish the SmartConsole session.

Note - This procedure deletes all standby and non-primary Domain Management Servers on the Secondary Multi-Domain Server. You cannot delete the Primary or Active Domain Management Server.

Re-Establishing SIC Trust for a Secondary Multi-Domain Server

Important - You can only re-establish the SIC trust on a Secondary Multi-Domain Server or Multi-Domain Log Servers. There is no option to establish SIC trust on the Primary Multi-Domain Server.

It is occasionally necessary to re-establish trust between a Primary and secondary Multi-Domain Server or Multi-Domain Log Server. This can occur for many reasons, including:

- Changes to the IP address of the Primary Multi-Domain Server, Secondary Multi-Domain Server or Multi-Domain Log Server
- Failure and recovery of the Primary Multi-Domain Server
- Promotion of a Secondary Multi-Domain Server to Primary Multi-Domain Server
- Internal Certificate Authority (ICA) failure on the Primary Multi-Domain Server

To re-establish the SIC trust:

1. Open a command line interface to the Secondary Multi-Domain Server or Multi-Domain Log Server.
2. Log in and run: `mdsconfig`
3. Enter the number for **Secure Internal Communication**, and then press **Enter**.
4. Enter `y` to confirm.
5. Enter and confirm the activation key.
6. Enter the number for **Exit**.
7. Wait for Check Point processes to stop and automatically restart.
8. In the SmartConsole **Multi-Domain** view, double-click a Secondary Multi-Domain Server or Multi-Domain Log Server object.
9. In the **Multi-Domain Server** window, click **Connect**.
10. In the **Initialize SIC** window, enter activation key that you entered in step 5 above.

    If successful, the **Certificate State** field shows **Trust established**.

Logging and Monitoring

This chapter includes information that is directly related to Multi-Domain Security Management, with some general background information and basic procedures. See the *R82 Logging and Monitoring Administration Guide* for the full set of conceptual information and procedures.

With R80, logging, event management, reporting, and monitoring, are more tightly integrated than ever before. Security data and trends are easy to understand at a glance, with Widgets and chart templates that optimize visual display. Logs are now tightly integrated with the Policy rules so that you can access all logs associated with a specific rule by simply clicking on that rule. Free-text search also lets you enter specific search terms to retrieve results from millions of logs in seconds.

One-click exploration makes it easy to move from high-level overview to specific event details such as type of attack, timeline, application type and source. After you investigate an event, it is easy to act on it. Depending on the severity of the event, you can choose to ignore it, act on it later, or block it immediately. You can also easily toggle over to the rules associated with the event to refine your Policy. Send reports to your manager or auditors that show only the content that is relevant to each stakeholder.

In R80.x, SmartReporter and SmartEvent functionality is integrated into SmartConsole.

Using rich and customizable views and reports, R80 introduces a new experience for log and event monitoring.

The new views are available from two locations:

- **SmartConsole > Logs & Events**
- **SmartView Web Application**. Browse to: *https://<Server IP Address>/smartview/*

  Where *Server IP Address* is IP address of the Multi-Domain Server or Multi-Domain Log Server.

  Note - Include the final backward slash: **/**

Note - When opening a Global SmartEvent object from a Domain in SmartConsole or SmartView Monitor, this error message appears: "`State: Secure Internal Communication is not operation with <Name of Global SmartEvent Server object>. Verify that SIC is initialized or was not reset.`"
This is only a cosmetic issue that does not have an effect on the functionality.
Domains do not have SIC connectivity with the Global SmartEvent Server. Therefore, Domains cannot report the real SIC status of the Global SmartEvent Server. To see the real SIC status, open the Global SmartEvent Server object in SmartConsole connected to the Multi-Domain Server context.

Working with Log Servers

A Domain Log Server is a dedicated host for Domain log files. A Multi-Domain Log Server is a dedicated container for Domain Log Servers. Domain Log Servers also handle these log management activities:

- Automatically start a new log file when an existing log file is larger than the specified maximum size
- Log file backup and restoration
- Export and import log files
- Index logs for faster log queries.

It is a best practice to use Multi-Domain Log Servers and Domain Log Servers to handle logs for a Multi-Domain Security Management environment because of the large volume of logs.

To see the logs for a Domain and its Security Gateways, click **Logs & Events** in SmartConsole for that Domain. To see logs for all Domains in one view, click **Logs & Events** in the Multi-Domain Server SmartConsole. You can filter the logs for specified Security Gateways, Domain Management Servers, or Domain Log Servers.

Configuring Logging

Creating a Multi-Domain Log Server with Domain Log Servers

This section shows you how to create a new Multi-Domain Log Server and its related Domain Log Servers.

Important - Before you start this procedure, make sure that you define the physical servers as the correct server type (Secondary Multi-Domain Server or Multi-Domain Log Server) during installation. An incorrect definition can cause deployment failure.

To create a new Multi-Domain Log Server:

1. If you did not do so, install a new Multi-Domain Log Server.

   Follow the procedures in the *R82 Installation and Upgrade Guide*.

   Make sure to define this server as a Multi-Domain Log Server in the First Time Configuration Wizard.
2. Connect with SmartConsole to the primary Multi-Domain Server - the **MDS** context.
3. From the left navigation panel, click **Multi-Domain > Domains**.
4. From the top toolbar, click **New** > **Multi-Domain Log Server**.
5. Enter a unique name for this Multi-Domain Log Server.
6. Enter the IPv4 address or click **Resolve IP** to get the IP address from the DHCP Server.
7. Click **Connect** to establish SIC trust.

   Enter the same Activation Key you entered during the First Time Configuration Wizard of the Multi-Domain Log Server.
8. In the **Platform** section:
   - In the **OS** field, select **Gaia**
   - In the **Version** field, select the correct version
   - In the **Hardware** field, select the applicable option
9. Click **OK**.

Note - To add a license for a Multi-Domain Log Server, go to the main Menu > **Manage licenses and packages**.

To create Domain Log Servers:

1. Connect with SmartConsole to the primary Multi-Domain Server - the **MDS** context.
2. From the left navigation panel, click **Multi-Domain > Domains**.
3. In the **Multi-Domain Log Server** column, right-click the **Domain Log Server** cell for each Domain and click **New Domain Server**.
4. Accept the default name or enter a different, unique name.
5. Enter the IPv4 address or click **Resolve IP** to automatically assign the IPv4 address.
6. Click **OK**.

   Wait for the cell to show the new Domain Log Server.
7. Configure the Security Gateway in each Domain to the send its logs to the new Domain Log Server on the Multi-Domain Log Server (see *"Configuring Security Gateways to Send Logs to a Log Servers" below*).

   The Domain Log Servers synchronize automatically.

The new Multi-Domain Log Server automatically synchronizes with all existing Multi-Domain Servers. The synchronization operation can take many minutes to complete, during which a notification indicator shows in the task information area.

Note - To add a license for a Domain Log Server, go to the main Menu > **Manage licenses and packages**.

Configuring Security Gateways to Send Logs to a Log Servers

Logs are not automatically forwarded to a Log Server. You must manually configure each relevant Security Gateway to send its logs to the new Domain Log Server.

To configure Domain Security Gateways to send logs to a Log Server:

1. Connect to the applicable Domain Management Server with SmartConsole, and then double-click the applicable Security Gateway.
2. In the **Logs** section, select the new Log Server from the list.

   You can delete or ignore other Log Servers in the list as necessary.
3. Click **OK**.
4. Configure other log settings as applicable.
5. Install Policy on the applicable Security Gateways.
6. Install the database on the Log Servers.

Deleting a Domain Log Server

To delete a Domain Log Server in SmartConsole:

1. Connect with SmartConsole to the primary Multi-Domain Server - the **MDS** context.
2. From the left navigation panel, click **Multi-Domain > Domains**.
3. In the Multi-Domain Log Server column, right-click the Domain Log Server and then select **Delete**.

Configuring Log Settings

Disk cleanup deletes the oldest log files when the available disk space is less than a specified value. Disk cleanup settings are controlled at the Multi-Domain Server level and apply to all Domains and Domain Management Servers. Disk cleanup settings configured at the Domain Management Server level are ignored.

These other log management activities, when configured on a Multi-Domain Server, apply only to that Multi-Domain Server:

- Run script before cleanup
- Alerts
- Stop logging
- Create new log file

Configure these activities individually for each Domain Management Server and Log Server.

To configure log settings for a Multi-Domain Server:

1. In SmartConsole, go to **Multi-Domain** > **Domains**.
2. Double-click the applicable Multi-Domain Server.
3. Click **Log Settings**.
4. In the **General** view, configure these settings:
   - **Cleanup when free disk space is below** - Start the disk cleanup procedure when available disk space is less than the specified quantity. Select to enable (default) or clear to disable. Enter the minimum disk space and unit of measure (Default = 5 GB).

     This parameter applies to the Multi-Domain Server and its Domain Management Servers.

- **Run the following script before cleanup** - Enter a predefined script to run before the cleanup starts.
- **Send Alert when free disk space is below** - Send an alert when available disk space is less that the specified quantity. Select to enable (default). Clear to disable.

  Enter the minimum disk space and unit of measure (Default = 3 GB).

5. In the **Advanced** view, configure these settings:
   - **Accept Syslog messages** - Include syslog messages in the log files.
   - **Stop Logging** - Stop all logging activity when the available disk space is less than the specified quantity.

     Enter the minimum disk space and unit of measure (Default = 100 MB).
   - **Create a new log file** - Close and save the active log file when the active log file is larger than the specified size. The log file has an extension that is a sequential number. You can move these saved log files to external storage or export them to an external database.

     Enter the maximum log file size. (Default = 1 GB).

Log Server Deployment Scenarios

Security Gateways generate logs. The Security Policy on each Security Gateway controls which rules generate log entries. In a Multi-Domain Security Management environment, the Security Gateways send logs to a Domain Management Server or to Domain Log Servers.

Domain Management Servers and Multi-Domain Servers also generate audit logs. The system typically saves audit logs on a Multi-Domain Server, which automatically synchronizes to other Multi-Domain Servers in a High Availability deployment.

You can use one of these strategies to deploy Domain Log Servers in a Multi-Domain Security Management environment:

1. Each Domain has one Domain Log Server on a Multi-Domain Server (default).
2. Each Domain keeps its Domain Log Servers on one or more Multi-Domain Log Servers. If this Domain has more than one Domain Log Server, you must install each one on a different Multi-Domain Log Server.

   Best Practice - Use this strategy in large, geographically distributed environments.

3. Each Domain Security Gateway works as the Log Server for its own logs. This is known as local logging.

For additional information, see *"Deploying a Domain Dedicated Log Server" on page 140*.

Deploying a Domain Dedicated Log Server

Introduction

In a Multi-Domain Security Management environment, the Security Gateways send logs to the Domain Management Server and dedicated Domain Log Servers.

The Multi-Domain Server unifies logs, and they can be stored on the Multi-Domain Server or on a dedicated Multi-Domain Log Server.

Starting in R81, Multi-Domain Server supports a dedicated Log Server (installed on a separate computer) for a Domain.

You can configure a Domain Dedicated Log Server to receive logs only from a specified Domain, and no other Domains can access these logs.

This allows you to locate the dedicated Log Server in a separate network from the Multi-Domain Security Management environment to comply with special regulatory requirements.

Logs reported to the Domain Dedicated Log Server can be viewed from any SmartConsole that has permissions for this Domain.

The Domain Dedicated Log Server communicates directly only with the associated Domain Server. No other Domain can access its log data.

Note - Connecting with SmartConsole to the Domain Dedicated Log Server to see Security Policies is not supported.

Procedure for an R82 Multi-Domain Environment

1. Install an R82 Multi-Domain Server.

   See the *R82 Installation and Upgrade Guide* > Chapter "*Installing a Multi-Domain Server*".

