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.

**Check Point R80.10**
For more about this release, see the R80.10 home page [http://supportcontent.checkpoint.com/solutions?id=sk111841](http://supportcontent.checkpoint.com/solutions?id=sk111841).

**Latest Version of this Document**
To learn more, visit the Check Point Support Center [https://supportcenter.checkpoint.com](https://supportcenter.checkpoint.com).

**Feedback**
Check Point is engaged in a continuous effort to improve its documentation. Please help us by sending your comments [mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Multi-Domain Security Management R80.10 Administration Guide](mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Multi-Domain Security Management R80.10 Administration Guide).

**Searching in Multiple PDFs**
To search for text in all the R80.10 PDF documents, download and extract the complete R80.10 documentation package [http://downloads.checkpoint.com/dc/download.htm?ID=54846](http://downloads.checkpoint.com/dc/download.htm?ID=54846).
Use **Shift-Control-F** in Adobe Reader or Foxit reader.

---

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 February 2020</td>
<td>Updated:</td>
</tr>
<tr>
<td></td>
<td>- mds_backup (<a href="#">on page 81</a>)</td>
</tr>
<tr>
<td></td>
<td>- mds_restore (<a href="#">on page 82</a>)</td>
</tr>
<tr>
<td>28 April 2019</td>
<td>Updated:</td>
</tr>
<tr>
<td></td>
<td>Overview of High Availability (<a href="#">on page 52</a>)</td>
</tr>
<tr>
<td>22 January 2018</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
**Contents**

Important Information ................................................................................................................. 3  
Terms ........................................................................................................................................... 7  
Getting Started ............................................................................................................................. 9  
Welcome .............................................................................................................................. 9  
About this Guide ......................................................................................................................... 9  
Basic Multi-Domain Management Components ...................................................................... 10  
  \- The Multi-Domain Server .............................................................................................. 10  
  \- Domain Servers .............................................................................................................. 10  
  \- Domain Log Servers ...................................................................................................... 10  
SmartConsole .............................................................................................................................. 12  
  \- Multi-Domain View ......................................................................................................... 12  
  \- Connecting to SmartConsole .......................................................................................... 13  
  \- Gateways & Servers View .............................................................................................. 14  
Architecture and Processes ......................................................................................................... 15  
Server Architecture .................................................................................................................... 15  
  \- CPM .................................................................................................................................. 15  
  \- PostgreSQL .................................................................................................................... 16  
  \- Solr ................................................................................................................................... 16  
  \- Multi-Domain Server Processes .................................................................................... 17  
  \- Domain Server Processes .............................................................................................. 17  
Check Point Registry .................................................................................................................. 18  
Automatic Start of Multi-Domain Server Processes ................................................................ 18  
Environment Variables .............................................................................................................. 18  
  \- Standard Check Point Environment Variables .............................................................. 19  
Deploying Multi-Domain Management ....................................................................................... 20  
Planning your Deployment ........................................................................................................... 20  
  \- Multi-Site High Availability Deployment ................................................................... 20  
  \- Single Site Deployments ................................................................................................. 20  
  \- Platform & Performance Issues ..................................................................................... 22  
  \- Topology, IP Addresses and Routing .......................................................................... 22  
  \- Using More than one Interface on a Multi-Domain Server ......................................... 23  
  \- Synchronizing Clocks ..................................................................................................... 23  
Protecting the Multi-Domain Management Deployment ......................................................... 24  
  \- Security Gateway Managed by a Domain Server ......................................................... 25  
  \- Defining an Access Control Policy for Multi-Domain Server Components ................. 25  
  \- Using External Authentication Servers ......................................................................... 26  
Managing Domains ..................................................................................................................... 27  
Creating a New Domain ............................................................................................................. 27  
  \- Assigning Trusted Clients to Domains ........................................................................... 28  
  \- Configuring Automatic Domain IP Address Assignment ............................................. 29  
Changing an Existing Domain Configuration ........................................................................... 29  
  \- Deleting a Domain Server ............................................................................................. 29  
  \- Deleting a Domain .......................................................................................................... 29  
Connecting to a Domain Server .............................................................................................. 30  
Working with Cross-Domain Management .............................................................................. 30  
Changing an Existing Multi-Domain Server ............................................................................ 31  
Setting the Domain Server Display Format ............................................................................. 31
Terms

Active Domain Server
The only Domain Server in a High Availability deployment that can manage a specified Domain.

Administrator
A SmartConsole user with permissions to manage Check Point security products and the network environment.

Best Practice
A set of processes methods, systems, or techniques that consistently shows better results than those achieved in other ways.

Domain
A network or a collection of networks related to an entity, such as a company, business unit or geographical location.

Domain Log Server
A Log Server for a specified Domain. It stores and processes logs from Security Gateways that are managed by the corresponding Domain Server.

Domain Management Server
A virtual Security Management Server that manages Security Gateways for one Domain, as part of a Multi-Domain Management environment.

Global Objects
For Multi-Domain Management, all network and objects defined in the Global Domain.

Global Policy
All Policies defined in the Global Domain that can be assigned to Domains, or to specified groups of Domains.

Management Server
A Check Point Security Management Server or a Multi-Domain Server.

Multi-Domain Log Server
A computer that runs Check Point software to store and process logs in Multi-Domain 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 Servers.

Multi-Domain Security Management
A centralized management solution for large-scale, distributed environments with many different Domain networks.

Multi-Domain Server
A computer that runs Check Point software to host virtual management servers called Domain Servers.

Network Objects
Logical representations of every part of corporate topology (physical machines, software components, IP Address ranges, services, and so on).

Permission Profile
A predefined group of SmartConsole access permissions assigned to Domains and administrators. With this feature you can configure complex permissions for many administrators with one definition.

Policy Package
A collection of different types of Security Policies, such as Access Control, Threat Prevention, QoS, and Desktop Security. After installation, Security Gateways enforce all Policies in the Policy Package.

Primary Multi-Domain Server
The Multi-Domain Server in Management High Availability that you install as Primary.

Rule
A set of traffic parameters and other conditions that cause specified actions to be taken for a communication session.
**Rule Base**
The database that contains the rules in a security policy and defines the sequence, in which they are enforced.

**Security Gateway**
A computer that runs Check Point software to inspect traffic and enforces Security Policies for connected network resources.

**Security Policy**
A collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

**SmartConsole**
A Check Point GUI application used to manage Security Policies, monitor products and events, install updates, provision new devices and appliances, and manage a multi-domain environment and each domain.

**Standby Domain Server**
All Domain Servers for a Domain that are not designated as the Active Domain Server.

**VPN Community**
A named collection of VPN domains, each protected by a VPN gateway.
Welcome

*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 Management features only.


- To learn how to work with logs, monitoring, and reports, see the Logging and Monitoring *Administration Guide* [http://downloads.checkpoint.com/dc/download.htm?ID=54830](http://downloads.checkpoint.com/dc/download.htm?ID=54830).

- To learn how to work with Software Blades and their features, see the applicable *Administration Guide(s).*
Basic Multi-Domain Management Components

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

The Multi-Domain Server

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

- Domain 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 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 Server is the functional equivalent of a Security Management Server in a single-domain environment. You connect directly to a Domain 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 Security Management Administration Guide http://downloads.checkpoint.com/dc/download.htm?ID=54842.

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

Domain Log Servers

A typical Multi-Domain 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.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>London Multi-Domain Server with an Active Domain Server for London and a Standby Domain Server for Tokyo</td>
</tr>
<tr>
<td>2</td>
<td>Multi-Domain Log Server with Domain Log Servers for London and Tokyo</td>
</tr>
<tr>
<td>3</td>
<td>Tokyo Multi-Domain Server with an Active Domain Server for Tokyo and a Standby Domain Server for London</td>
</tr>
<tr>
<td>4</td>
<td>Tokyo network</td>
</tr>
<tr>
<td>5</td>
<td>London network</td>
</tr>
<tr>
<td>6</td>
<td>Internet</td>
</tr>
<tr>
<td>![Active Domain Server]</td>
<td>Active Domain Server</td>
</tr>
<tr>
<td>![Standby Domain Server]</td>
<td>Standby Domain Server</td>
</tr>
<tr>
<td>![Domain Log Server]</td>
<td>Domain Log Server</td>
</tr>
</tbody>
</table>
SmartConsole

SmartConsole is the unified application of Check Point R80.10 Security Management. The 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 Management

SmartConsole makes it easy to manage your Multi-Domain 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
Connecting to SmartConsole

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

To connect to a Multi-Domain Server:

1. Run SmartConsole.
2. Enter your user name and password.
3. Enter the Multi-Domain Server IP address, 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 directly to a Domain:

1. Run SmartConsole.
2. Enter your user name and password.
3. Enter the Multi-Domain Server IP address, and then click Login.
4. In the Welcome screen, select a Domain from the list, and then click Proceed.
   SmartConsole opens with the selected Domain Server.
To connect to a Domain Server from the SmartConsole Multi-Domain view:

1. Connect to a Multi-Domain Server with SmartConsole.
2. In the Multi-Domain > Domains view, right-click the required Domain Server in the grid.
3. Select Connect to Domain Server.