2. Install a regular dedicated R82 Log Server.

   See the *R82 Installation and Upgrade Guide* > Chapter "*Installing a Dedicated Log Server or SmartEvent Server*".

3. Connect with SmartConsole to the specific Domain.

   See the *R82 Multi-Domain Security Management Administration Guide*.

4. Add a regular Log Server object for the dedicated R82 Log Server you installed in Step 2.

Limitation - An administrator who is connected to a Domain Dedicated Log Server in the assigned Domain cannot see the Domain's data in Views, Reports, and Correlated Events that are based on events from the Global SmartEvent Server.

Requirement post upgrade to R82:

For any environment, which uses SmartEvent Server or a Domain Dedicated Log Server, this is a required step to complete post upgrade to R82 from any source version:

After you upgrade the SmartEvent Server or Domain Dedicated Log Server, run this command in the Expert mode on each Multi-Domain Security Management Server:

```
$MDS_FWDIR/scripts/cpm.sh -tm -op reset -d all -sd
```

Procedure for an R77.x Multi-Domain Environment

Upgrade with CPUSE

1. Upgrade all servers from R77.x to R80.20 (or R80.30 or R80.40).

   This applies to all Multi-Domain Servers, Multi-Domain Log Servers, Domain Dedicated Log Servers, and SmartEvent Servers.

   a. Follow the instructions in the *R80.40 Installation and Upgrade Guide*.

      Important - Stop after the CPUSE **Verifier** shows the upgrade / installation is allowed.

      - For Multi-Domain Servers:

        See the chapter "*Upgrade of Multi-Domain Servers and Multi-Domain Log Servers*" > select the applicable section to upgrade "*from R80.10 and lower*" > select the applicable section to upgrade "*with CPUSE*".

      - For Log Servers:

        See the chapter "*Upgrade of Security Management Servers and Log Servers*" > section "*Upgrading a Dedicated Log Server from R80.10 and lower*" > select the applicable section to upgrade "*with CPUSE*".

      - For SmartEvent Servers:

        See the chapter "*Upgrade of Security Management Servers and Log Servers*" > section "*Upgrading a Dedicated SmartEvent Server from R80.10 and lower*" > select the applicable section to upgrade "*with CPUSE*".

   b. Fix all the errors, except the one specified for Log Servers on a Domain Management Server:

      ```
      Log Servers on the Domain Management Server level are
      not yet supported in R80.x
      ```

c. On each Multi-Domain Security Management Server, modify the Pre-Upgrade Verifier to treat the upgrade errors as warnings:

   i. Connect to the command line on the Multi-Domain Server.

   ii. Log in to the Expert mode.

   iii. Enter these commands as they appear below (after each command, press the Enter key):

```
cp -v $CPDIR/tmp/.CPprofile.sh{,_BKP}
cat >> $CPDIR/tmp/.CPprofile.sh << EOF
> export PUV_ERRORS_AS_WARNINGS=1
> EOF
```

d. Restart the CPUSE daemon:

```
DAClient stop ; DAClient start
```

e. Follow the instructions in the *R80.40 Installation and Upgrade Guide* to upgrade all the servers "*with CPUSE*".

2. Upgrade all Multi-Domain Servers to R82.

   See the *R82 Installation and Upgrade Guide* > chapter "*Upgrade of Multi-Domain Servers and Multi-Domain Log Servers*" > select the applicable section to upgrade "*from R80.20 and higher*" > select the applicable section to upgrade "*with CPUSE*".

3. On each Multi-Domain Security Management Server, run this script in the Expert mode:

```
$MDS_FWDIR/scripts/configureCrlDp.sh
```

4. Reboot each Multi-Domain Security Management Server:

```
reboot
```

5. Upgrade all Log Servers and SmartEvent Servers to R82.

   See the *R82 Installation and Upgrade Guide* > chapter "*Upgrade of Security Management Servers and Log Servers*" > section "*Upgrading a Security Management Servers or Log Server from R80.20 and higher*" > section "*Upgrading a Security Management Server or Log Server from R80.20 and higher with CPUSE*".

   Note - To install an R82 Log Server or an R82 SmartEvent Server, see the chapter "*Installing a Dedicated Log Server or SmartEvent Server*".

6. On each Multi-Domain Security Management Server, run this script in the Expert mode:

```
$MDS_FWDIR/scripts/cpm.sh -tm -op reset -d all -sd
```

7. Reboot all the Domain Dedicated Log Servers and the SmartEvent Servers:

```
reboot
```

Advanced Upgrade

1. Upgrade all servers from R77.x to R80.20 (or R80.30 or R80.40).

   This applies to all Multi-Domain Servers, Multi-Domain Log Servers, Domain Dedicated Log Servers, and SmartEvent Servers.

   a. Run the Pre-Upgrade Verifier, as detailed in the *R80.40 Installation and Upgrade Guide*.

      - For Multi-Domain Servers:

        See the chapter "*Upgrade of Multi-Domain Servers and Multi-Domain Log Servers*" > select the applicable section to upgrade "*from R80.10 and lower*" > select the applicable section to upgrade "*with Advanced Upgrade*".

      - For Log Servers:

        See the chapter "*Upgrade of Security Management Servers and Log Servers*" > section "*Upgrading a Dedicated Log Server from R80.10 and lower*" > select the applicable section to upgrade "*with Advanced Upgrade*".

      - For SmartEvent Servers:

        See the chapter "*Upgrade of Security Management Servers and Log Servers*" > section "*Upgrading a Dedicated SmartEvent Server from R80.10 and lower*" > select the applicable section to upgrade "*with Advanced Upgrade*".

   b. Fix all the errors, except the one specified for Log Servers on a Domain Management Server:

```
Log Servers on Domain Management Server level are not
yet supported in R80.x
```

   c. In your active shell window, run this command in the Expert mode:

```
export PUV_ERRORS_AS_WARNINGS=1
```

d. Follow the instructions in the *R80.40 Installation and Upgrade Guide* to upgrade all the servers "*with Advanced Upgrade*".

2. Upgrade all Multi-Domain Servers to R82.

   See the *R82 Installation and Upgrade Guide* > chapter "*Upgrade of Multi-Domain Servers and Multi-Domain Log Servers*" > select the applicable section to upgrade "*from R80.10 and lower*" > select the applicable section to upgrade "*with Advanced Upgrade*".

3. On each Multi-Domain Security Management Server, run this script in the Expert mode:

   ```
   $MDS_FWDIR/scripts/configureCrlDp.sh
   ```

4. Reboot each Multi-Domain Security Management Server:

   ```
   reboot
   ```

5. Upgrade all Log Servers and SmartEvent Servers to R82.

   See the *R82 Installation and Upgrade Guide* > chapter "*Upgrade of Security Management Servers and Log Servers*" > section "*Upgrading a Security Management Servers or Log Server from R80.20 and higher*" > section "*Upgrading a Security Management Server or Log Server from R80.20 and higher with Advanced Upgrade*".

   Note - To install an R82 Log Server or an R82 SmartEvent Server, see the chapter "*Installing a Dedicated Log Server or SmartEvent Server*".

6. On each Multi-Domain Security Management Server, run this script in the Expert mode:

   ```
   $MDS_FWDIR/scripts/cpm.sh -tm -op reset -d all -sd
   ```

7. Reboot all the Domain Dedicated Log Servers and SmartEvent Servers:

   ```
   reboot
   ```

Using the Log View

This is an example of the **Log** view.

Item	Description
1	**Queries** - Predefined and favorite search queries.
2	**Time Period** - Search with predefined custom time periods.
3	**Query search bar** - Define custom queries in this field. You can use the GUI tools or manually enter query criteria. Shows the query definition for the most recent query.
4	**Log statistics pane** (Tab hidden) - Top results of the most recent log query.
5	**Log Servers** - All Multi-Domain Log Servers, Domain Log Servers, and other Log Server objects in the Multi-Domain Security Management deployment. Select one or more Log Servers from this list to include in a query.
6	**Results pane** - All log entries for the most recent query.

Monitoring Multi-Domain Security Management

R80.x includes many powerful, integrated features that let monitor your Multi-Domain Security Management environment directly in SmartConsole. Additionally, you can use the SmartView Monitor client application to work with advanced monitor features, such as:

- Custom queries to filter monitor data
- Custom monitor views
- Monitor Cooperative enforcement
- Monitor users and user activity

Monitoring Multi-Domain Server Status

To see status and general information for Multi-Domain Servers or Multi-Domain Log Servers, select **Multi-Domain** in the SmartConsole Multi-Domain Security Management window. This information appears in the **System Information** area:

- Multi-Domain Server/Multi-Domain Log Servers IP address
- Server type
- SIC trust status
- Last change date and the administrator who worked on it

You can use SmartView Monitor to see other, detailed status information, such as:

- Errors
- CPU, Disk, and Memory utilization
- Active events
- Alert destination

Note - SNMP monitoring on a Multi-Domain Security Management Server and on a Multi-Domain Log Server supports only the main context "MDS", displaying only data that exists in the main context "MDS".

Monitoring Domain Management Server Status

Use the SmartConsole **Logs & Events** view to see Domain and Domain Management Server status. You can also show the combined statistics, in real time, for all Security Gateways in the Domain:

- **Device Status** - Shows Security Gateway device and Software Blade status information
- **License Status** - Shows license status for Software Blades and features
- **System Counters** - Shows operational and performance statistics

You can apply filters and show different types of graphical displays. You can also save the results to your local computer in these formats:

- HTML
- JPG
- CSV file (compatible with Microsoft Excel)
- Plain text file

To see Security Gateway status and monitoring information

1. Open the Domain SmartConsole.
2. Select a Security Gateway.
3. Click **Monitor** on the **Actions** toolbar.

   The **Monitor Information** window opens.
4. Use the toolbar to filter data and change the graph type.

Monitoring Security Gateway Status

You can use the SmartConsole **Logs & Events** view to see Security Gateway status and show operational statistics in real time:

- **Device Status** - Shows Security Gateway device and Software Blade status information
- **License Status** - Shows license status for Software Blades and features
- **System Counters** - Shows operational and performance statistics
- **Traffic information** - Shows traffic, throughput, and other related statistics

You can apply filters and show different types of graphical presentation. You can also save the results to your local computer in these formats:

- HTML
- JPG
- CSV file (compatible with Microsoft Excel)
- Plain text file

To see Security Gateway status and monitoring information

1. Open the Domain SmartConsole.
2. Select a Security Gateway.
3. Click **Monitor** on the **Actions** toolbar.

The **Monitor Information** window opens.

4. Use the toolbar to filter data and change the graph type.

Creating and Changing an Administrator Account

To successfully manage security for a large network, we recommend that you first set up your administrative team, and delegate tasks.

We recommend that you create administrator accounts in SmartConsole, with the procedure below or with the First Time Configuration Wizard.

If you create it through the SmartConsole, you can choose one of these authentication methods:

- **Check Point Password**

  Check Point password is a static password that is configured in SmartConsole. For administrators, the password is stored in the local database on the Management Server. For users, it is stored on the local database on the Security Gateway. No additional software is required.

- **OS Password**

  OS Password is stored on the operating system of the computer on which the Security Gateway (for users) or Security Management Server (for administrators) is installed. You can also use passwords that are stored in a Windows domain. No additional software is required.

- **RADIUS**

  Remote Authentication Dial-In User Service (RADIUS) is an external authentication method that provides security and scalability by separating the authentication function from the access server.

  Using RADIUS, the Security Gateway forwards authentication requests by remote users to the RADIUS server. For administrators, the Security Management Server forwards the authentication requests. The RADIUS server, which stores user account information, does the authentication.

  The RADIUS protocol uses UDP to communicate with the Security Gateway or the Security Management Server.

  RADIUS servers and RADIUS server group objects are defined in SmartConsole.

- **SecurID**

SecurID requires users to both possess a token authenticator and to supply a PIN or password. Token authenticators generate one-time passwords that are synchronized to an RSA Authentication Manager and may come in the form of hardware or software. Hardware tokens are key-ring or credit card-sized devices, while software tokens reside on the PC or device from which the user wants to authenticate. All tokens generate a random, one-time use access code that changes approximately every minute. When a user attempts to authenticate to a protected resource, the one-time use code must be validated by the Authentication Manager.

Using SecurID, the Security Gateway forwards authentication requests by remote users to the Authentication Manager. For administrators, it is the Security Management Server that forwards the requests. The Authentication Manager manages the database of RSA users and their assigned hard or soft tokens. The Security Gateway or the Security Management Server act as an Authentication Manager agent and direct all access requests to the RSA Authentication Manager for authentication. For additional information on agent configuration, refer to RSA Authentication Manager documentation.

There are no specific parameters required for the SecurID authentication method.

- **TACACS**

  Terminal Access Controller Access Control System (TACACS) provides access control for routers, network access servers and other networked devices through one or more centralized servers.

  TACACS is an external authentication method that provides verification services. Using TACACS, the Security Gateway forwards authentication requests by remote users to the TACACS server. For administrators, it is the Security Management Server that forwards the requests. The TACACS server, which stores user account information, authenticates users. The system supports physical card key devices or token cards and Kerberos secret key authentication. TACACS encrypts the user name, password, authentication services and accounting information of all authentication requests to ensure secure communication.

If you create an administrator through `mdsconfig`, the Check Point configuration tool, Check Point password is automatically configured

To create an administrator account using SmartConsole:

1. Click **Manage & Settings > Permissions & Administrators**.

   The **Administrators** pane shows by default.

2. Click **New Administrator**.

   The **New Administrators** window opens.

3. Enter a unique name for the administrator account.

Note - This parameter is case-sensitive.

4. Set the Authentication Method, or create a certificate, or the two of them.

   Note - If you do not do this, the administrator will not be able to log in to SmartConsole.

   To define an Authentication Method:

   In the **Authentication Method** section, select a method and follow the instructions in *Configuring Authentication Methods for Administrators*.

   To create a Certificate - If you want to use a certificate to log in:

   In the **Certificate Information** section, click **Create**, and follow the instructions in *"Creating a Certificate for Logging in to SmartConsole" on page 101*.

5. Select a **Permissions** profile for this administrator, or create a new one.
6. Set the account **Expiration** date:
   - For a permanent administrator - select **Never**
   - For a temporary administrator - select an **Expire At** date from the calendar

   The default expiration date shows, as defined in the Default Expiration Settings. After the expiration date, the account is no longer authorized to access network resources and applications.
7. **Optional**: Configure **Additional Info - Contact Details**, **Email** and **Phone Number** of the administrator.
8. Click **OK**.

To change an existing administrator account:

1. Click **Manage & Settings** > **Permissions & Administrators**.
2. Double-click an administrator account.

   The **Administrators** properties window opens.

Managing Security through API

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

API

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

The API Server runs scripts that automate daily tasks and integrate the Check Point solutions with 3rd-party systems, such as virtualization servers, ticketing systems, 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`

    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 the 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 command line 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 in SmartConsole > **Permissions & Administrators** > **Trusted Clients**.