**Note** - In a High Availability deployment (on page 52), you can only make changes to a Domain from the active Domain Server. The active Domain Server shows with a black icon. If you connect to a standby Domain Server (white icon), SmartConsole opens in the Read Only mode.

**Gateways & Servers View**

The Gateways & Servers view shows all Security Gateway, Domain Server, and Domain Log Server objects in the Multi-Domain 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 Server opens in SmartConsole and shows the **GW105** configuration window.

**The Gateways & Servers view**

<table>
<thead>
<tr>
<th>Status</th>
<th>Name</th>
<th>Domain</th>
<th>IP</th>
<th>Version</th>
<th>Active Blades</th>
<th>Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>GW105</td>
<td>London</td>
<td>192.168.3.105</td>
<td>R7.20</td>
<td></td>
<td>4000 Appliances</td>
</tr>
<tr>
<td></td>
<td>GW106</td>
<td>NewYork</td>
<td>192.168.3.106</td>
<td>R7.20</td>
<td></td>
<td>12000 Appliances</td>
</tr>
<tr>
<td></td>
<td>GW107</td>
<td>Tokyo</td>
<td>192.168.3.107</td>
<td>R7.20</td>
<td></td>
<td>13000 Appliances</td>
</tr>
<tr>
<td></td>
<td>GW115</td>
<td>London</td>
<td>192.168.3.115</td>
<td>R7.30</td>
<td></td>
<td>21000 Appliances</td>
</tr>
<tr>
<td></td>
<td>GW116</td>
<td>NewYork</td>
<td>192.168.3.116</td>
<td>R7.30</td>
<td></td>
<td>13000 Appliances</td>
</tr>
<tr>
<td></td>
<td>GW117</td>
<td>Tokyo</td>
<td>192.168.3.117</td>
<td>R7.30</td>
<td></td>
<td>61000 Appliances</td>
</tr>
<tr>
<td></td>
<td>London_Server</td>
<td>London</td>
<td>192.168.3.150</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>London_Server_2</td>
<td>London</td>
<td>192.168.3.161</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>London_Server_3</td>
<td>London</td>
<td>192.168.3.170</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>London_Server_4</td>
<td>London</td>
<td>192.168.3.190</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>New_York_Server</td>
<td>NewYork</td>
<td>192.168.3.160</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>New_York_Server</td>
<td>NewYork</td>
<td>192.168.3.161</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>New_York_Server</td>
<td>NewYork</td>
<td>192.168.3.171</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>New_York_Server</td>
<td>NewYork</td>
<td>192.168.3.181</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>Tokyo_Server</td>
<td>Tokyo</td>
<td>192.168.3.152</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>Tokyo_Server_2</td>
<td>Tokyo</td>
<td>192.168.3.162</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>Tokyo_Server_3</td>
<td>Tokyo</td>
<td>192.168.3.172</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>Tokyo_Server_4</td>
<td>Tokyo</td>
<td>192.168.3.182</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
</tbody>
</table>
Architecture and Processes

In This Section:

Server Architecture .................................................................................................................. 15
Check Point Registry .................................................................................................................. 18
Automatic Start of Multi-Domain Server Processes ............................................................... 18
Environment Variables ............................................................................................................. 18

Server Architecture

This section is an overview of the new management architecture introduced in R80, as shown in this diagram:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>R80.10 SmartConsole application</td>
</tr>
<tr>
<td>2</td>
<td>CPM - Legacy Check Point Management Interface</td>
</tr>
<tr>
<td>3</td>
<td>Web Services - Handles communication with the new CPM process</td>
</tr>
<tr>
<td>4</td>
<td>FWM - Legacy management server process</td>
</tr>
<tr>
<td>5</td>
<td>CPM - R80.10 main management server process</td>
</tr>
<tr>
<td>6</td>
<td>PostgreSQL - Relational database system that contains the Rule Base, management objects and configuration settings</td>
</tr>
<tr>
<td>7</td>
<td>Solr - Query and search platform</td>
</tr>
</tbody>
</table>

Communication between the SmartConsole application (1) and the CPM (5) process uses Web Services (3). CPM communicates directly with the PostgreSQL (7) database to update tables or
records. CPM can also use a use Solr (6) to run a query to get information or locate records in the PostgreSQL database.

SmartConsole uses the CPMI (2) protocol to communicate with the legacy FWM (4) process. This is necessary for backward compatibility with pre-R80 Security Gateways. In this case, CPM and FWM communicate directly with each other.

In a Multi-Domain Management environment, only one CPM, PostgreSQL, and Solr instance is necessary to handle transactions with all Domain Servers. In the backward compatibility mode, there is one FWM instance for each Domain Server.

**Note** - Because many of the processes are shared between the MDS and all the Domains, it is not possible to stop or start a Domain server independently of all the other Domains. It is only possible to stop per Domain processes, like FWM, for specific Domains.

**CPM**

**CPM** is the Check Point main management server process for this release. It is a multi-threaded, Java process that uses Web services to expose its functionality and to efficiently handle many, concurrent requests.

- CPM uses port 19009 for remote communication and port 9009 for local SIC traffic
- Log files are located in $MDS_TEMPLATE/log (<file_name>.elg)
- Jar files are located in $MDS_TEMPLATE/cpm-server

**PostgreSQL**

**PostgreSQL** is the relational database manager that handles all data of the Multi-Domain Management and the single Domains Management, and configuration parameters. It also manages a connection pool to support concurrent connections, where each connection is a different process. The pool size is between 10 to 50 concurrent connections.

- PostgreSQL uses port 5432
- The PostgreSQL database is located at $CPDIR/database/postgresql (Also known as $PGDIR)
- PostgreSQL logs are in $MDS_TEMPLATE/log/postgres.elg

**Solr**

**Solr** is the enterprise search platform that handles the state-of-the-art search capabilities in SmartConsole. When a user searches for data in SmartConsole, Solr handles the request and gets the data from the PostgreSQL tables. Solr stores some partial data in a cache for better search performance.

- Solr uses port 8983
- Solr is deployed at $FWDIR/solr
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.

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpd</td>
<td>SVN Foundation infrastructure process</td>
</tr>
<tr>
<td>cpca</td>
<td>The Certificate Authority management process</td>
</tr>
<tr>
<td>fwd</td>
<td>Audit Log server process</td>
</tr>
<tr>
<td>fwm</td>
<td>Legacy Check Point management server main process (R77.x and earlier)</td>
</tr>
</tbody>
</table>

For proper operation of the Multi-Domain Server, these processes must run together with CPM, postres, 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 Servers.

Domain Server Processes

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

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpd</td>
<td>SVN Foundation infrastructure process</td>
</tr>
<tr>
<td>cpca</td>
<td>The Certificate Authority manager process (Domain Servers only)</td>
</tr>
<tr>
<td>fwd</td>
<td>Log server process</td>
</tr>
<tr>
<td>fwm</td>
<td>Legacy Check Point management server main process (R77.x and earlier)</td>
</tr>
<tr>
<td>status_proxy</td>
<td>Status collection of SmartLSM Security Gateways</td>
</tr>
<tr>
<td>sms</td>
<td>Manages communication with UTM-1 Edge Security Gateways</td>
</tr>
</tbody>
</table>

For proper operation of the Domain 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.
Check Point Registry

The Check Point registry, at $CPDIR/registry/HKLM_registry.data, contains installation and version information for the different components of Check Point products. Each Multi-Domain Server, Multi-Domain Log Server, Domain Server, and Log Server has its own registry. The $CPDIR environment variable points to the registry location on each platform or context.

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 C-Shell and for Bourne Shell, which define the necessary environment variables:

- The C-Shell version is /opt/CPshrd-R80.10/tmp/.CPprofile.csh
- The Bourne Shell version is /opt/CPshrd-R80.10/tmp/.CPprofile.sh

Sourcing these files (or in other words, using "source" command in C-Shell or "." command in Bourne Shell) will define the environment necessary for the Multi-Domain Server processes to run.
## Standard Check Point Environment Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FWDIR</td>
<td>Location of Check Point Security Gateway binary/configuration/library files</td>
</tr>
</tbody>
</table>
| MSDIR        | • In the Multi-Domain Server environment, this environment variable is equal to MDSDIR  
• In Domain Server environment, it contains /opt/CPmds-R80/customers/<Domain Server Name>/CPsuite-R80/fw1                                                                                                                                                                                                                                                                                                             |
| PGDIR        | Location of the PostgreSQL database - $CPDIR/database/postgresql                                                                                                                                                                                                                                                                                                                                                                       |
| MDS_TEMPLATE | Location of log files and J ARs                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| CPDIR        | Location of Check Point SVN Foundation binary/configuration/library files that point to different directories in Multi-Domain Server and Domain Server environments                                                                                                                                                                                                                                                                 |
| MDSDIR       | Location of the Multi-Domain Server installation (/opt/CPmds-R80)                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SUROOT       | Points to the location of SmartUpdate packages                                                                                                                                                                                                                                                                                                                                                                                                                                       |
Deploying Multi-Domain Management

In This Section:

Planning your Deployment .............................................................................................................. 20
Protecting the Multi-Domain Management Deployment ............................................................. 24

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 Management deployment work efficiently.

Multi-Site High Availability Deployment

Large enterprises use Multi-Domain 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 Server redundancy
- Domain 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

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.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>London Domain and networks</td>
</tr>
<tr>
<td>2</td>
<td>New York (Headquarters) Domain and networks</td>
</tr>
<tr>
<td>3</td>
<td>Tokyo Domain and networks</td>
</tr>
<tr>
<td>4</td>
<td>SmartConsole clients, typically at a network control center.</td>
</tr>
<tr>
<td>5</td>
<td>Multi-Domain Server</td>
</tr>
<tr>
<td>6</td>
<td>London Domain Server</td>
</tr>
<tr>
<td>7</td>
<td>New York Domain Server</td>
</tr>
<tr>
<td>8</td>
<td>Tokyo Domain Server</td>
</tr>
<tr>
<td>9</td>
<td>Internet</td>
</tr>
</tbody>
</table>
This illustration shows the configuration grid in the SmartConsole Multi Domain view for the example deployment:

<table>
<thead>
<tr>
<th>Domains (4)</th>
<th>Servers (3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>London</td>
<td>London_Server 192.168.3.156</td>
</tr>
<tr>
<td>NewYork</td>
<td>NewYork_Server 192.168.3.155</td>
</tr>
<tr>
<td>Tokyo</td>
<td>Tokyo_Server 192.168.3.157</td>
</tr>
<tr>
<td>Global</td>
<td></td>
</tr>
</tbody>
</table>

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

**Platform & Performance Issues**

Make sure that your Multi-Domain 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 Servers and Multi-Domain Log Servers
- Different Domains, if necessary
- Domain Servers, Domain Log Servers and Security Gateways in a Domain
- A Domain Server and its Domain High Availability peers
- SmartConsole and Multi-Domain Servers, Domain 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.
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 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 the Portal or the operating system CLI
- A third-party synchronization utility
Protecting the Multi-Domain 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 Server or a Security Management Server that is not part of a Multi-Domain 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 Servers manages these Security Gateways.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Active Domain Servers</td>
</tr>
<tr>
<td>2</td>
<td>Standby Domain Servers</td>
</tr>
<tr>
<td>3</td>
<td>Primary Multi-Domain Server with Active and Standby Domain Servers</td>
</tr>
<tr>
<td>4</td>
<td>Security Gateways</td>
</tr>
<tr>
<td>5</td>
<td>Internet</td>
</tr>
<tr>
<td>6</td>
<td>Secondary Multi-Domain Server with Active and Standby Domain Servers</td>
</tr>
</tbody>
</table>
Security Gateway Managed by a Domain Server

You can create a Domain and Domain 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 Server.
3. Connect to the new Domain SmartConsole and create a Security Gateway object.
4. Enable the **Firewall** and other Software Blades on this gateway.

Defining an Access Control Policy for Multi-Domain Server Components

You must create rules in your Security Policies to allow communication between the different Multi-Domain 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:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow connections between SmartConsole and the Multi-Domain Server</td>
<td>SmartConsole Multi-Domain Server</td>
<td>Multi-Domain Server SmartConsole</td>
</tr>
<tr>
<td>Allow connections between Multi-Domain Servers</td>
<td>Multi-Domain Servers</td>
<td>Multi-Domain Servers</td>
</tr>
<tr>
<td>Allow Domain Server status data and certificate exchange between Domain Server High Availability peers</td>
<td>Domain Server peer</td>
<td>Domain Server peer</td>
</tr>
<tr>
<td>Allow Domain Server synchronization between peers</td>
<td>Domain Server peer</td>
<td>Domain Server peer</td>
</tr>
</tbody>
</table>

See the [R80.10 Security Management Administration Guide](http://downloads.checkpoint.com/dc/download.htm?ID=54842) to learn how to create a Security Policy.
Using External Authentication Servers

Multi-Domain Management supports these external authentication solutions:

- RADIUS
- TACACS
- RSA SecurID ACE/Server

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 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 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 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 ACE/Server, 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

In This Section:
- Creating a New Domain .................................................................27
- Changing an Existing Domain Configuration ........................ 29
- Connecting to a Domain Server .......................................................30
- Working with Cross-Domain Management ...................................30
- Changing an Existing Multi-Domain Server ................................31
- Setting the Domain Server Display Format ................................ 31

A Domain Server is the functional equivalent of a Security Management Server in a single-domain environment. You connect directly to a Domain 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

This chapter shows how to create and manage Domains and Domain Servers. Also included in this chapter are procedures for creating and configuring a Secondary Multi-Domain Server.

Creating a New Domain

Use this procedure to create a new Domain together with the first Domain 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.
   a) Enter a unique Domain Server name or accept the default name.
   b) Enter the Domain Server IP address, or click Resolve IP to get the IP Address from the Multi-Domain Server address pool.
   c) Accept the default Domain 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 Server.
   e) Optional: Click Additional Information and enter contact information for the person responsible for this Domain Server.
5. Click OK to save the new Domain and Domain Server.
Notes:
- When you create a new Domain, you must always create at least one new Domain Server with it.
- You can also use this procedure to create Standby Domains and Domain Servers for Domain 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.

Assigning Trusted Clients to Domains

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

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

To add another Domain to an existing trusted client:
1. Select Multi-Domain > Permissions & Administrators > Trusted Clients.
2. Double-click the trusted client name.
3. In the Trusted Client window, add one or more Domains to the Domains Assignment list.

To change a Domain assignment:
1. Select Multi-Domain > Permissions & Administrators > Trusted Clients.
2. Double-click an existing trusted client name.
3. Select an identification criterion from the Type list and enter or change the applicable information.
4. Add or delete one or more Domains in the Domain Assignment list.
5. Optional: Select Multi-Domain Server Trusted Client to apply this assignment to Multi-Domain Servers in addition to the specified Domains.
Configuring Automatic Domain IP Address Assignment

You can configure a Multi-Domain Server to assign an IP address to Domain 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 Servers.

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

1. In the Multi-Domain view, right-click a Multi-Domain Server and select Edit.
   The Multi-Domain Server window opens.
2. From the navigation tree, select Multi-Domain.
3. In the IP Range section, enter the first and last IP address in the range.
4. Click OK.

Changing an Existing Domain Configuration

To change an existing Domain configuration:

1. Connect to the Multi-Domain Server with SmartConsole.
2. In the Multi-Domain >Domains view, double-click the applicable Domain.
3. In the Domain window, select the Domain Server and click the pencil icon (edit).
   Note - You cannot change the Domain name. If you try to do this, an error message shows.
4. Add, delete or change the other Domain definitions as necessary.

Deleting a Domain Server

To delete a Domain Server:

1. Connect to the Multi-Domain Server with SmartConsole and go to the Domains view.
2. Right click a Domain Server in the grid, and then select Delete.

Deleting a Domain

To delete a Domain:

1. In the Domains section, right-click a Domain.
2. Select Delete from the context menu.

This action automatically deletes the active and secondary Domain Servers, Domain Log Servers, and the Domain object.
Connecting to a Domain Server

To connect directly to a Domain:

1. Login to SmartConsole.
2. In the Welcome screen, select a Domain from the list, and then click Proceed.

   SmartConsole opens with the active Domain Server in the Gateways & Servers view.

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

1. Connect to a Multi-Domain Server with SmartConsole.
2. In the Multi-Domain >Domains view, right-click the active Domain Server in the grid.
3. Select Connect to Domain Server.

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

Working with Cross-Domain Management

The Multi-Domain Management Gateways & Servers view lets administrators see and work with Domain 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 to a Multi-Domain Server with SmartConsole.
2. Click Gateways & Servers.

   The Gateways & Servers view shows all Security Gateway and Domain Server objects.

<table>
<thead>
<tr>
<th>Status</th>
<th>Name</th>
<th>Domain</th>
<th>IP</th>
<th>Version</th>
<th>Active Blades</th>
<th>Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>GW105</td>
<td>London</td>
<td>192.168.3.105</td>
<td>R77.20</td>
<td></td>
<td>4000 Appliances</td>
</tr>
<tr>
<td></td>
<td>GW106</td>
<td>NewYork</td>
<td>192.168.3.106</td>
<td>R77.20</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>GW107</td>
<td>Tokyo</td>
<td>192.168.3.107</td>
<td>R77.20</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>GW115</td>
<td>London</td>
<td>192.168.3.115</td>
<td>R77.30</td>
<td></td>
<td>21000 Appliances</td>
</tr>
<tr>
<td></td>
<td>GW116</td>
<td>NewYork</td>
<td>192.168.3.116</td>
<td>R77.30</td>
<td></td>
<td>13000 Appliances</td>
</tr>
<tr>
<td></td>
<td>GW117</td>
<td>Tokyo</td>
<td>192.168.3.117</td>
<td>R77.30</td>
<td></td>
<td>61000 Appliances</td>
</tr>
<tr>
<td></td>
<td>London_Server</td>
<td>London</td>
<td>192.168.3.150</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>London_Server_2</td>
<td>London</td>
<td>192.168.3.161</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>London_Server_3</td>
<td>London</td>
<td>192.168.3.170</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>London_Server_4</td>
<td>London</td>
<td>192.168.3.180</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>NewYork_Server</td>
<td>NewYork</td>
<td>192.168.3.160</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>NewYork_Server</td>
<td>NewYork</td>
<td>192.168.3.151</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>NewYork_Server</td>
<td>NewYork</td>
<td>192.168.3.171</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>NewYork_Server</td>
<td>NewYork</td>
<td>192.168.3.181</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>Tokyo_Server</td>
<td>Tokyo</td>
<td>192.168.3.152</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>Tokyo_Server_2</td>
<td>Tokyo</td>
<td>192.168.3.162</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>Tokyo_Server_3</td>
<td>Tokyo</td>
<td>192.168.3.172</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
<tr>
<td></td>
<td>Tokyo_Server_4</td>
<td>Tokyo</td>
<td>192.168.3.182</td>
<td>R80</td>
<td></td>
<td>Open server</td>
</tr>
</tbody>
</table>