  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 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   ...
```

Configuring Implied Rules or Kernel Tables for Security Gateways

Introduction

An administrator configures Security Policy and other inspection settings in SmartConsole.

During a policy installation, the Management Server creates the applicable files and transfers them to the target Security Gateways.

The Management Server creates these files based on:

- Security Policy in SmartConsole
- Global properties in SmartConsole
- Security Gateway properties
- Multiple configuration files on the Management Server that control the inspection of various network protocols

It is possible to modify these configuration files on the Management Server to fine-tune the inspection in your network (in Check Point INSPECT language).

There are two main categories of these configuration files:

- Files for Security Gateways that have the same software version as the Management Server.
- Files for Security Gateways that have the a lower software version than the Management Server. This category is called "Backward Compatibility".

Configuration files

File Name	Controls	Location
`user.def`	User-defined implied rules.	See *"Location of 'user.def' Files on the Management Server" on page 160*

File Name	Controls	Location
`implied_rules.def`	Default implied rules.	See *"Location of 'implied_rules.def' Files on the Management Server" on page 177*
`table.def`	Definitions of various kernel tables.	See *"Location of 'table.def' Files on the Management Server" on page 161*
`crypt.def`	VPN encryption macros.	See *"Location of 'crypt.def' Files on the Management Server" on page 163*
`vpn_table.def`	Definitions for various kernel tables that hold VPN data. For example, VPN timeouts, number of VPN tunnels, whether a specific kernel table should be synchronized between cluster members, and others.	See *"Location of 'vpn_table.def' Files on the Management Server" on page 165*
`communities.def`	VPN encryption macros for X11 server (X Window System) traffic.	See *"Location of 'communities.def' Files on the Management Server" on page 169*
`base.def`	Definitions of packet inspection for various network protocols.	See *"Location of 'base.def' Files on the Management Server" on page 171*
`dhcp.def`	Definitions of packet inspection for DHCP traffic - DHCP Request, DHCP Reply, and DHCP Relay.	See *"Location of 'dhcp.def' Files on the Management Server" on page 173*
`gtp.def`	Definitions of packet inspection for GTP (GPRS Tunnelling Protocol) traffic.	See *"Location of 'gtp.def' Files on the Management Server" on page 175*

Configuration Procedure

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 applicable Domain Management Server:

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

4. Back up the current file:

   ```
   cp -v /<Full Path to File>/<File Name>{,_BKP}
   ```

   Example:

   ```
   cp -v $FWDIR/conf/user.def.FW1{,_BKP}
   ```

5. Edit the current file:

   ```
   vi /<Full Path to File>/<File Name>
   ```

   Example:

   ```
   vi $FWDIR/conf/user.def.FW1
   ```

6. Make the applicable changes as described in the applicable SK article, or as instructed by Check Point Support.
7. Save the changes in the file and exit the editor.
8. Connect with SmartConsole to the applicable Domain Management Server.
9. In SmartConsole, install the Access Control Policy on the applicable Security Gateway or Cluster object.

Location of 'user.def' Files on the Management Server

The '`user.def`' files contain the user-defined implied rules.

Important:

- You must edit this file in the context of the applicable Domain Management Server.
  To go to the required context, use the command:
  `mdsenv <IP Address or Name of Domain Management Server>`
- If the required file does not exist, create a copy of the `$FWDIR/conf/user.def.FW1` file, rename it, and edit it.

Location of files on an R82 Domain Management Server:

Version of the Target Security Gateway	Location of the File
R82	`$FWDIR/conf/user.def.FW1`
R81.20	`$FWDIR/conf/user.def.R8120CMP`
R81.10	`$FWDIR/conf/user.def.R8120CMP`
R81.10.x on Quantum Spark Appliances 1500 / 1600 / 1800	`$FWDIR/conf/user.def.SFWR81CMP`
R81	`$FWDIR/conf/user.def.R8120CMP`
R80.40	`$FWDIR/conf/user.def.R8040CMP`
R80.30SP in Maestro	`$FWDIR/conf/user.def.R8040CMP`
R80.30	`$FWDIR/conf/user.def.R8040CMP`
R80.20SP in Maestro, or Scalable Chassis	`$FWDIR/conf/user.def.R8040CMP`
R80.20	`$FWDIR/conf/user.def.R8040CMP`
R80.20.x on Quantum Spark Appliances 1500 / 1600 / 1800	`$FWDIR/conf/user.def.SFWR80CMP`
R80.10	`$FWDIR/conf/user.def.R8040CMP`

Location of 'table.def' Files on the Management Server

The '`table.def`' files contain definitions of various kernel tables for Security Gateways.

Important:

- You must edit this file in the context of the applicable Domain Management Server.
  To go to the required context, use the command:
  `mdsenv <IP Address or Name of Domain Management Server>`
- If the required file does not exist, create a copy of the `$FWDIR/lib/table.def` file, rename it, and edit it.

Location of files on an R82 Domain Management Server:

Version of the Target Security Gateway	Location of the File
R82	`$MDSDIR/customers/<Name_of_Domain>/CPsuite-R82/fw1/lib/table.def`
R81.20	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82/lib/table.def`
R81.10	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82/lib/table.def`
R81.10.x on Quantum Spark Appliances 1500 / 1600 / 1800	`/opt/CPmds-R82/customers/<Name_of_Domain>/CPSFWR81CMP-R82/lib/table.def`
R81	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82/lib/table.def`
R80.40	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/table.def`
R80.30SP in Maestro	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/table.def`
R80.30	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/table.def`
R80.20SP in Maestro, or Scalable Chassis	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/table.def`

Version of the Target Security Gateway	Location of the File
R80.20	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/table.def`
R80.20.x on Quantum Spark Appliances 1500 / 1600 / 1800	`$MDSDIR/customers/<Name_of_Domain>/CPSFWR80CMP-R82/lib/table.def`
R80.10	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/table.def`

Location of 'crypt.def' Files on the Management Server

The '`crypt.def`' files contain VPN encryption macros.

Important:

- You must edit this file in the context of the applicable Domain Management Server.
  To go to the required context, use the command:
  `mdsenv <IP Address or Name of Domain Management Server>`
- If the required file does not exist, create a copy of the `$FWDIR/lib/crypt.def` file, rename it, and edit it.

Location of files on an R82 Domain Management Server:

Version of the Target Security Gateway	Location of the File
R82	`$MDSDIR/customers/<Name_of_Domain>/CPsuite-R82/fw1/lib/crypt.def`
R81.20	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82/lib/crypt.def`
R81.10	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82/lib/crypt.def`
R81.10.x on Quantum Spark Appliances 1500 / 1600 / 1800	`/opt/CPmds-R82/customers/<Name_of_Domain>/CPSFWR81CMP-R82/lib/crypt.def`
R81	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82/lib/crypt.def`
R80.40	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/crypt.def`
R80.30SP in Maestro	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/crypt.def`
R80.30	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/crypt.def`
R80.20SP in Maestro, or Scalable Chassis	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/crypt.def`

Version of the Target Security Gateway	Location of the File
R80.20	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/crypt.def`
R80.20.x on Quantum Spark Appliances 1500 / 1600 / 1800	`$MDSDIR/customers/<Name_of_Domain>/CPSFWR80CMP-R82/lib/crypt.def`
R80.10	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/crypt.def`

Location of 'vpn_table.def' Files on the Management Server

The '`vpn_table.def`' files contain definitions for various kernel tables that hold VPN data.

For example, VPN timeouts, number of VPN tunnels, whether a specific kernel table should be synchronized between cluster members, and others.

Important:

- You must edit this file in the context of the applicable Domain Management Server.
  To go to the required context, use the command:
  `mdsenv <IP Address or Name of Domain Management Server>`
- If the required file does not exist, create a copy of the `$FWDIR/lib/vpn_table.def` file, rename it, and edit it.

Location of files on an R82 Domain Management Server:

Version of the Target Security Gateway	Location of the File
R82	`$MDSDIR/customers/<Name_of_Domain>/CPsuite-R82/fw1/lib/vpn_table.def`
R81.20	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82/lib/vpn_table.def`
R81.10	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82/lib/vpn_table.def`
R81.10.x on Quantum Spark Appliances 1500 / 1600 / 1800	`/opt/CPmds-R82/customers/<Name_of_Domain>/CPSFWR81CMP-R82/lib/vpn_table.def`
R81	`$MDSDIR/customers/<Name_of_Domain>/opt/CPR8120CMP-R82/lib/vpn_table.def`
R80.40	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/vpn_table.def`
R80.30SP in Maestro	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/vpn_table.def`

Version of the Target Security Gateway	Location of the File
R80.30	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/vpn_table.def`
R80.20SP in Maestro, or Scalable Chassis	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/vpn_table.def`
R80.20	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/vpn_table.def`
R80.20.x on Quantum Spark Appliances 1500 / 1600 / 1800	`$MDSDIR/customers/<Name_of_Domain>/CPSFWR80CMP-R82/lib/vpn_table.def`
R80.10	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/vpn_table.def`

Location of 'vpn_route.conf' Files on the Management Server

The '`vpn_route.conf`' files contain the configuration for Domain-Based Site to Site VPN.

Important:

- You must edit this file in the context of the applicable Domain Management Server.
  To go to the required context, use the command:
  `mdsenv <IP Address or Name of Domain Management Server>`
- If the required file does not exist, create a copy of the `$FWDIR/conf/vpn_route.conf` file, rename it, and edit it.

Location of files on an R82 Domain Management Server:

Version of the Target Security Gateway	Location of the File
R82	`$MDSDIR/customers/<Name_of_Domain>/CPsuite-R82/fw1/conf/vpn_route.conf`
R81.20	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82/conf/vpn_route.conf`
R81.10	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82/conf/vpn_route.conf`
R81.10.x on Quantum Spark Appliances 1500 / 1600 / 1800	`/opt/CPmds-R82/customers/<Name_of_Domain>/CPSFWR81CMP-R82/conf/vpn_route.conf`
R81	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82/conf/vpn_route.conf`
R80.40	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/conf/vpn_route.conf`

Version of the Target Security Gateway	Location of the File
R80.30SP in Maestro	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/conf/vpn_route.conf`
R80.30	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/conf/vpn_route.conf`
R80.20SP in Maestro, or Scalable Chassis	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/conf/vpn_route.conf`
R80.20	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/conf/vpn_route.conf`
R80.20.x on Quantum Spark Appliances 1500 / 1600 / 1800	`$MDSDIR/customers/<Name_of_Domain>/CPSFWR80CMP-R82/conf/vpn_route.conf`
R80.10	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/conf/vpn_route.conf`

Location of 'communities.def' Files on the Management Server

The '`communities.def`' files contain VPN encryption macros for X11 server (X Window System) traffic.

Important:

- You must edit this file in the context of the applicable Domain Management Server.
  To go to the required context, use the command:
  `mdsenv <IP Address or Name of Domain Management Server>`
- If the required file does not exist, create a copy of the `$FWDIR/lib/communities.def` file, rename it, and edit it.

Location of files on an R82 Domain Management Server:

Version of the Target Security Gateway	Location of the File
R82	`$MDSDIR/customers/<Name_of_Domain>/CPsuite-R82/fw1/lib/communities.def`
R81.20	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82/lib/communities.def`
R81.10	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82/lib/communities.def`
R81.10.x on Quantum Spark Appliances 1500 / 1600 / 1800	`/opt/CPmds-R82/customers/<Name_of_Domain>/CPSFWR81CMP-R82/lib/communities.def`
R81	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82/lib/communities.def`
R80.40	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/communities.def`

Version of the Target Security Gateway	Location of the File
R80.30SP in Maestro	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/communities.def`
R80.30	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/communities.def`
R80.20SP in Maestro, or Scalable Chassis	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/communities.def`
R80.20	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/communities.def`
R80.20.x on Quantum Spark Appliances 1500 / 1600 / 1800	`$MDSDIR/customers/<Name_of_Domain>/CPSFWR80CMP-R82/lib/communities.def`
R80.10	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/communities.def`

Location of 'base.def' Files on the Management Server

The '`base.def`' files contain definitions of packet inspection for various network protocols.

Important:

- You must edit this file in the context of the applicable Domain Management Server.
  To go to the required context, use the command:
  `mdsenv <IP Address or Name of Domain Management Server>`
- If the required file does not exist, create a copy of the `$FWDIR/lib/base.def` file, rename it, and edit it.

Location of files on an R82 Domain Management Server:

Version of the Target Security Gateway	Location of the File
R82	`$MDSDIR/customers/<Name_of_Domain>/CPsuite-R82/fw1/lib/base.def`
R81.20	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82/lib/base.def`
R81.10	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82/lib/base.def`
R81.10.x on Quantum Spark Appliances 1500 / 1600 / 1800	`/opt/CPmds-R82/customers/<Name_of_Domain>/CPSFWR81CMP-R82/lib/base.def`
R81	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82/lib/base.def`
R80.40	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/base.def`
R80.30SP in Maestro	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/base.def`
R80.30	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/base.def`
R80.20SP in Maestro, or Scalable Chassis	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/base.def`

Version of the Target Security Gateway	Location of the File
R80.20	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/base.def`
R80.20.x on Quantum Spark Appliances 1500 / 1600 / 1800	`$MDSDIR/customers/<Name_of_Domain>/CPSFWR80CMP-R82/lib/base.def`
R80.10	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/base.def`

Location of 'dhcp.def' Files on the Management Server

The '`dhcp.def`' files contain definitions of packet inspection for DHCP traffic - DHCP Request, DHCP Reply, and DHCP Relay.

Important:

- You must edit this file in the context of the applicable Domain Management Server.
  To go to the required context, use the command:
  `mdsenv <IP Address or Name of Domain Management Server>`
- If the required file does not exist, create a copy of the `$FWDIR/lib/dhcp.def` file, rename it, and edit it.

Location of files on an R82 Domain Management Server:

Version of the Target Security Gateway	Location of the File
R82	`$MDSDIR/customers/<Name_of_Domain>/CPsuite-R82/fw1/lib/dhcp.def`
R81.20	`$MDSDIR/customers/<Name_of_Domain>/CPsuite-R82/fw1/lib/dhcp.def`
R81.10	`$MDSDIR/customers/<Name_of_Domain>/CPsuite-R82/fw1/lib/dhcp.def`
R81.10.x on Quantum Spark Appliances 1500 / 1600 / 1800	`/opt/CPmds-R82/customers/<Name_of_Domain>/CPSFWR81CMP-R82/lib/dhcp.def`
R81	`$MDSDIR/customers/<Name_of_Domain>/CPsuite-R82/fw1/lib/dhcp.def`
R80.40	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/dhcp.def`
R80.30SP in Maestro	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/dhcp.def`
R80.30	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/dhcp.def`

Version of the Target Security Gateway	Location of the File
R80.20SP in Maestro, or Scalable Chassis	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/dhcp.def`
R80.20	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/dhcp.def`
R80.20.x on Quantum Spark Appliances 1500 / 1600 / 1800	`$MDSDIR/customers/<Name_of_Domain>/CPSFWR80CMP-R82/lib/dhcp.def`
R80.10	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/dhcp.def`

Location of 'gtp.def' Files on the Management Server

The '`gtp.def`' files contain definitions of packet inspection for GTP (GPRS Tunnelling Protocol) traffic.

Important:

- You must edit this file in the context of the applicable Domain Management Server.
  To go to the required context, use the command:
  `mdsenv <IP Address or Name of Domain Management Server>`
- If the required file does not exist, create a copy of the `$FWDIR/lib/gtp.def` file, rename it, and edit it.

Location of files on an R82 Domain Management Server:

Version of the Target Security Gateway	Location of the File
R82	`$MDSDIR/customers/<Name_of_Domain>/CPsuite-R82/fw1/lib/gtp.def`
R81.20	`$MDSDIR/customers/<Name_of_Domain>//CPR8120CMP-R82/lib/gtp.def`
R81.10	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82lib//gtp.def`
R81.10.x on Quantum Spark Appliances 1500 / 1600 / 1800	`/opt/CPmds-R82/customers/<Name_of_Domain>/CPSFWR81CMP-R82/lib/gtp.def`
R81	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82/lib/gtp.def`
R80.40	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/gtp.def`
R80.30SP in Maestro	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/gtp.def`
R80.30	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/gtp.def`

Version of the Target Security Gateway	Location of the File
R80.20SP in Maestro, or Scalable Chassis	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/gtp.def`
R80.20	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/gtp.def`
R80.20.x on Quantum Spark Appliances 1500 / 1600 / 1800	`$MDSDIR/customers/<Name_of_Domain>/CPSFWR80CMP-R82/lib/gtp.def`
R80.10	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/gtp.def`

Location of 'implied_rules.def' Files on the Management Server

The '`implied_rules.def`' files contain the default implied rules.

Important:

- You must edit this file in the context of the applicable Domain Management Server.
  To go to the required context, use the command:
  `mdsenv <IP Address or Name of Domain Management Server>`
- If the required file does not exist, create a copy of the `$FWDIR/lib/implied_rules.def` file, rename it, and edit it.

Location of files on an R82 Domain Management Server:

Version of the Target Security Gateway	Location of the File
R82	`$MDSDIR/customers/<Name_of_Domain>/CPsuite-R82/fw1/lib/implied_rules.def`
R81.20	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82/lib/implied_rules.def`
R81.10	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82/lib/implied_rules.def`
R81.10.x on Quantum Spark Appliances 1500 / 1600 / 1800	`/opt/CPmds-R82/customers/<Name_of_Domain>/CPSFWR81CMP-R82/lib/implied_rules.def`
R81	`$MDSDIR/customers/<Name_of_Domain>/CPR8120CMP-R82/lib/implied_rules.def`
R80.40	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/implied_rules.def`

Version of the Target Security Gateway	Location of the File
R80.30SP in Maestro	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/implied_rules.def`
R80.30	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/implied_rules.def`
R80.20SP in Maestro, or Scalable Chassis	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/implied_rules.def`
R80.20	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/implied_rules.def`
R80.20.x on Quantum Spark Appliances 1500 / 1600 / 1800	`$MDSDIR/customers/<Name_of_Domain>/CPSFWR80CMP-R82/lib/implied_rules.def`
R80.10	`$MDSDIR/customers/<Name_of_Domain>/CPR8040CMP-R82/lib/implied_rules.def`

Command Line Reference

See the *R82 CLI Reference Guide*.

Below is a limited list of applicable commands.

Syntax Legend for CLI Commands

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.
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.

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 *R82 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@R82_MDS:0]# cma_migrate /var/log/orig_R7x_database.tgz
/opt/CPmds-R82/customers/MyDomain3/CPsuite-R82/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.
`cpmacro <options>`	Overwrites the current `cp.macro` file with the specified `cp.macro` file.
`download <options>`	Downloads all associated Check Point Service Contracts from the User Center, or from a local file.
`mgmt`	Delivers the Service Contract information from the Management Server to the managed Security Gateways.
`print <options>`	Shows all the installed licenses and whether the Service Contract covers these license, which entitles them for upgrade or not.
`summary <options>`	Shows post-installation summary.
`update <options>`	Updates Check Point Service Contracts from your User Center account.

Parameter	Description
`verify`	Checks whether the Security Gateway is eligible for an upgrade. This command also interprets the return values and shows a meaningful message.

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 267*).
`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 computer 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 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 computer 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>
```

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 195*.
`auto <options>`	Shows and configures the automatic start of Check Point products during boot. See *"cp_conf auto" on page 198*.
`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 199*.
`client <options>`	Configures the GUI clients that can use SmartConsole to connect to the Security Management Server. See *"cp_conf client" on page 201*.

Parameter	Description
`finger <options>`	Shows the ICA's Fingerprint. See *"cp_conf finger" on page 205*.
`lic <options>`	Manages Check Point licenses. See *"cp_conf lic" on page 206*.
`snmp <options>`	Do **not** use these outdated commands. To configure SNMP, see the *R82 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 menu.
  To define additional administrators, use SmartConsole.
- This command corresponds to the option **Administrator** in the 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 - On a Multi-Domain Server, use the option **Automatic Start of Multi-Domain Server** in the *"mdsconfig" on page 501* menu.

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

cp_conf ca

Description

This command changes the settings of 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

```
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 236*
`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 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 - 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 501* 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:
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]
```

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 269*.
`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 269*.
`del <Signature Key>`	Delete the license based on its signature. This is the same command as the *"cplic del" on page 274*.
`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 278*.