To work with a Security Gateway, double-click Security Gateway object. A SmartConsole instance for the applicable Domain Server opens and automatically shows the Gateway window for the selected Security Gateway. In a High Availability environment, the Active Domain Server opens.
To work with a Domain, double-click its Domain Server object. A SmartConsole instance for the applicable opens and automatically shows the Host window for the selected Domain Server. In a High Availability environment, make sure that you select the Active Domain Server, which opens in the Read/Write mode. Standby Domain 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. Double-click the Multi-Domain Server or Multi-Domain Log Server in the top row of the Domains grid.
2. In the Multi-Domain Server window, change the parameters in the General, Multi-Domain (on page 29) and Log Settings views.

Note - You cannot change the Multi-Domain Server name.

Setting the Domain Server Display Format

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

To set the Domain Server display format:

1. Go to Multi-Domain > Preferences.
2. Select a display format:
   - Domain Server Name and IP (default)
   - Domain Server IP
   - Domain Server Name
Global Management

In This Section:
- The Global Domain ................................................................. 32
- Global Assignments .................................................................. 40
- Updating IPS Protections .......................................................... 43
- Updating the Application & URL Filtering Database .................. 44

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 Management. You cannot delete the Global Domain.

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.

These activities are not supported in this release:

- Create a new Global Domain.
- Define 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.

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 (on page 40). 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 global Policies. To learn more about Policy rules and their configuration procedures, see the R80.10 Security Management Administration Guide http://downloads.checkpoint.com/dc/download.htm?ID=54842.

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.
4. Publish your changes.
5. Go to Multi-Domain > Global Assignments, and assign the configuration (on page 41) to the local Domains. If you assigned the configuration before, and made changes to the Global Domain Policy, reassign the global (on page 42) 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.

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

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Services &amp; Applications</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Management to Gateway traffic</td>
<td>Gateway objects</td>
<td>Management Gateway objects</td>
<td>Any</td>
<td>Any</td>
<td>Accept</td>
</tr>
<tr>
<td>2</td>
<td>FB &amp; Twitter</td>
<td>Internal Net</td>
<td>Any</td>
<td>Any</td>
<td>Facebook Twitter</td>
<td>Drop</td>
</tr>
<tr>
<td>3</td>
<td>Placeholder for Domain Rules</td>
<td>Domain Layer</td>
<td>Domain Layer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>DMZ Notify</td>
<td>Internal Net</td>
<td>DMZ Net</td>
<td>Any</td>
<td>Any</td>
<td>Inform</td>
</tr>
<tr>
<td>5</td>
<td>Cleanup</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Drop</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Services &amp; Applications</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Management to Gateway traffic</td>
<td>Gateway objects</td>
<td>Management Gateway objects</td>
<td>Any</td>
<td>Any</td>
<td>Accept</td>
</tr>
<tr>
<td>2</td>
<td>FB &amp; Twitter</td>
<td>Internal Net</td>
<td>Any</td>
<td>Any</td>
<td>Facebook Twitter</td>
<td>Drop</td>
</tr>
<tr>
<td>3</td>
<td>Parent Rule for Local Domain Policy</td>
<td>Domain Layer</td>
<td>Domain Layer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>External to SD server</td>
<td>External Net</td>
<td>Host_10.10.10.11</td>
<td>Any</td>
<td>Any</td>
<td>Accept</td>
</tr>
<tr>
<td>3.2</td>
<td>Finance</td>
<td>Finance Top Mgmt.</td>
<td>Finance Dept</td>
<td>Any</td>
<td>Any</td>
<td>Accept</td>
</tr>
<tr>
<td>3.3</td>
<td>File Sharing Allowed</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Dropbox Google Docs CP Threat Cloud</td>
<td>Accept</td>
</tr>
<tr>
<td>4</td>
<td>DMZ Notify</td>
<td>Internal Net</td>
<td>DMZ Net</td>
<td>Any</td>
<td>Any</td>
<td>Inform</td>
</tr>
</tbody>
</table>
### 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

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Protected Scope</th>
<th>Protection Site</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Max Security</td>
<td>Portal Server Finance</td>
<td>N/A</td>
<td>Strict</td>
<td>Alert</td>
<td>Policy Targets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Server</td>
<td></td>
<td>Packet</td>
<td>Log Packet</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Finance</td>
<td>N/A</td>
<td>Capture</td>
<td>Capture</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Printers &amp; Other Devices</td>
<td>Peripheral Net</td>
<td>N/A</td>
<td>Basic</td>
<td>Log Packet</td>
<td>Policy Targets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Capture</td>
<td>Capture</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Parent Rule for Domain Policy</td>
<td>Domain Layer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Cleanup</td>
<td>Any</td>
<td>N/A</td>
<td>Optimized</td>
<td>Log Packet</td>
<td>Policy Targets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Capture</td>
<td>Capture</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Protected Scope</th>
<th>Protection Site</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Max Security</td>
<td>Portal Server Finance Server</td>
<td>N/A</td>
<td>Strict</td>
<td>Alert Packet Capture</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

**Global Exceptions (No Rules)**

<table>
<thead>
<tr>
<th></th>
<th>Name</th>
<th>Protected Scope</th>
<th>Protection Site</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-1.1</td>
<td>MS Office False Positives</td>
<td>Any</td>
<td>MS Word MS Publisher MS Excel</td>
<td>Detect</td>
<td>Facebook Twitter</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>2</td>
<td>Printers &amp; Other Devices</td>
<td>Peripheral Net</td>
<td>N/A</td>
<td>Basic</td>
<td>Log Packet Capture</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

**Global Exceptions (No Rules)**

<table>
<thead>
<tr>
<th></th>
<th>Name</th>
<th>Protected Scope</th>
<th>Protection Site</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Placeholder for Domain Policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>Management Threats</td>
<td>Management</td>
<td>N/A</td>
<td>Optimized</td>
<td>Log Packet Capture</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>3.2</td>
<td>Guests</td>
<td>Guest</td>
<td>N/A</td>
<td>Strict</td>
<td>Log Packet Capture</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>4</td>
<td>Cleanup</td>
<td>Any</td>
<td>N/A</td>
<td>Optimized</td>
<td>Log Packet Capture</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

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

**Using Layers with the Global Domain**


- 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 contains pre-R80.10 gateways, 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 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 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 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. Click Publish, and then 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 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, Edge 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 Management view, re-assign the global policy to the related Domains.

**Global Assignments**

A *global assignment* is a Multi-Domain 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](image)
  - 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.](image)
  - 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. Click **Security Policies > Threat Prevention**.
3. In the **Related Tools** section, click **Updates**.
4. In the **IPS** section, click **Update Now**.
5. Connect to the Multi-Domain Server with SmartConsole.
6. Reassign the global configuration.

To revert to an earlier protection package:

1. Connect to the Global Domain with SmartConsole.
2. Click **Security Policies > Threat Prevention**.
3. In the **IPS** section of the **Threat Prevention Updates** page, click **Switch to version**.
4. In the window that opens, select an **IPS Package Version**, and click **OK**.
5. Connect to the Multi-Domain Server with SmartConsole.
6. Reassign the global configuration.

To make sure that **Contract Downloads** is enabled:
1. Connect to the global Domain with SmartConsole.
2. From the main menu, select **Global Properties**.
3. In the **Global Properties** window, click **Security Management**.
4. 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.
5. If you enabled the parameter, connect to Multi-Domain Server and reassign the global configuration.

### 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 **Related Tools** section, click **Updates**.
4. In the **Application & URL Filtering** section, click **Update Now**.
5. Connect to the Multi-Domain Server with SmartConsole.
6. Assign or reassign the global configuration.
Managing Administrators and Permissions

In This Section:

- Configuring Administrators ................................................................. 45
- Creating a Certificate for Logging in to SmartConsole ................................ 47
- Working with Permission Profiles .......................................................... 47

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

- Multi-Domain Servers and Multi-Domain Log Servers
- Domains and Domain 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 Management administrators, based on their area of responsibility. You can assign granular permissions to administrators that manage different elements of the Multi-Domain 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.

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 R80.10 Security Management Administration Guide [http://downloads.checkpoint.com/dc/download.htm?ID=54842].

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 (on page 47).
  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

You can optionally add contact information for this user:

- 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 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 Management environment.
- Domain permission profiles - Defines the permission set per Domain

Predefined Multi-Domain Permission Profiles

Multi-Domain 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:

<table>
<thead>
<tr>
<th>Permission Profile</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Multi-Domain Superuser</strong></td>
<td>Manage all elements of the Multi-Domain Management environment, including: Multi-Domain Servers, Multi-Domain Log Servers, Domains, Domain Servers, Global Policies, administrators and permission profiles. Multi-Domain Superusers manage all Domain objects, including Security Gateways, Policies, rules, networks and other objects.</td>
</tr>
</tbody>
</table>
| **Domain Superuser**     | Manage all Domains, Domain 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. |
| **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 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.

<table>
<thead>
<tr>
<th>Permission Profile</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read/Write</td>
<td>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.</td>
</tr>
<tr>
<td>Read Only</td>
<td>Read only permissions for all Domain data. Read Only lets the administrator see an item, but not change it.</td>
</tr>
</tbody>
</table>

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 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 Management Activities
Enable or disable permissions for these activities:

- **MDMS 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 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.

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.
Overview of 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.

Multi-Domain 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 Server High Availability** is both a redundancy and a Load Sharing solution for Domains. You create a Domain Server on two or more Multi-Domain Servers. These Domain Servers synchronize fully for continuous redundancy.

  One Domain 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 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 Servers

You can only use the Active Domain Server to manage Domain Security Gateways, networks, Security Policies objects and system configuration. Standby Domain Servers synchronize fully for redundancy. You can connect to a Standby Domain 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 Server for each Domain. All others are Standby Domain Servers. If the Active Domain Server fails, you must manually change a Standby Domain 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. (This does not apply to Multi-Domain Log Servers.)
- 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 R80.10 Gaia Administration Guide
  https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_Gaia_Admin

- About the migrate export and migrate import commands, see the R80.10 CLI Reference
  Guide
  ameset.htm.

- About the mds_backup and mds_restore commands, see the R80.10 Multi-Domain
  Management Administration Guide
  https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_Multi-Domai

- 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 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.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>London Multi-Domain Server with an Active Domain Server for London and a Standby Domain Server for Tokyo</td>
</tr>
<tr>
<td>2</td>
<td>Multi-Domain Log Server with Domain Log Servers for London and Tokyo</td>
</tr>
<tr>
<td>3</td>
<td>Tokyo Multi-Domain Server with an Active Domain Server for Tokyo and a Standby Domain Server for London</td>
</tr>
<tr>
<td>4</td>
<td>Tokyo network</td>
</tr>
<tr>
<td>5</td>
<td>London network</td>
</tr>
<tr>
<td>6</td>
<td>Internet</td>
</tr>
</tbody>
</table>

Active Domain Server

Standby Domain Server

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

![Configuration Grid](image)

The system automatically creates the Global Domain when you install Multi-Domain 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 R80.10 secondary Multi-Domain Server.

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.

**Domain Server High Availability and Load Sharing**

This section includes procedures for configuring the Multi-Domain Management environment for secondary Multi-Domain Servers and a Multi-Domain Log Server. When you install Multi-Domain 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 Servers. For example, if a deployment has three Multi-Domain Servers, each Domain can have one Active and two Standby Domain Servers. This lets the Domains load be shared between several physical Multi-Domain Servers.
Example of Domain Server High Availability with Load Sharing:

<table>
<thead>
<tr>
<th>Domains (4)</th>
<th>Servers (3)</th>
<th>MDS110 192.168.3.110</th>
<th>MDS104 192.168.3.104</th>
<th>MDS111 192.168.3.111</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOM155</td>
<td>192.168.3.155</td>
<td></td>
<td>192.168.3.176</td>
<td>192.168.3.166</td>
</tr>
<tr>
<td>DOM165</td>
<td>192.168.3.156</td>
<td></td>
<td>192.168.3.178</td>
<td>192.168.3.165</td>
</tr>
<tr>
<td>DOM175</td>
<td>192.168.3.158</td>
<td>192.168.3.175</td>
<td>192.168.3.167</td>
<td></td>
</tr>
<tr>
<td>Global</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

By default, the Primary Domain Server is Active. All other Domain Servers for that Domain are Standbys. You can change a Standby Domain 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 Server. Standby Domain Servers automatically synchronize with the Active Domain Server. Security Gateways can get a Security Policy and a Certificate Revocation List (CRL) from either the Active or Standby Domain Servers.

Creating a Secondary Domain Server

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

To create a secondary Domain 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.
4. In the Domain Server window, configure the Domain Server name and IP address.

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

- **Note** - You cannot change settings for an existing Domain Server. You must first delete the Domain Server and then create a new one.

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

Initial Synchronization

Initial synchronization occurs automatically when you create a secondary Multi-Domain Server, Multi-Domain Log Server, or Domain 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 Servers synchronize to the standby Domain 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 Servers, you can only run a manual synchronization from the active Domain 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 Servers*

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

To manually synchronize Domain Servers for a Domain:

1. Open SmartConsole for the active Domain 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.

*Changing the Active Domain Server*

If the current Active Domain Server is responsive, use this procedure to set a different Domain Server to Active.

To change an Active Domain Server:

1. Right-click the cell for a Standby Domain Server, and then select **Connect to Domain Server**.
2. In the Domain SmartConsole instance, click **Menu > High Availability**.
3. In the **High Availability Status** window, click a Standby Domain Server **Actions > Set Active**.
4. Close SmartConsole and re-connect to the newly Active Domain SmartConsole.

The Standby Domain Server changes to Active. The Standby Domain Servers automatically synchronize, and a confirmation message shows in the **High Availability** Status window. The synchronization operation can take many minutes to complete.
To manually set the Active Domain Server to Standby
1. Right-click the cell for the Active Domain Server, and select **Connect to Domain Server**.
2. Click **Menu > Management High Availability**.
3. In the **High Availability Status** window, click **Actions > Set Standby**.
4. Confirm when prompted.

The Active Domain Server changes to Standby. Continue the procedure to set a different Domain Server to Active. Until you do this, Domain SmartConsole clients open in the Read Only mode and you cannot work with Domain objects or Policies.

**Note** - SmartConsole clients connected to the Active Domain Server will be disconnected during the procedure for changing the Active Domain Server.

### Looking at High Availability Status

To see Multi-Domain Server and Multi-Domain Log Server High Availability status:

1. Select **Management High Availability** from the **SmartConsole menu**.

   The **High Availability Status window** shows all Multi-Domain Servers and Multi-Domain Log Servers in your environment, together with their synchronization status.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>🌐</td>
<td>Multi-Domain Server (that you are connected to) - Synchronization OK</td>
</tr>
<tr>
<td>🕔</td>
<td>Multi-Domain Server Synchronization OK</td>
</tr>
<tr>
<td>📜</td>
<td>Multi-Domain Log Server Synchronization OK</td>
</tr>
<tr>
<td>-o-</td>
<td>Multi-Domain Server - Not synchronized - No connection with peer</td>
</tr>
</tbody>
</table>

To see Domain Server High Availability status:

1. Connect to a Domain with SmartConsole.
   By default, SmartConsole connects to the Active Domain Server.
2. Select **Management High Availability** from the **SmartConsole menu**.

   The **High Availability Status** window shows the status of all Domain Servers for the selected Domain. You can manually synchronize the peer servers with the Domain Server to which you are connected. You can also connect with SmartConsole to a peer Domain Server in the Read Only mode.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>🌐</td>
<td>Active Domain Server - Synchronization OK</td>
</tr>
<tr>
<td>🕔</td>
<td>Standby Domain Server - Synchronization OK</td>
</tr>
<tr>
<td>📜</td>
<td>Domain Log Server - Synchronization OK</td>
</tr>
<tr>
<td>🖩</td>
<td>Domain Server not synchronized - No connection with peer</td>
</tr>
<tr>
<td>🛠️</td>
<td>Domain Server synchronization in process or has a problem</td>
</tr>
</tbody>
</table>
Note - Domain servers status is reflected also in the Domains view in the SmartConsole connected to the Multi-Domain Server. For more information on synchronization status see the *R80.10 Security Management Administrator Guide*

Failure Recovery

In many cases, you can recover a failed Primary Multi-Domain Server in a High Availability deployment. To do this, promote an existing Secondary Multi-Domain Server to become the Primary. Promote a Secondary Domain Server to become Primary Domain Server. You can then install and configure a new secondary Multi-Domain Server.

**Important:** Use Domain Server promotion only to recover a failed Multi-Domain Server.

Connecting to a Secondary Multi-Domain Server

To connect to a secondary Multi-Domain Server:

1. Make sure that all functional, Secondary Multi-Domain Servers and Multi-Domain Log Servers are up and running.
2. Connect to a secondary Multi-Domain Server with SmartConsole.
3. If the Global Domain Server to be promoted to Primary 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 the connected Global Domain.
Promoting 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.

To promote a Secondary Multi-Domain Server to Primary:

1. Run these commands on the Secondary Multi-Domain Server to be promoted:
   - `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 Secondary Multi-Domain Server registry.