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 *R82 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}`	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 & Events** 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 & Events** 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 232*.

Parameter	Description
`double_sign <options>`	Creates a second signature for a certificate. See *"cpca_client double_sign" on page 234*.
`get_crldp <options>`	Shows how to access a CRL file from a CRL Distribution Point. See *"cpca_client get_crldp" on page 236*.
`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 238*.
`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 239*.
`lscert <options>`	Shows all certificates issued by the ICA. See *"cpca_client lscert" on page 240*.
`revoke_cert <options>`	Revokes a certificate issued by the ICA. See *"cpca_client revoke_cert" on page 243*.
`revoke_non_exist_ cert <options>`	Revokes a non-existent certificate issued by the ICA. See *"cpca_client revoke_non_exist_cert" on page 246*.
`search <options>`	Searches for certificates in the ICA. See *"cpca_client search" on page 247*.
`set_ca_services <options>`	Controls the Certificate Authority Services Portal. See *"cpca_client set_ca_services" on page 250*.
`set_cert_validity <options>`	Configures the default certificate validity period for new certificates. See *"cpca_client set_cert_validity" on page 252*.
`set_mgmt_tool <options>`	Controls the ICA Management Tool. See *"cpca_client set_mgmt_tool" on page 253*.
`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 258*.

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 199*" 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 240* 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 240* 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 240* 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 <Maximum 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 <Maximum Number of Results>`	Optional. Specifies the maximum 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 R82, 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).

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.

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 computers.
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 *R82 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 265*.
`contract <options>`	Manages (deletes and installs) the Check Point Service Contract on the local Check Point computer. See *"cplic contract" on page 267*.
`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 269*.

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 271*.
`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 273*.
`del <options>`	Deletes a Check Point license on a host, including unwanted evaluation, expired, and other licenses. See *"cplic del" on page 274*.
`del <Object Name> <options>`	Detaches a Central license from a remote managed Security Gateway or Cluster Member. See *"cplic del <object name>" on page 275*.
`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 276*.
`print <options>`	Prints details of the installed Check Point licenses on the local Check Point computer. See *"cplic print" on page 278*.
`put <options>`	Installs and attaches licenses on a Check Point computer. See *"cplic put" on page 280*.
`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 283*.
`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 286*.

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]#
```

cplic contract

Description

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

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

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 276* 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 `$CPDIR/conf/cp.contract` file on the local Check Point computer.
`put`	Merges the Service Contract to the `$CPDIR/conf/cp.contract` file on the local Check Point computer.
<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 274* 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 278* 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 computer, and on remote managed computers.

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 278* 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 278* 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 computer.

Notes:

- On a Security Gateway / Cluster Member / Scalable Platform Security Group, this command prints all installed licenses (both Local and Central).
- Before installing a valid license, and after you establish SIC between this Security Gateway / Cluster Member and its Management Server, this command shows the trial license.

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.

Parameter	Description
{-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 computer.

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 computer and if the signature is valid.
`{-s | -select}`	Selects only the local license whose IP address matches the IP address of the Check Point computer.

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 computer. 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 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`

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 *R82 Security Management Administration Guide*.

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 290*.
`{del | delete} <options>`	Deletes a SmartUpdate software package from the repository. See *"ppkg delete" on page 291*.
`get`	Updates the list of the SmartUpdate software packages in the repository. See *"cppkg get" on page 293*.
`getroot`	Shows the path to the root directory of the repository (the value of the environment variable `$SUROOT`). See *"cppkg getroot" on page 294*.
`print`	Prints the list of SmartUpdate software packages in the repository. See *"cppkg print" on page 295*.
`setroot <options>`	Configures the path to the root directory of the repository. See *"cppkg setroot" on page 296*.

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               R77.20Gaia 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 295* 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               R77.20Gaia 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               R77.20Gaia 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 computer.
- Enables and disables Check Point products and features on this Check Point computer.

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`

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 computer is configured as a Management Server

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

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 504* 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]#
```

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`).

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>
```

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.

Parameter	Description
`-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.
`-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 - 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]#
```

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 316*.
`cprestart <options>`	Runs the `cprestart` command on the managed Security Gateway. See *"cprinstall cprestart" on page 317*.
`cpstart <options>`	Runs the `cpstart` command on the managed Security Gateway. See *"cprinstall cpstart" on page 318*.
`cpstop <options>`	Runs the `cpstop` command on the managed Security Gateway. See *"cprinstall cpstop" on page 319*.
`delete <options>`	Deletes a snapshot (backup) file on the managed Security Gateway. See *"cprinstall delete" on page 320*.
`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 321*.
`install <options>`	Installs Check Point products on the managed Security Gateway. See *"cprinstall install" on page 322*.
`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 325*.
`show <options>`	Displays all snapshot (backup) files on the managed Security Gateway that runs on SecurePlatform OS. See *"cprinstall show" on page 326*.
`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 327*.
`transfer <options>`	Transfers a software package from the repository to the managed Security Gateway without installing the package. See *"cprinstall transfer" on page 328*.
`uninstall <options>`	Uninstalls Check Point products on the managed Security Gateway. See *"cprinstall uninstall" on page 330*.

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 332*.

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     R75.20R75.20

Vendor             Product            Major Version       Minor Version
-------------------------------------------------------------------
Check Point        VPN-1 Power/UTM    R75.20R75.20Check Point        SecurePlatform
R75.20R75.20Check Point        SmartPortal        R75.20R75.20
[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 332* 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 295* 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 326* 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 326* 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 295* 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 332* command.
- After uninstalling a product package, you must run the *"cprinstall get" on page 321* command.
- To see the values for the package attributes, run the *"cppkg print" on page 295* 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 295* 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.
```

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.

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 computer, 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
```

Parameters

Parameter	Description
`config <options>`	Configures the Check Point WatchDog. See *"cpwd_admin config" on page 339*.
`del <options>`	Temporarily deletes a monitored process from the WatchDog database of monitored processes. See *"cpwd_admin del" on page 342*.
`detach <options>`	Temporarily detaches a monitored process from the WatchDog monitoring. See *"cpwd_admin detach" on page 343*.
`exist`	Checks whether the WatchDog process `cpwd` is alive. See *"cpwd_admin exist" on page 344*.
`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 345*.
`getpid <options>`	Shows the PID of a monitored process. See *"cpwd_admin getpid" on page 347*.

Parameter	Description
`kill <options>`	Terminates the WatchDog process `cpwd`. See *"cpwd_admin kill" on page 348*. **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 349*.
`monitor_list`	Prints the status of actively monitored processes on the screen. See *"cpwd_admin monitor_list" on page 352*.
`start <options>`	Starts a process as monitored by the WatchDog. See *"cpwd_admin start" on page 353*.
`start_monitor`	Starts the active WatchDog monitoring - WatchDog monitors the predefined processes actively. See *"cpwd_admin start_monitor" on page 355*.
`stop <options>`	Stops a monitored process. See *"cpwd_admin stop" on page 356*.
`stop_monitor`	Stops the active WatchDog monitoring - WatchDog monitors all processes only passively. See *"cpwd_admin stop_monitor" on page 358*.

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
```

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
`no_limit`	■ Range: -1, 0, >0 ■ Default: 5	If `rerun_mode=1`, specifies the maximum 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 - 20000 ■ Default: 10000	Configures the maximum 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 349* command does not show the deleted process anymore.
- This change applies until all Check Point services restart during boot, or with the *"mdsstart_customer" on page 512* command.

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

```
cpwd_admin del -name <Application Name>
```

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 349* command in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`

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 349* command does not show the detached process anymore.
- This change applies until all Check Point services restart during boot, or with the *"mdsstart_customer" on page 512* command.

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

```
cpwd_admin detach -name <Application Name>
```

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 349* command in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`

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
```

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]
```

Parameters

Parameter	Description
`-full`	Shows the verbose output.

Output

Column	Description
`APP`	Shows the WatchDog name of the monitored process.
`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 339*).
`MON`	Shows how the WatchDog monitors this process (see the explanation for the *"cpwd_admin" on page 336*): ■ `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-R82/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>
```

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 349* command in the leftmost column `APP`. Examples: ■ `FWM` ■ `FWD` ■ `CPD` ■ `CPM`

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 *"mdsstop_customer" on page 519* and *"mdsstart_customer" on page 512* commands.

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

```
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 10000 processes.
To increase this threshold, use the command "`cpwd_admin config -a num_of_procs=<value>`".
See *"cpwd_admin config" on page 339*.

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

```
cpwd_admin list [-full]
```

Parameters

Parameter	Description
`-full`	Shows the verbose output.

Output

Column	Description
APP	Shows the WatchDog name of the monitored process.
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 339*).
MON	Shows how the WatchDog monitors this process (see the explanation for the *"cpwd_admin" on page 336*): ■ 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-
R82/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-R82/log_indexer/log_
indexer
SMARTLOG_SERVER 20100  E     1       [17:50:55] 31/5/2019   N    /opt/CPSmartLog-
R82/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 - 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-R82/bin/cpviewd
            COMMAND = cpviewd
-------------------------------------------------------------------------------
HISTORYD    0      T     0       [17:54:44] 31/5/2019   60/5       N
            PATH = /opt/CPshrd-R82/bin/cpview_historyd
            COMMAND = cpview_historyd
-------------------------------------------------------------------------------
CPD         19730  E     1       [17:54:45] 31/5/2019   60/5       Y
            PATH = /opt/CPshrd-R82/bin/cpd
            COMMAND = cpd
-------------------------------------------------------------------------------
SOLR        19935  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPrt-R82/bin/java_solr
            COMMAND = java_solr /opt/CPrt-R82/conf/jetty.xml
-------------------------------------------------------------------------------
RFL         19951  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPrt-R82/bin/LogCore
            COMMAND = LogCore
-------------------------------------------------------------------------------
SMARTVIEW   19979  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPrt-R82/bin/SmartView
            COMMAND = SmartView
-------------------------------------------------------------------------------
INDEXER     20032  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPrt-R82/log_indexer/log_indexer
            COMMAND = /opt/CPrt-R82/log_indexer/log_indexer
-------------------------------------------------------------------------------
SMARTLOG_SERVER 20100  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPSmartLog-R82/smartlog_server
            COMMAND = /opt/CPSmartLog-R82/smartlog_server
            ENV = LANG=C
-------------------------------------------------------------------------------
CP3DLOGD    20237  E     1       [17:50:55] 31/5/2019   60/5       N
            PATH = /opt/CPuepm-R82/bin/cp3dlogd
            COMMAND = cp3dlogd
-------------------------------------------------------------------------------
EPM         20251  E     1       [17:50:56] 31/5/2019   60/5       N
            PATH = /opt/CPuepm-R82/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]#
```

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 336*.

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

```
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}]
```

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`
`-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: "`$FWDIR/bin/fwm`" ■ For FWD: "`/opt/CPsuite-R82/fw1/bin/fw`" ■ For CPD: "`$CPDIR/bin/cpd`" ■ For CPM: "`/opt/CPsuite-R82/fw1/scripts/cpm.sh`" ■ For SICTUNNEL: "`/opt/CPshrd-R82/bin/cptnl`"

Parameter	Description
`-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-R82/fw1/scripts/cpm.sh -s`" ■ For SICTUNNEL: "`/opt/CPshrd-R82/bin/cptnl -c "/opt/CPuepm-R82/engine/conf/cptnl_srv.conf"`"
`-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 339*.
`-retry_limit {<Limit> | u}`	Configures the value of the "`retry_limit`" configuration parameter. See *"cpwd_admin config" on page 339*. ■ *<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 336* command.

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

```
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>]
```

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`
`-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: "`$FWDIR/bin/fwm`" ■ For FWD: "`/opt/CPsuite-R82/fw1/bin/fw`" ■ For CPD: "`$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`"

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

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 336* command.