2. Connect to the Check Point Database tool with the Secondary Multi-Domain Server IP address.

   C:\Program Files (x86)\CheckPoint\SmartConsole\R80.10\PROGRAM\GuiDBedit.exe /mds

3. On the Tables tab, select Other and then select (or search for) Multi-Domain Servers.

4. Delete the failed Domain Server object from the Object Name column.

5. Select the Multi-Domain Server to promote.

6. Double-click the Primary field in the bottom pane.
7. Change the value to **true**.
8. Save the database (**File > Save All** or **Ctrl-s**).

**Restoring Domain Servers**

Follow these instructions for each Domain on the failed Primary Domain Server.

⚠️ **Important** - To use this procedure, there must be at least one Active Domain Server on a different Multi-Domain Server.

To restore the Domain Servers:

1. In SmartConsole **Domain** view, select a Domain Server to promote to Primary Domain Server.
2. If the selected Domain Server is Standby, change it to Active:
   a) Open the selected Domain Server in SmartConsole.
   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 command line to change the active Domain Server from Secondary to Primary:
   `> mdsenv <domain_server_name> > promote_util`
   These steps set the Multi-Domain Server context to the specified Domain Server.
4. Open the newly promoted Domain Server in SmartConsole.
5. Find (with **Where Used**) and delete all instances of the failed Domain Server, including the failed Domain Server itself.
6. Publish the changes.
7. If necessary, manually synchronize the Domain Servers.
9. If the promoted Domain Server is using a High Availability Domain Server license, replace it with a standard Domain Server license.

To make Domain Server Active when there is no corresponding peer and the **High Availability Status** window is not available, run these commands:

```
# mdsenv <domain_name>
# mgmt_cli make-server-active force true --domain <domain_name> --user <user_name> --password <password>
```

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

**Finishing the Promotion**

To restore your High Availability deployment, run these commands:

```
mdsstop
mdsstart
```
Deleting a Secondary Multi-Domain Server or Multi-Domain Log Server

To delete a secondary Multi-Domain Server:

1. Move each Active Domain Server on the secondary Multi-Domain Server to another Domain 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 change.

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

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

⚠️ Important - You can only re-establish 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 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

In This Section:

- Working with Log Servers ................................................................. 66
- Configuring Logging ............................................................................. 66
- Log Server Deployment Scenarios ....................................................... 68
- Using the Log View ............................................................................... 69
- Monitoring Multi-Domain Management .............................................. 70

This chapter includes information that is directly related to Multi-Domain Management, with some general background information and basic procedures. See the R80.10 Logging & Monitoring Administration Guide http://downloads.checkpoint.com/dc/download.htm?ID=54830 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 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 & Monitor**
- **SmartView Web Application.** By browsing to: https://<Server IP>/smartview/
  Where *Server IP* is IP address of the Multi-Domain Server or Multi-Domain Log Server.

  **Note** - Include the final backward slash: /
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 Management environment because of the large volume of logs.

To see the logs for a Domain and its Security Gateways, click Logs & Monitor in SmartConsole for that Domain. To see logs for all Domains in one view, click Logs & Monitor in the Multi-Domain Server SmartConsole. You can filter the logs for specified Security Gateways, Domain 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 R80.10 Multi-Domain Log Server. Follow the procedures in the R80.10 Installation and Upgrade Guide http://downloads.checkpoint.com/dc/download.htm?ID=60369. Make sure to define this server as a Multi-Domain Log Server in the First Time Wizard. Connect to the Multi-Domain Server with SmartConsole and go to the Domains view.

2. In the Multi-Domain navigation toolbar, click New > Multi-Domain Log Server.

3. Enter a unique name for this Multi-Domain Log Server.

4. Enter the IPv4 address or click Resolve IP to get the IP address from the DHCP.

5. Select the platform operating system, software version, and hardware type.

6. Click Connect to establish SIC trust.

To create Domain Log Servers:

1. In the SmartConsole Multi-Domain view, right-click the Log Server cell for each Domain in the Multi-Domain Log Server column.

2. Accept the default name or enter a different, unique name.

3. Enter the IPv4 address or click Resolve IP to automatically assign the IPv4 address.

5. In the SmartConsole Multi-Domain view, click Menu > Install Database.

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.

Configuring Security Gateways to Send Logs to a Log Server

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 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 Servers. Disk cleanup settings configured at the Domain 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 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 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 Management environment, the Security Gateways send logs to a Domain Server or to Domain Log Servers.

Domain 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 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.
Using the Log View

This is an example of the Log view.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Queries - Predefined and favorite search queries.</td>
</tr>
<tr>
<td>2</td>
<td>Time Period - Search with predefined custom time periods.</td>
</tr>
<tr>
<td>3</td>
<td>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.</td>
</tr>
<tr>
<td>4</td>
<td>Log statistics pane (Tab hidden) - Top results of the most recent log query.</td>
</tr>
<tr>
<td>5</td>
<td>Log Servers - All Multi-Domain Log Servers, Domain Log Servers, and other Log Server objects in the Multi-Domain Management deployment. Select one or more Log Servers from this list to include in a query.</td>
</tr>
<tr>
<td>6</td>
<td>Results pane - All log entries for the most recent query.</td>
</tr>
</tbody>
</table>
Monitoring Multi-Domain Management

R80.x includes many powerful, integrated features that let monitor your Multi-Domain 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 Management window. This information shows 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

Monitoring Domain Server Status

Use the SmartConsole Logs & Monitor view to see Domain and Domain 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 & Monitor** 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
- JPEG
- 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.
VPN and Multi-Domain Management

In This Section:

- VPN Connectivity.................................................................................................................. 72
- VPN Communities.................................................................................................................... 72
- Global VPN Communities........................................................................................................ 73

VPN Connectivity

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

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

The ICA of the Domain Server issues certificates used by Domain Security Gateways to create SIC trust.

When you establish Global VPN Communities, it automates part of the configuration of Externally Managed Security Gateways and the exchange of certificates for each Domain Server. For more information on VPN with Externally Managed Gateways, see the R80.10 Site to Site VPN Administration Guide https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_SitetoSiteVPN_AdminGuide/html_frameset.htm.

VPN Communities

A VPN Domain is a collection of internal networks that use Security Gateways to send and receive VPN traffic. Define the resources that are included in the VPN Domain for each Security Gateway. Then join the Security Gateways into a VPN community - collection of VPN tunnels and their attributes. Network resources of different VPN Domains can securely communicate with each other through VPN tunnels that terminate at the Security Gateways in the VPN communities.

VPN communities are based on Star and Mesh topologies. In a Mesh community, there are VPN tunnels between each pair of Security Gateway. In a Star community, each satellite Security Gateway has a VPN tunnel to the central Security Gateway, but not to other Security Gateways in the community.

Note - Global VPN Communities are not supported in this release.
Sometimes Domains must establish VPN between Security Gateways that are managed by different Domain Servers. This might happen, for example, in large enterprises that created different Domain Servers to manage corporate networks in different cities or countries. Alternatively, an MSP deployment may require communication between partners, managed as different Domains.

Cross-Domain VPN is handled by the establishment of Global VPN Communities. This community is similar to the regular VPN community with the exception that it can deal with Security Gateways managed by different Domain Servers. An administrator creates a VPN connection between Domain Security Gateways using the Domain Server SmartDashboard. A Global VPN Community however is defined at the Multi-Domain Management level, using SmartConsole and Global SmartDashboard.

Multi-Domain Management utilizes its knowledge about different Domain network environments to ease the definition of VPN for environments run by different Domain Servers. In the standalone model, cross-Domain VPN is established by creating Security Gateways that are defined as externally managed Security Gateway objects. Then certificates and network information are imported into the Security Management Server databases.

In Multi-Domain Management, during the Global VPN Community setup, the Multi-Domain Server automatically exports relevant ICA information (such as the CA certificate) for each Domain Server, so that both sides can trust the other’s ICA.
Security Gateway Global Names

You can configure an existing Domain Security Gateway as a global Security Gateway. This action imports the Security Gateway into the global policy database, making it accessible by all other Domain Servers in your deployment.

Different Domains may coincidentally contain Security Gateways using the same name. Each global Security Gateway object must have its own unique Global Name. To resolve this issue, the Global Names Template automatically assigns a unique name for each global Security Gateway. The default global name format is \texttt{g<Security Gateway name>\_of\_<Domain name>}. For example:

- Security Gateway name =\texttt{MyGateway}
- Domain name =\texttt{MyDomain}
- Global name =\texttt{gMyGateway\_of\_MyDomain}

\textit{Global or Neighbor VPN Security Gateway}

In a global VPN community, VPN tunnels are created between Security Gateways in neighboring Domains. This is analogous to externally managed VPN Security Gateways in a single-domain deployment.

Each Security Gateway supports certificates issued by the CAs of the other Domains.

VPN Domains in Global VPN

The administrator defines each Domain Security Gateway using SmartDashboard. When defining if the Security Gateway is a VPN Security Gateway, the administrator specifies whether the VPN Domain is to be based on the network’s topology or a specific address range.

You manage this network information at the Domain level. The is included in the Domain Server database. For VPN connections between Security Gateways, the VPN domain is flexible and can be defined by the Domain administrator.

Domain Server databases would have to maintain complete data on all other Domain networks, which could also be a security breach. Instead, Multi-Domain Management computes address ranges from those specified in VPN Security Gateway properties. It uses this list as the base for the VPN domain of a particular Security Gateway from another Domain network.