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

```
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 computer 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`

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 computer. See *"fw fetchlogs" on page 374*.
`hastat <options>`	Shows information about Check Point computers in High Availability configuration and their states. See *"fw hastat" on page 378*.

Parameter	Description
`kill <options>`	Kills the specified Check Point process. See *"fw kill" on page 379*.
`log <options>`	Shows the content of Check Point log files - Security (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`). See *"fw log" on page 380*.
`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 390*.
`lslogs <options>`	Shows a list of Check Point log files - Security (`$FWDIR/log/*.log*`) or Audit (`$FWDIR/log/*.adtlog*`), located on the local computer or a remote computer. See *"fw lslogs" on page 394*.
`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 397*.
`repairlog <options>`	Rebuilds pointer files for Check Point log files - Security (`$FWDIR/log/*.log`) or Audit (`$FWDIR/log/*.adtlog`). See *"fw repairlog" on page 400*.
`sam <options>`	Manages the Suspicious Activity Monitoring (SAM) rules. See *"fw sam" on page 401*.

`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 409*.

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 390*.

     ```
     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-R82/fw1/log/MyGW__2019-06-01_000000.log
/opt/CPsuite-R82/fw1/log/MyGW__2019-06-01_000000.logaccount_ptr
/opt/CPsuite-R82/fw1/log/MyGW__2019-06-01_000000.loginitial_ptr
/opt/CPsuite-R82/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 Management Servers, run the *"cpstat" on page 305* 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]#
```

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`

Field Header	Description	Example
`src`	Object name or IP address of the connection's source computer	`MyHost`
`dst`	Object name or IP address of the connection's destination computer	`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 374* 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-R82/fw1/log/fw.log
/opt/CPsuite-R82/fw1/log/MyGW__2018-06-13_185451.log
[Expert@MGMT:0]#

[Expert@MyGW:0]# ls $FWDIR/log/*.log
/opt/CPsuite-R82/fw1/log/fw.log
/opt/CPsuite-R82/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 390* 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 390* 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:

- See the *"fw sam_policy" on page 409* and *"sam_alert" on page 538* 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.

Important:

- You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).
- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must connect to the applicable Security Group.
- VSNext mode and Traditional VSX mode do **not** support Suspicious Activity Monitoring (SAM) Rules. See sk79700.

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.

Parameter	Description
`-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`.
`-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 the SIC names comparison. ■ For more information about enabling the 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 computer (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.

Parameter	Description
`-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.
`-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.

Parameter	Description
`-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.
`-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 sk182350 - How to configure Rate Limiting rules for DoS Mitigation.

Also, see these commands:

- *"fw sam" on page 401*
- *"sam_alert" on page 538*

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.
- You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).
- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must connect to the applicable Security Group.
- VSNext mode and Traditional VSX mode do **not** support Suspicious Activity Monitoring (SAM) Rules. See sk79700.

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 412*.
`batch`	Adds or deletes many Rate Limiting rules at a time. See *"fw sam_policy batch" on page 425*.
`del <options>`	Deletes one configured Rate Limiting rule one at a time. See *"fw sam_policy del" on page 427*.
`get <options>`	Shows all the configured Rate Limiting rules. See *"fw sam_policy get" on page 430*.

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.
- You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).
- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must connect to the applicable Security Group.
- VSNext mode and Traditional VSX mode do **not** support Suspicious Activity Monitoring (SAM) Rules. See sk79700.

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 maximum number of concurrent active connections that match this rule. ■ `concurrent-conns-ratio <Value>` Specifies the maximum 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 maximum 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 maximum total number of bytes per second in packets that match this rule. ■ `byte-rate-ratio <Value>` Specifies the maximum 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 maximum number of connections per second that match the rule. ■ `new-conn-rate-ratio <Value>` Specifies the maximum 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 maximum 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.
- You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).
- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must connect to the applicable Security Group.
- VSNext mode and Traditional VSX mode do **not** support Suspicious Activity Monitoring (SAM) Rules. See sk79700.

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" on page 412*
     - *"fw sam_policy del" on page 427*
   - 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.
- You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).
- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must connect to the applicable Security Group.
- VSNext mode and Traditional VSX mode do **not** support Suspicious Activity Monitoring (SAM) Rules. See sk79700.

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. ■ See *"fw sam_policy get" on page 430*.

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.
- You can run this command in the Expert mode or in Gaia Clish (Gaia gClish on Scalable Platforms).
- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms, you must connect to the applicable Security Group.
- VSNext mode and Traditional VSX mode do **not** support Suspicious Activity Monitoring (SAM) Rules. See sk79700.

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 *"fw sam_policy add" on page 412*.
`-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 439*.
`exportcert <options>`	Export a SIC certificate of the specified object to file. See *"fwm exportcert" on page 440*.
`fetchfile <options>`	Fetches a specified OPSEC configuration file from the specified source computer. See *"fwm fetchfile" on page 441*.
`fingerprint <options>`	Shows the Check Point fingerprint. See *"fwm fingerprint" on page 443*.
`getpcap <options>`	Fetches the IPS packet capture data from the specified Security Gateway. See *"fwm getpcap" on page 445*.
`ikecrypt <options>`	Encrypts a secret with a key. See *"fwm ikecrypt" on page 447*.
`load <options>`	This command is obsolete for R80 and higher. Use the *"mgmt_cli" on page 520* command to load a policy to a managed Security Gateway. See *"fwm load" on page 448*.
`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 449*.
`mds <options>`	Shows information and performs various operations on Multi-Domain Server. See *"fwm mds" on page 454*.
`printcert <options>`	Shows a SIC certificate's details. See *"fwm printcert" on page 456*.
`sic_reset`	Resets SIC on the Management Server. See *"fwm sic_reset" on page 462*.
`snmp_trap <options>`	Sends an SNMP Trap to the specified host. See *"fwm snmp_trap" on page 463*.
`unload <options>`	Unloads the policy from the specified managed Security Gateways. See *"fwm unload" on page 466*.

Parameter	Description
`ver <options>`	Shows the Check Point version of the Management Server. See *"fwm ver" on page 470*.
`verify <options>`	This command is obsolete for R80 and higher. Use the *"mgmt_cli" on page 520* command to verify a policy. See *"fwm verify" on page 471*.

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 computer.

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 computer, from which to fetch the file. **Note** - The local and the remote source computers 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 computer.
<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 & Events > 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 R82 - 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`" 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`"
  - "`cpstart`"

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 R82 - Build 11
[Expert@MGMT:0]#
```

fwm verify

Important - This command is obsolete for R80 and higher. Use the *"mgmt_cli" on page 520* 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 (maximum 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 (maximum 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" • "chainingRrequired" • "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 computer 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 (maximum level, recommended).
`-h <LDAP Server>`	Specifies the LDAP Server computer 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 maximum 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 (maximum level, recommended).
`-h <LDAP Server>`	Specifies the LDAP Server computer 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 (maximum level, recommended).
`-h <LDAP Server>`	Specifies the LDAP Server computer 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 maximum 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-R82/customers/MyDomain_Server/CPsuite-R82/fw1/
[Expert@MDS:0]#
[Expert@MDS:0]# pwd
/opt/CPmds-R82/customers/MyDomain_Server/CPsuite-R82/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-R82/customers/MyDomain_Server/CPsuite-R82/fw1/av
[Expert@MDS:0]#
[Expert@MDS:0]# mcd bin
changing to /opt/CPmds-R82/customers/MyDomain_Server/CPsuite-R82/fw1/bin
[Expert@MDS:0]#
[Expert@MDS:0]# mcd conf
changing to /opt/CPmds-R82/customers/MyDomain_Server/CPsuite-R82/fw1/conf
[Expert@MDS:0]#
[Expert@MDS:0]# mcd log
changing to /opt/CPmds-R82/customers/MyDomain_Server/CPsuite-R82/fw1/log
[Expert@MDS:0]#
[Expert@MDS:0]# mcd scripts
changing to /opt/CPmds-R82/customers/MyDomain_Server/CPsuite-R82/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 *R82 Gaia Administration Guide*.
- About Virtual Machine Snapshots, see the vendor documentation.

Notes:

- 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 495* command.

Important - You must restore on the server that runs same software version, 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 *R82 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 520*.
`mdscmd addlogserver <options>`	`mgmt_cli add-domain` See *"mgmt_cli" on page 520*.
`mdscmd addmanagement <options>`	`mgmt_cli add-domain` See *"mgmt_cli" on page 520*.
`mdscmd assign-globalpolicy <options>`	`mgmt_cli set global-assignment` See *"mgmt_cli" on page 520*.
`mdscmd assignadmin <options>`	`mgmt_cli set-administrator` See *"mgmt_cli" on page 520*.
`mdscmd assignguiclient <options>`	None
`mdscmd deleteadministrator <options>`	None
`mdscmd deletedomain <options>`	`mgmt_cli delete-domain` See *"mgmt_cli" on page 520*.
`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 520*.
`mdscmd disableglobaluse <options>`	None
`mdscmd enableglobaluse <options>`	None
`mdscmd install-globalpolicy <options>`	`mgmt_cli assign-global-assignment` See *"mgmt_cli" on page 520*.
`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 520*.

`mdscmd remove-globalpolicy <options>`	`mgmt_cli delete global-assignment` See *"mgmt_cli" on page 520*.
`mdscmd removeadmin <options>`	`mgmt_cli set-administrator` See *"mgmt_cli" on page 520*.
`mdscmd removeguiclient <options>`	None
`mdscmd runcrossdomainquery <options>`	None
`mdscmd startmanagement <options>`	`mdsstart_customer` See *"mdsstart_customer" on page 512*.
`mdscmd stopmanagement <options>`	`mdsstop_customer` See *"mdsstop_customer" on page 519*.

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 *R82 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.

Menu Option	Description
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.
IPv6 Support for Existing Domain Management Servers	Enables or disables the IPv6 Support on the Domain Management Servers.
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 (*"mdsstat" on page 513*, *"mdsstop" on page 515*, 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-R82/customers/MyDomain_Server/CPsuite-R82/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 512* 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 519* command.

To start the entire Multi-Domain Server, see the *"mdsstart" on page 508* 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

+------+----------------+-----------------+------------+----------+----------+----------+
| Typ e| 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 519* 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 515* 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 512* 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 *R82 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 *R82 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 `$FWDIR/bin/upgrade_tools/` directory.
- If you plan to import the management database on a Management Server that runs a higher software version, then you must use the `migrate` utility from the migration tools package created specifically for that higher software version. See the **Installation and Upgrade Guide** for that higher software version.
- If this command completes successfully, it creates this log file:
  `/var/log/opt/CPshrd-R82/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  For example: */var/log/opt/CPshrd-R82/migrate-2019.06.14_11.03.46.log*
- If this command fails, it creates this log file:
  `$CPDIR/log/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  For example: */opt/CPshrd-R82/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-R82/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-R82/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 *R82 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 *R82 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 `$FWDIR/scripts/` directory.
- If you plan to import the management database on a Management Server that runs a higher software version, then you must use the `migrate_server` utility from the migration tools package created specifically for that higher software version. See the **Installation and Upgrade Guide** for that higher software version.
- If this command completes successfully, it creates this log file:
  `/var/log/opt/CPshrd-R82/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  For example: */var/log/opt/CPshrd-R82/migrate-2022.06.14_11.03.46.log*
- If this command fails, it creates this log file:
  `$CPDIR/log/migrate-<YYYY.MM.DD_HH.MM.SS>.log`
  For example: */opt/CPshrd-R82/log/migrate-2024 - 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 run the Pre-Upgrade Verifier:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server verify -v R82 [-skip_
upgrade_tools_check]
```

- To export the management database and configuration:

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server export -v R82 [-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 R82 [-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 R82
[-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 R82`	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 `$FWDIR/log/` directory. **Important:** ■ The command can export only closed logs (to which the information is not currently written). ■ If you use this parameter, it can take the command a long time to complete (depends on the number of logs).
`-x`	Exports and imports the Check Point logs *with* their log indexes in the `$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).

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.

Example 1 - Export operation succeeded

```
[Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server 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-R82/migrate-2024 - 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-R82/log/migrate-2024 - 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@R82_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 520* 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 401* and *"fw sam_policy" on page 409* 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>
```

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>
```

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.
`-r <Polling Duration>`	Specifies the time in seconds, during which to run consecutive queries. **Note** - Use only when you query a Statistical OID.
`-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.

Parameter	Description
<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 "$CPDIR/bin/cpd_admin" -command "cpd_admin stop"` See *"cpwd_admin stop" on page 356*.
8	Start the CPD daemon: `[Expert@HostName:0]# cpwd_admin start -name CPD -path "$CPDIR/bin/cpd" -command "cpd"` See *"cpwd_admin start" on page 353*.
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 349*.
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 *"$MDSVERUTIL AllCMAs" on page 562*.
`AllVersions`	Returns the internal representation of versions, this Multi-Domain Server recognizes. See *"$MDSVERUTIL AllVersions" on page 563*.
`CMAAddonDir <options>`	Returns the path to the Management Addon directory in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMAAddonDir" on page 566*.
`CMACompDir <options>`	Returns the full path for the specified Backward Compatibility Package in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMACompDir" on page 567*.

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 568*.
`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 569*.
`CMAFw41Dir <options>`	Returns the full path for the `$FWDIR` directory for Edge devices (that are based on FireWall-1 4.1) in the context of the specified Domain Management Server. **Note** - R82 does not support UTM-1 Edge and Safe@Office devices. The information about this command is provided only to describe the existing syntax option until it is removed completely. See *"$MDSVERUTIL CMAFw41Dir" on page 570*.
`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 571*.
`CMAFwDir <options>`	Returns the full path for the `$FWDIR` directory in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMAFwDir" on page 572*.
`CMAIp <options>`	Returns the IPv4 address of the Domain Management Server specified by its name. See *"$MDSVERUTIL CMAIp" on page 573*.
`CMAIp6 <options>`	Returns the IPv6 address of the Domain Management Server specified by its name. See *"$MDSVERUTIL CMAIp6" on page 574*.
`CMALogExporterDir <options>`	Returns the full path for the `$EXPORTERDIR` directory in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMALogExporterDir" on page 575*.

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 576*.
`CMANameByFwDir <options>`	Returns the name of the Domain Management Server based on the context of the current `$FWDIR` directory. See *"$MDSVERUTIL CMANameByFwDir" on page 577*.
`CMANameByIp <options>`	Returns the name of the Domain Management Server based on the specified IPv4 address. See *"$MDSVERUTIL CMANameByIp" on page 578*.
`CMARegistryDir <options>`	Returns the full path for the `$CPDIR/registry/` directory in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMARegistryDir" on page 579*.
`CMAReporterDir <options>`	Returns the full path for the `$RTDIR` directory in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMAReporterDir" on page 580*.
`CMASmartLogDir <options>`	Returns the full path for the `$SMARTLOGDIR` directory in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMASmartLogDir" on page 581*.
`CMASvnConfDir <options>`	Returns the full path for the `$CPDIR/conf/` directory in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMASvnConfDir" on page 582*.
`CMASvnDir <options>`	Returns the full path for the `$CPDIR` directory in the context of the specified Domain Management Server. See *"$MDSVERUTIL CMASvnDir" on page 583*.

Parameter	Description
`ConfDirVersion <options>`	Returns the internal Version ID based on the context of the current `$FWDIR/conf/` directory. See *"$MDSVERUTIL ConfDirVersion" on page 584*.
`CpdbUpParam <options>`	Returns internal version numbers from the internal database. See *"$MDSVERUTIL CpdbUpParam" on page 585*.
`CPprofileDir <options>`	Returns the path to the directory that contains the `.CPprofile.sh` and the `.CPprofile.csh` shell scripts. See *"$MDSVERUTIL CPprofileDir" on page 586*.
`CPVer <options>`	Returns internal Check Point version number. See *"$MDSVERUTIL CPVer" on page 587*.
`CustomersBaseDir <options>`	Returns the full path for the `$MDSDIR/customers/` directory. See *"$MDSVERUTIL CustomersBaseDir" on page 588*.
`DiskSpaceFactor <options>`	Returns the disk-space factor (the `mds_setup` command uses this value during an upgrade). See *"$MDSVERUTIL DiskSpaceFactor" on page 589*.
`InstallationLogDir <options>`	Returns the full path for directory with all installation logs (`/opt/CPInstLog/`). See *"$MDSVERUTIL InstallationLogDir" on page 590*.
`IsIPv6Enabled`	Returns `true`, if IPv6 is enabled in Gaia OS. Returns `false`, if IPv6 is disabled in Gaia OS. See *"$MDSVERUTIL IsIPv6Enabled" on page 591*.
`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 592*.

Parameter	Description
`IsOsSupportsIPv6`	Returns `true`, if the OS supports IPv6. Returns `false`, if the OS does not support IPv6. See *"$MDSVERUTIL IsOsSupportsIPv6" on page 593*.
`LatestVersion`	Returns the internal Version ID of the latest installed version. See *"$MDSVERUTIL LatestVersion" on page 594*.
`MDSAddonDir <options>`	Returns the path to the Management Addon directory in the MDS context. See *"$MDSVERUTIL MDSAddonDir" on page 595*.
`MDSCompDir <options>`	Returns the full path for the specified Backward Compatibility Package in the MDS context. See *"$MDSVERUTIL MDSCompDir" on page 596*.
`MDSDir <options>`	Returns the full path in the `/opt/` directory to the `$MDSDIR` directory. See *"$MDSVERUTIL MDSDir" on page 597*.
`MDSFgDir <options>`	Returns the full path for the `$FGDIR` directory in the MDS context. See *"$MDSVERUTIL MDSFgDir" on page 598*.
`MDSFwbcDir <options>`	Returns the full path in the `/opt/` directory (in the MDS context) for the Backward Compatibility directory for Edge devices. See *"$MDSVERUTIL MDSFwbcDir" on page 599*.
`MDSFwDir <options>`	Returns the full path in the `/opt/` directory for the `$FWDIR` directory in the MDS context. See *"$MDSVERUTIL MDSFwDir" on page 600*.
`MDSIp <options>`	Returns the IPv4 address of Multi-Domain Server. See *"$MDSVERUTIL MDSIp" on page 601*.
`MDSIp6 <options>`	Returns the IPv6 address of Multi-Domain Server. See *"$MDSVERUTIL MDSIp6" on page 602*.
`MDSLogExporterDir <options>`	Returns the full path for the `$EXPORTERDIR` directory in the MDS context. See *"$MDSVERUTIL MDSLogExporterDir" on page 603*.

Parameter	Description
`MDSLogIndexerDir <options>`	Returns the full path for the `$INDEXERDIR` directory in the MDS context. See *"$MDSVERUTIL MDSLogIndexerDir" on page 604*.
`MDSPkgName <options>`	Returns the name of the MDS software package. See *"$MDSVERUTIL MDSPkgName" on page 605*.
`MDSRegistryDir <options>`	Returns the full path for the `$CPDIR/registry/` directory in the MDS context. See *"$MDSVERUTIL MDSRegistryDir" on page 606*.
`MDSReporterDir <options>`	Returns the full path for the `$RTDIR` directory in the MDS context. See *"$MDSVERUTIL MDSReporterDir" on page 607*.
`MDSSmartLogDir <options>`	Returns the full path for the `$SMARTLOGDIR` directory in the MDS context. See *"$MDSVERUTIL MDSSmartLogDir" on page 608*.
`MDSSvnDir <options>`	Returns the full path in the `/opt/` directory for the `$CPDIR` directory in the MDS context. See *"$MDSVERUTIL MDSSvnDir" on page 609*.
`MDSVarCompDir <options>`	Returns the full path in the `/var/opt/` directory for the specified Backward Compatibility Package in the MDS context. See *"$MDSVERUTIL MDSVarCompDir" on page 610*.
`MDSVarDir <options>`	Returns the full path in the `/var/opt/` directory to the `$MDSDIR` directory. See *"$MDSVERUTIL MDSVarCompDir" on page 610*.
`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 612*.

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 613*.
`MDSVarSvnDir <options>`	Returns the full path in the `/var/opt/` directory for the `$CPDIR` directory in the MDS context. See *"$MDSVERUTIL MDSVarSvnDir" on page 614*.
`MSP <options>`	Returns the Minor Service Pack version. See *"$MDSVERUTIL MSP" on page 615*.
`OfficialName <options>`	Returns the official version name. See *"$MDSVERUTIL OfficialName" on page 616*.
`OptionPack <options>`	Returns the internal Option Pack version. See *"$MDSVERUTIL OptionPack" on page 617*.
`ProductName <options>`	Returns the official name of the Multi-Domain Server product. See *"$MDSVERUTIL ProductName" on page 618*.
`RegistryCurrentVer <options>`	Returns the current internal version of Check Point Registry. See *"$MDSVERUTIL RegistryCurrentVer" on page 619*.
`ShortOfficialName <options>`	Returns the short (without spaces) official version name. See *"$MDSVERUTIL ShortOfficialName" on page 620*.
`SmartCenterPuvUpgradeParam <options>`	Returns the version to the Pre-Upgrade Verifier (PUV) in order for it to upgrade to that version. See *"$MDSVERUTIL SmartCenterPuvUpgradeParam" on page 621*.
`SP <options>`	Returns the Service Pack version. See *"$MDSVERUTIL SP" on page 622*.
`SVNPkgName <options>`	Returns the name of the Secure Virtual Network (SVN) package. See *"$MDSVERUTIL SVNPkgName" on page 623*.

Parameter	Description
`SvrDirectory <options>`	Returns the full path for the SmartReporter directory. See *"$MDSVERUTIL SvrDirectory" on page 624*.
`SvrParam <options>`	Returns the SmartReporter version. See *"$MDSVERUTIL SvrParam" on page 625*.

$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 563* 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:

- *"$MDSVERUTIL IsLegalVersion" on page 592*
- *"$MDSVERUTIL OfficialName" on page 616*

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 595* 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 563* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL CMAAddonDir -n MyDomain_Server
/opt/CPmds-R82/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:

- *"$MDSVERUTIL MDSCompDir" on page 596*
- *"$MDSVERUTIL MDSVarCompDir" on page 610*

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-R82
/opt/CPmds-R82/customers/MyDomain_Server/CPR77CMP-R82
[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 598* 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 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL CMAFgDir -n MyDomain_Server
/opt/CPmds-R82/customers/MyDomain_Server/CPsuite-R82/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 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL CMAFw40Dir -n MyDomain_Server
/opt/CPmds-R82/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 - R82 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 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL CMAFw41Dir -n MyDomain_Server
/opt/CPmds-R82/customers/MyDomain_Server/CPEdgecmp-R82
[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 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL CMAFwConfDir -n MyDomain_Server
/opt/CPmds-R82/customers/MyDomain_Server/CPsuite-R82/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 600* 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 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL CMAFwDir -n MyDomain_Server
/opt/CPmds-R82/customers/MyDomain_Server/CPsuite-R82/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 601* 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 563* 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 602* command.

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 563* 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 603* 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 563* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL CMALogExporterDir -n MyDomain_Server
/opt/CPmds-R82/customers/MyDomain_Server/CPrt-R82/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 604* 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 563* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL CMALogIndexerDir -n MyDomain_Server
/opt/CPmds-R82/customers/MyDomain_Server/CPrt-R82/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 563* 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 563* 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 606* 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 563* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL CMARegistryDir -n MyDomain_Server
/opt/CPmds-R82/customers/MyDomain_Server/CPshrd-R82/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 607* 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 563* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL CMAReporterDir -n MyDomain_Server
/opt/CPmds-R82/customers/MyDomain_Server/CPrt-R82
[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 608* 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 563* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL CMASmartLogDir -n MyDomain_Server
/opt/CPmds-R82/customers/MyDomain_Server/CPSmartLog-R82
[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 563* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL CMASvnConfDir -n MyDomain_Server
/opt/CPmds-R82/customers/MyDomain_Server/CPshrd-R82/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:

- *"$MDSVERUTIL MDSSvnDir" on page 609*
- *"$MDSVERUTIL MDSVarSvnDir" on page 614*

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 563* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL CMASvnDir -n MyDomain_Server
/opt/CPmds-R82/customers/MyDomain_Server/CPshrd-R82
[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 563* 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:

- *"$MDSVERUTIL MSP" on page 615*
- *"$MDSVERUTIL SP" on page 622*

Syntax

```
$MDSVERUTIL CpdbUpParam [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* 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 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL CPprofileDir
/opt/CPshrd-R82/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 563* 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 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL CustomersBaseDir
/opt/CPmds-R82/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 563* 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 563* command.