Access Control at the Network Boundary

Check Point Security Gateway provides secure access control through its granular understanding of all underlying services and applications traveling on the network. Stateful Inspection technology provides full application-layer awareness, and comprehensive access control for more than 150 pre-defined applications, services and protocols as well as the ability to specify and define custom services.

Stateful Inspection extracts state-related information required for security decisions from all application layers and maintains this information in dynamic state tables for evaluating subsequent connection attempts. Access Control and Global VPN Communities

Configuring Security Gateways for a Domain Global VPN Community does not create a de facto access control policy between the Security Gateways. The fact that two Security Gateways belong to the same VPN community does not mean the Security Gateways have access to each other.
The configuration of the Security Gateways into a Global VPN Community means that if these Security Gateways are allowed to communicate using an access control policy, then that communication is encrypted. Access control is configured in the security policy rule base.

Using the VPN column of the security policy rule base, it is possible to create access control rules that apply only to members of a VPN community, for example:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Community_A</td>
<td>HTTP</td>
<td>Accept</td>
</tr>
</tbody>
</table>

If all conditions of the rule are met, the rule is matched and the connection allowed.

**Access Control in Global VPN**

Access control for global communities is the same as for a VPN community that belongs to a single Domain.

- If the **Accept all encrypted connections** setting is active, the applicable implied VPN rules appear in the Domain Server policy.
- The community shows in the VPN tab of a rule.


**Joining a Security Gateway to a Global VPN Community**

There are several steps necessary to join a Domain Security Gateway to a Global VPN Community. First, each Domain Security Gateway must be enabled for global use. Then a VPN Community must be defined in Global SmartDashboard, including the global Security Gateway objects representing participating Domain Security Gateways.

Lastly, a Global Policy must be assigned to participating Domains' Domain Servers, and installed on the Domain Security Gateway, for each Domain and Security Gateway participating in the VPN Community. All Security Gateways participating in the Global VPN Community must employ a Simplified VPN policy. The global policy itself may be either neutral or Simplified.

When assigning a global policy to one or more Domains, global objects are copied to the database of the Domain Server. Whether all the global objects in the database are copied, or only those related to the global policy, is configurable per Domain using the **Domain Configuration** window. Rules belonging to the global policy package being assigned are being added above and below the rules inside all local policies defined in that Domain Server database.

For more information about global policies, see Global Policy Management (on page 32).

**Considerations**

When you install policy on Security Gateways in a Domain, they receive the latest Domain Server policy, including the most recent Global Policy. You can make changes to the global policy, and then reassign the global policy to one or more Domains. When a Domain Server then installs the updated policy on the Domain Security Gateways, all modifications to global and local objects and rules are updated on the selected Security Gateways.

The assign and install procedures are two different processes. The administrator can assign a global policy without installing a local policy on Domain Security Gateways.
During the assignment process, each participating Domain receives the CA certificates of the other Domains. For each participating Domain, a global CA Server object is created in the Domain Server. The CA Server object represents the Certificate Authority of the peer Domains. This object allows authentication by Matching Criteria. If the certificate of the peer Domain was already imported manually into the Domain, the Matching Criteria refers to the existing certificate.

Configuring Global VPN Communities

Enabling a Domain Gateway to Join a Global VPN Community

You must close the Global SmartDashboard and SmartDashboard (if they are open in Read/Write mode), in order to perform the Enable for Global Use operation. If they are open in Read Only mode, they can remain open.

> **Note** - Security Gateways enabled for global use do not show in SmartConsole under a Domain Server this is assigned to all global objects, with these exceptions:

- Global services always show if they are used in global rules
- Security Gateways show under a Domain Server that is part of a VPN Community or rules associated thereto.

**Step 1 - In SmartConsole**

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

1. In the General View - Domain Contents Mode (or Network Objects Mode) right click a Domain Security Gateway and select Enable for Global Use (or Manage > Enable for Global Use). You will be required to provide a Global Name for the Security Gateway. A global Security Gateway object and a VPN Domain object are created for the Domain Security Gateway in the Global Database.

2. Enabling clusters: The user can enable a VPN cluster for global use in the same way that a Domain Security Gateway is enabled. The cluster is exported to the Global Policy as a global Security Gateway object.

**Step 2 - In Global SmartDashboard**

1. Define a Global Site-to-Site VPN Community.
2. Add the global Security Gateway objects, defined in step 1, as participating Security Gateways in this community.
3. Define global rules as needed for the new Global VPN Community, the global Security Gateway objects, and the External Domains.

**Step 3 - In SmartConsole**

In the Global Policies View, assign and install the Global Policy to Domains and selected Domain Security Gateways. The Global Policies View has two modes which allow slightly different activities, the Security Policies Mode and the VPN Communities Mode.

Different SmartConsole views allow you to perform this step in slightly different ways. You can assign the policy to one Domain at a time, for greater load management. Or you can assign the policy to all the Domains at once, if load management is not an issue.
To assign to one Domain at a time

Through the Security Policies Mode, select a global policy. Then choose Reassign/Install Global Policy from the Manage menu, or right-click the Domain and select Reassign/Install Global Policy. Select the Domain Security Gateways to which the policy should be installed. The policy is assigned to the Domain Server database, then to the selected Domain Security Gateways.

or

Use the VPN Communities Mode, but the procedure is much the same. Right click a Domain, then select Reassign/Install Global Policy from the Manage menu, or select Reassign/Install Global Policy from the mouse menu.

To assign to many Domains at one time

The procedure is through the Security Policies Mode, similar to the above. Select a Global Policy and right click, then select Manage > Assign/Install Global Policy or Reassign/Install Global Policy, or right-click and select Assign/Install Global Policy.

This operation assigns the Policy to all selected Domains, and then installs the Policy to all Domain Security Gateways, in one step. It does not allow you to select specific Security Gateways to which to install the Policy. If chosen, the Policy will be installed to all of the Security Gateways for the selected Domains. Assigning the Policy to many Domains and all their Security Gateways may take some time. Use this option with caution.

You can now create security rules regarding VPN using SmartDashboard for a Domain Server. Security Gateways which are external to a Domain but are part of the Global VPN Community, will appear as global externally managed Security Gateway objects in the Domain Server SmartDashboard.

The Domain own participating Security Gateways will appear as they usually do. It is not necessary to define authentication for the external global Security Gateway objects. Matching criteria are automatically defined for the global Security Gateway objects referring to the other Domain Server Certificate Authority.

A Domain can be assigned a Global Policy which references a Global VPN Community, in which, however, none of the Domain Security Gateways participate. If this happens, the Domain Server database will have an empty community (without community members).
Managing Security through API and CLI

You can configure and control the Management Server with the new command line tools and through web services. You must first configure the API server.

The API server runs scripts that automate daily tasks and integrate the Check Point solutions with third party systems such as virtualization servers, ticketing systems, and change management systems.

You can use these tools to run API scripts on the Management Server:

- Standalone management tool, included with SmartConsole. You can copy this tool to computers that run Windows or Gaia operating system.
  - mgmt_cli.exe (for Windows operating system)
  - mgmt_cli (for Gaia operating system)
- Web Services API that allows communication and data exchange between the clients and the Management Server over the HTTP protocol. It also lets other Check Point processes communicate with the Management Server over the HTTPS protocol.

All API clients use the same port as the Gaia Portal.

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

- The Online Check Point Management API Reference Guide
- The Developers Network section of CheckMates https://community.checkpoint.com

Configuring the API Server

To configure the API Server:

1. In SmartConsole, go to Manage & Settings > Blades.
2. In the Management API section, click Advanced Settings.
   The Management API Settings window opens.
3. Configure the Startup Settings and the Access Settings.
API Settings

Startup Settings

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

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

If you change the **Automatic start** option:

1. Publish the session changes in SmartConsole.
2. Run the `api restart` command on the Management Server.

Access Settings

Select one of these options to configure which SmartConsole clients 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 to send API requests. You cannot use SmartConsole or web services to send API requests.

- **All IP addresses that can be used for GUI clients** - You can send API requests from all IP addresses that are defined as **Trusted Clients** in SmartConsole. This includes requests from SmartConsole, Web services and the `mgmt_cli` utility.

- **All IP addresses** - You can send API requests from all IP addresses. This includes requests from SmartConsole, Web services and the `mgmt_cli` utility.
Multi-Domain Management Commands and Utilities

Command Line Reference

This section includes documentation CLI Commands that are associated with Multi-Domain Management.

cpmiquerybin

cpmiquerybin connects to a specified database, runs a user-defined query and shows the query results. The results can be a collection of Firewall 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 Server database, run mdsenv (on page 83) and define the necessary environment variables. Use the Domain Server name or IP address as the first parameter.

Note - 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>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| <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 – display FW-1 sets containing data of each retrieved object.  
| <database>      | Name of the database file in quotes. For example, "mdsdb". Use "" 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 the null (""") query to return all objects in the database table.  
|                 | You can use wildcard character (*) as a 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__ |

You can see complete documentation of the cpmiquerybin utility, with the full query syntax, examples and a list of common attributes in sk65181.  
http://supportcontent.checkpoint.com/solutions?id=sk65181
Return Values

0 - Query returns data successfully
1 - Query does not return data or there is a query syntax error

Example:

```bash
# cpmiquerybin attr "" network_objects "" -a __name__
```

DMZZone
WirelessZone
ExternalZone
InternalZone
AuxiliaryNet
LocalMachine_All_Interfaces
CPDShield
InternalNet
LocalMachine
DMZNet

This example shows the names of the currently defined network objects.