Example

```
[Expert@MDS:0]# $MDSVERUTIL InstallationLogDir
/opt/CPInstLog
[Expert@MDS:0]#
```

$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 563* 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.

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 563* 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 566* command.

Syntax

```
$MDSVERUTIL MDSAddonDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* 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:

- *"$MDSVERUTIL CMACompDir" on page 567*
- *"$MDSVERUTIL MDSVarCompDir" on page 610*

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-R82
/opt/CPR77CMP-R82
[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 611* command.

Syntax

```
$MDSVERUTIL MDSDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSDir
/opt/CPmds-R82
[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 568* command.

Syntax

```
$MDSVERUTIL MDSFgDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSFgDir
/opt/CPsuite-R82/fg1
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL MDSFgDir -v VID_90
/opt/CPsuite-R77/fg1
[Expert@MDS:0]#
```

$MDSVERUTIL MDSFwbcDir

Note - R82 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 612* command.

Syntax

```
$MDSVERUTIL MDSFwbcDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSFwbcDir
/opt/CPEdgecmp-R82
[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:

- *"$MDSVERUTIL MDSVarFwDir" on page 613*
- *"$MDSVERUTIL CMAFwDir" on page 572*

Syntax

```
$MDSVERUTIL MDSFwDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSFwDir
/opt/CPsuite-R82/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 573* command.

Syntax

```
$MDSVERUTIL MDSIp [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* 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 574* command.

Syntax

```
$MDSVERUTIL MDSIp6 [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* command.

$MDSVERUTIL MDSLogExporterDir

Description

Returns the full path for the `$EXPORTERDIR` directory in the MDS context.

In addition, see the *"$MDSVERUTIL CMALogExporterDir" on page 575* command.

Syntax

```
$MDSVERUTIL MDSLogExporterDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSLogExporterDir
/opt/CPrt-R82/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 576* command.

Syntax

```
$MDSVERUTIL MDSLogIndexerDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSLogIndexerDir
/opt/CPrt-R82/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 623* command.

Syntax

```
$MDSVERUTIL MDSPkgName [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSPkgName
CPmds-R82-00
[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 579* command.

Syntax

```
$MDSVERUTIL MDSRegistryDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSRegistryDir
/opt/CPshrd-R82/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 580* command.

Syntax

```
$MDSVERUTIL MDSReporterDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSReporterDir
/opt/CPrt-R82
[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 581* command.

Syntax

```
$MDSVERUTIL MDSSmartLogDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSSmartLogDir
/opt/CPSmartLog-R82
[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:

- *"$MDSVERUTIL CMASvnDir" on page 583*
- *"$MDSVERUTIL MDSVarSvnDir" on page 614*

Syntax

```
$MDSVERUTIL MDSSvnDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSSvnDir
/opt/CPshrd-R82
[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:

- *"$MDSVERUTIL CMACompDir" on page 567*
- *"$MDSVERUTIL MDSCompDir" on page 596*

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-R82
/var/opt/CPR77CMP-R82
[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 597* command.

Syntax

```
$MDSVERUTIL MDSVarDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSVarDir
/var/opt/CPmds-R82
[Expert@MDS:0]#
```

Example 2

```
[Expert@MDS:0]# $MDSVERUTIL MDSVarDir -v VID_90
/var/opt/CPmds-R77
[Expert@MDS:0]#
```

$MDSVERUTIL MDSVarFwbcDir

Note - R82 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 599* command.

Syntax

```
$MDSVERUTIL MDSVarFwbcDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSVarFwbcDir
/var/opt/CPEdgecmp-R82
[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 600* command.

Syntax

```
$MDSVERUTIL MDSVarFwDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSVarFwDir
/var/opt/CPsuite-R82/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:

- *"$MDSVERUTIL CMASvnDir" on page 583*
- *"$MDSVERUTIL MDSSvnDir" on page 609*

Syntax

```
$MDSVERUTIL MDSVarSvnDir [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL MDSVarSvnDir
/var/opt/CPshrd-R82
[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:

- *"$MDSVERUTIL SP" on page 622*
- *"$MDSVERUTIL CpdbUpParam" on page 585*

Syntax

```
$MDSVERUTIL MSP [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* 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 620* command.

Syntax

```
$MDSVERUTIL OfficialName [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* 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 563* 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 563* 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 563* 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 616* command.

Syntax

```
$MDSVERUTIL ShortOfficialName [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* 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 563* 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:

- *"$MDSVERUTIL MSP" on page 615*
- *"$MDSVERUTIL CpdbUpParam" on page 585*

Syntax

```
$MDSVERUTIL SP [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* 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 605* command.

Syntax

```
$MDSVERUTIL SVNPkgName [-v <Version_ID>]
```

Parameters

Parameter	Description
`-v <Version_ID>`	Specifies the internal Version ID. See the *"$MDSVERUTIL AllVersions" on page 563* command.

Example 1

```
[Expert@MDS:0]# $MDSVERUTIL SVNPkgName
CPsuite-R82-00
[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 563* 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 563* 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 520*.

   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.

Glossary

A

Active Domain Server
The only Domain Management Server in a Management High Availability deployment that can manage a specified Domain.

Anti-Bot
Check Point Software Blade on a Security Gateway that blocks botnet behavior and communication to Command and Control (C&C) centers. Acronyms: AB, ABOT.

Anti-Spam
Check Point Software Blade on a Security Gateway that provides comprehensive protection for email inspection. Synonym: Anti-Spam & Email Security. Acronyms: AS, ASPAM.

Anti-Virus
Check Point Software Blade on a Security Gateway that uses real-time virus signatures and anomaly-based protections from ThreatCloud to detect and block malware at the Security Gateway before users are affected. Acronym: AV.

Application Control
Check Point Software Blade on a Security Gateway that allows granular control over specific web-enabled applications by using deep packet inspection. Acronym: APPI.

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

Bridge Mode
Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

C

Cluster
Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Member
Security Gateway that is part of a cluster.

Compliance
Check Point Software Blade on a Management Server to view and apply the Security Best Practices to the managed Security Gateways. This Software Blade includes a library of Check Point-defined Security Best Practices to use as a baseline for good Security Gateway and Policy configuration.

Content Awareness
Check Point Software Blade on a Security Gateway that provides data visibility and enforcement. Acronym: CTNT.

CoreXL
Performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

CoreXL Firewall Instance
On a Security Gateway 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 Distributer. 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.

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.

D

DAIP Gateway
Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway, on which the IP address of the external interface is assigned dynamically by the ISP.

Data Loss Prevention
Check Point Software Blade on a Security Gateway 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.

Distributed Deployment
Configuration in which the Check Point Security Gateway and the Security Management Server products are installed on different computers.

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 Security Gateways 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 Security Gateways that are managed by the corresponding Domain Management Server.

Domain Management Server
Virtual Security Management Server that manages Security Gateways for one Domain, as part of a Multi-Domain Security Management environment. Acronym: DMS.

Dynamic Object
Special object type, whose IP address is not known in advance. The Security Gateway resolves the IP address of this object in real time.

E

Endpoint Policy Management
Check Point Software Blade on a Management Server to manage an on-premises Harmony Endpoint Security environment.

Expert Mode
The name of the elevated command line shell that gives full system root permissions in the Check Point Gaia operating system.

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.

Global Domain
Domain on a Multi-Domain Security Management Server, on which the Multi-Domain 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

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 Security Gateway that inspects traffic encrypted by the Secure Sockets Layer (SSL) protocol for malware or suspicious patterns. Synonym: SSL Inspection. Acronyms: HTTPSI, HTTPSi.

I

ICA
Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

Identity Awareness
Check Point Software Blade on a Security Gateway 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 Logging
Check Point Software Blade on a Management Server to view Identity Logs from the managed Security Gateways with enabled Identity Awareness Software Blade.

Internal Network
Computers and resources protected by the Firewall and accessed by authenticated users.

IPS
Check Point Software Blade on a Security Gateway that inspects and analyzes packets and data for numerous types of risks (Intrusion Prevention System).

IPsec VPN
Check Point Software Blade on a Security Gateway that provides a Site to Site VPN and Remote Access VPN access.

J

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

Log Server
Dedicated Check Point server that runs Check Point software to store and process logs.

Logging & Status
Check Point Software Blade on a Management Server to view Security Logs from the managed Security Gateways.

M

Management Interface
(1) Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway 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.

Mobile Access
Check Point Software Blade on a Security Gateway 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 Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

Multi-Domain 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.

N

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 Policy Management
Check Point Software Blade on a Management Server to manage an on-premises environment with an Access Control and Threat Prevention policies.

O

Open Server
Physical computer manufactured and distributed by a company, other than Check Point.

P

Primary Multi-Domain Server
The Multi-Domain Security Management Server in Management High Availability that you install as Primary.

Provisioning
Check Point Software Blade on a Management Server that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: SmartProvisioning, SmartLSM, Large-Scale Management, LSM.

Q

QoS
Check Point Software Blade on a Security Gateway that provides policy-based traffic bandwidth management to prioritize business-critical traffic and guarantee bandwidth and control latency.

R

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

Secondary Multi-Domain Server
The Multi-Domain Security Management Server in Management High Availability that you install as Secondary.

SecureXL
Check Point product on a Security Gateway that accelerates IPv4 and IPv6 traffic that passes through a Security Gateway.

Security Gateway
Dedicated Check Point server that runs Check Point software to inspect traffic and enforce Security Policies for connected network resources.

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.

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.

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.

SmartProvisioning
Check Point Software Blade on a Management Server (the actual name is "Provisioning") that manages large-scale deployments of Check Point Security Gateways 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 Security Gateway, 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 Security Gateway and the Security Management Server products are installed and configured on the same server.

Standby Domain Server
All Domain Management Servers for a Domain that are not designated as the Active Domain Management Server.

T

Threat Emulation
Check Point Software Blade on a Security Gateway that monitors the behavior of files in a sandbox to determine whether or not they are malicious. Acronym: TE.

Threat Extraction
Check Point Software Blade on a Security Gateway that removes malicious content from files. Acronym: TEX.

U

Updatable Object
Network object that represents an external service, such as Microsoft 365, AWS, Geo locations, and more.

URL Filtering
Check Point Software Blade on a Security Gateway that allows granular control over which web sites can be accessed by a given group of users, computers or networks. Acronym: URLF.

User Directory
Check Point Software Blade on a Management Server that integrates LDAP and other external user management servers with Check Point products and security solutions.

V

VSX
Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

VSX Gateway
Physical server that hosts 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.

Z

Zero Phishing
Check Point Software Blade on a Security Gateway (R81.20 and higher) that provides real-time phishing prevention based on URLs. Acronym: ZPH.