**mds_backup**

`mds_backup` 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.

`mds_backup` runs the `gtar` and `dump` commands to backup 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`


To back up a Multi-Domain Server:

1. Run `mds_backup` from a location outside the product directory tree to be backed up. This becomes the working directory.
2. After the backup completes, copy the backup `.tgz` file, together with the `mds_restore`, `gtar` and `gzip` command files, to your external backup location.

**Syntax**

```
mds_backup 
mds_backup [-h] [-g] [-b { -d <target_directory>} -s] [-v] [-l]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>Shows help text.</td>
</tr>
<tr>
<td>-g</td>
<td>Executes without prompting to disconnect GUI clients.</td>
</tr>
<tr>
<td>-b</td>
<td>Batch mode - executes without asking anything (-g is implied).</td>
</tr>
<tr>
<td>Argument</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>-d</td>
<td>Target directory for the backup file. If not specified, the backup file is saved to the current directory. You cannot save the backup file to the root directory.</td>
</tr>
<tr>
<td>-v</td>
<td>&quot;Dry run&quot; - Show all files to be backed up, but does not perform the backup operation.</td>
</tr>
<tr>
<td>-l</td>
<td>Exclude logs from the backup.</td>
</tr>
<tr>
<td>-s</td>
<td>Stop Multi-Domain processes before the backup starts.</td>
</tr>
</tbody>
</table>

**Notes:**
- Do not create or delete Domains or Domain Servers until the backup operation completes.
- It is important not to run mds_backup from directories that will be backed up. For example, when backing up a Multi-Domain Server, do not run mds_backup from `/opt/CPmds-<current_release>` because it is a circular reference (backing up directory that you need to write into).
- Active log files are not backed up. This is necessary to prevent inconsistencies during the read-write operations.
  **Best Practice** - We recommend that you do 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/*
  ```

**mds_restore**

Use this command to restore a Multi-Domain Server that was backed up with `mds_backup`.

If the Multi-Domain Management environment has multiple Multi-Domain Servers, restore all Multi-Domain Servers at the same time.

**Important** - You must restore on the server that runs the 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".

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 a Multi-Domain Server to a new IP address, configure the new address.
mdsenv

Use `mdsenv` to set shell environment variables to run commands on a specified Domain Server. When run without an argument, the command sets the shell for Multi-Domain Server level commands (mdsstart, mdsstop, and so on).

**Syntax**

```
mdsenv [<name>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;name&gt;</td>
<td>Domain Server name.</td>
</tr>
</tbody>
</table>

mdsquerydb

`mdsquerydb` is an advanced database query tool that lets administrators use shell scripts to get information from Check Point Security Management Server databases. Use `mdsquerydb` to get information from the Multi-Domain Server, Domain Server and global databases.

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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;key_name&gt;</td>
<td>Query key, which must be defined in the pre-defined queries configuration file.</td>
</tr>
<tr>
<td>-f &lt;output_file_name&gt;</td>
<td>Send the query results to the specified file name. If this parameter is not specified, the data is sent to the standard output.</td>
</tr>
</tbody>
</table>

**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
- 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
Examples:

To retrieve list of all defined keys, run: `# mdsquerydb`

To send a list of Domains in the Multi-Domain Server database to the standard output, run:
```
# mdsenv
# mdsquerydb Domains
```

To send a list of network objects in the global database to `/tmp/gateways.txt`, run:
```
mdsenv
mdsquerydb NetworkObjects -f /tmp/gateways.txt
```

To get a list of gateway objects in the Domain Server DServer1, run:
```
mdsenv DServer1
mdsquerydb Gateways -f /tmp/gateways.txt
```

mdsstart

Use `mdsstart` to start the Multi-Domain Server and all Domain Servers and `mdsstop` to stop the Multi-Domain Server and all Domain Servers.

**Syntax**

```
mdsstart [-m|-s]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-m</td>
<td>Starts only the Multi-Domain Server and not the Domain Servers.</td>
</tr>
<tr>
<td>-s</td>
<td>Starts the Domain Servers sequentially. The system waits for each Domain Server to come up before it starts the next one.</td>
</tr>
</tbody>
</table>

You can decrease the amount of time it takes to start and stop the Multi-Domain Server when there are many Domain Servers. To do this, set the environment variable `NUM_EXEC_SIMUL` to a smaller number of Domain Servers that start or stop at the same time. By default, the system attempts to start or stop up to 10 Domain Servers at the same time.

mdsstat

`mdsstat` shows the status of processes on the Multi-Domain Server and Domain Servers. The status can be UP or Down.

**Syntax**

```
mdsstat [-h] [-m] [<name>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>Displays help message.</td>
</tr>
<tr>
<td>-m</td>
<td>Test status for Multi-Domain Server only.</td>
</tr>
<tr>
<td>&lt;name&gt;</td>
<td>Enter the name of a Domain Server to show its status.</td>
</tr>
</tbody>
</table>

**Status:**

- **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:

```
# mdsstat
+-----------------------------------------------------------
| Processes status checking                                 |
+-----------------------------------------------------------
| Type| Name           | IP address      | FWM | FWD | CPD | CPCA |
+-----------------|-----------------|-----------------|-----|-----|-----|-----|
| MDS |                | 192.168.3.101   | up 17284 | up 17266 | up 17251 | up 17753 |
| CMA |DOM211_Server   | 192.168.3.211   | up 32227 | up 32212 | up 25725 | up 32482 |
| CMA |DOM212_Server   | 192.168.3.212   | up 4248  | up 4184  | up 4094  | up 4441  |
| Total Domain Management Servers checked: 2     2 up   0 down |
| Tip: Run mdsstat -h for legend                  |
+-----------------------------------------------------------
```

migrate_global_policies

This utility transfers (and upgrades, if necessary) the global configuration database from one Multi-Domain Server to another Multi-Domain Server. `migrate_global_policies` 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 Servers) to a new Multi-Domain Server, disable all Security Gateways that are enabled for global use.

Note - You can only use `migrate_global_policies` when the target Multi-Domain Server does not have global configurations defined.

You can migrate global Policies from these Multi-Domain Management versions:

- R75.x
- R76.x
- R77.x

You can only use `migrate_global_policies` to import files created with `export_database` from Multi-Domain Servers with the above versions. You cannot export an R80.x global configuration database and then use `migrate_global_policies` on an R80.x Multi-Domain Server.

Syntax

```
migrate_global_policies <path>
```

<table>
<thead>
<tr>
<th>parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;path&gt;</td>
<td>The fully qualified path to the directory where the global policies files, originally exported from the source Multi-Domain Server ($MDSDIR/conf), are located.</td>
</tr>
</tbody>
</table>

Example

```
# migrate_global_policies /tmp/exported_global_db.22Jul2007-124547.tgz
```
threshold_config

Use `threshold_config` to configure Policy thresholds. You must be in expert mode to run this command. After you run `threshold_config`, follow the on-screen instructions to make selections and configure the global settings and each threshold.

**Syntax**

`threshold_config`

When you run `threshold_config`, you get these options:

- **Show Policy name** - Shows you the name configured for the threshold Policy.
- **Set Policy name** - Lets you set a name for the threshold Policy.
- **Save Policy** - Lets you save the Policy.
- **Save Policy to file** - Lets you export the Policy to a file.
- **Load Policy from file** - Lets you import a threshold Policy from a file.
- **Configure global alert settings** - Lets you configure global settings for how frequently alerts are sent and how many alerts are sent.
- **Configure alert destinations** - Lets you configure a location or locations where the SNMP alerts are sent.
- **View thresholds overview** - Shows a list of all thresholds that you can set.
- **Configure thresholds** - Open the list of threshold categories to let you select thresholds to configure.
Creating a Domain Server

Prerequisites

- Name or Identifier of the domain, for example `MyDomain`
- Name or Identifier of the new Domain Server, for example `MyDMS`
- IPv4 address for the new Domain 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 Server.

To create a new Domain Server:

1. Open a terminal emulation program (such as PuTTY).
2. Open an SSH connection to the Multi-Domain Server.
3. Log in with the superuser credentials.
4. Enter expert mode.
5. 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 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"
   
   The Domain Server is created. Log in to 192.0.2.1 to configure the settings.
   ```
Using XML to Export Settings for a Domain Server

You can export the settings for a Domain Server to an XML file that you can use with external automation systems. You can include the `printxml` commands in a script or run them individually from the CLI.

This sample script exports these settings to XML:

- Security policy Rule Base
- Network objects
- Services

```
printxml fw_policies ##Standard
printxml network_objects
printxml services
```

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
- OS Password
- RADIUS
- SecurID
- TACACS

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 and Administrators. The Administrators pane shows by default.
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 Configuring Certificates for Administrators (on page 47).
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 and Administrators.
2. Double-click an administrator account.
   The Administrators properties window opens.