Provider-1

R71

Administration Guide
More Information

The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=10311

For additional technical information about Check Point visit Check Point Support Center (http://supportcenter.checkpoint.com).

Feedback

Check Point is engaged in a continuous effort to improve its documentation. Please help us by sending your comments to us (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Provider-1 R71 Administration Guide).

© 2010 Check Point Software Technologies Ltd.

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

RESTRICTED RIGHTS LEGEND:

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

TRADEMARKS:

Please refer to our Copyright page (http://www.checkpoint.com/copyright.html) for a list of our trademarks.

Please refer to our Third Party copyright notices (http://www.checkpoint.com/3rd_party_copyright.html) for a list of relevant copyrights.
Enabling OPSEC .................................................................44

Provisioning Provider-1 ..........................................................46
Overview .............................................................................46
Provisioning Process Overview .............................................46
Setting Up Your Network Topology .......................................47
Creating a Primary MDS Manager .........................................47
Using the MDG for the First Time ........................................47
Launching the MDG .............................................................47
Adding Licenses using the MDG ............................................48
Multiple MDS Deployments ................................................50
Synchronizing Clocks ..........................................................50
Adding a New MDS or MLM ................................................50
Modifying an Existing MDS ................................................52
Deleting an MDS ...............................................................53
Protecting the Provider-1 Environment .................................53
Standalone Gateway/Security Management ...........................53
Provider-1 CMA and MDG Management ..............................53
Defining a Security Policy for the Gateway ..........................54
Enabling Connections Between Different Components of the System .......................................................54

Customer Management ..........................................................56
Overview .............................................................................56
Creating Customers: A Sample Deployment .........................57
Introduction to Creating Customers: A Sample Deployment ......57
Setup Considerations ..........................................................62
IP Allocation for CMAs ........................................................62
Assigning Groups ................................................................62
Management Plug-ins ........................................................63
Introducing Management Plug-ins .......................................63
Installing Plug-ins .............................................................63
Activating Plug-ins ............................................................63
Plug-in Status ......................................................................65
High Availability Mode .......................................................65
Plug-in Mismatches ............................................................65
Configuration ......................................................................66
Configuring a New Customer ...............................................66
Creating Administrator and Customer Groups ......................68
Changing Administrators .....................................................69
Modifying a Customer’s Configuration .................................69
Changing GUI Clients ........................................................70
Deleting a Customer ..........................................................70
Configuring a CMA .............................................................70
Starting or Stopping a CMA ................................................70
Checking CMA Status ........................................................71
Deleting a CMA ...............................................................71

Global Policy Management ......................................................72
Security Policies in Provider-1 .................................................72
Introduction to Security Policies in Provider-1 .........................72
The Need for Global Policies .................................................73
The Global Policy as a Template ...........................................74
Global Policies and the Global Rule Base ...............................74

Global SmartDashboard ..........................................................75
Introduction to Global SmartDashboard .................................75
Global Services ....................................................................75
Dynamic Objects and Dynamic Global Objects .......................76
Applying Global Rules to Gateways by Function .....................76
Synchronizing the Global Policy Database ..............................77
Creating a Global Policy through Global SmartDashboard ........78

Global IPS ............................................................................79
Introduction to Global IPS ....................................................79
IPS in Global SmartDashboard ......................................................... 80
IPS Profiles ................................................................................. 80
Subscribing Customers to IPS Service .......................................... 81
Managing IPS from a CMA ............................................................ 82
Assigning Global Policy ................................................................ 83
Assigning Global Policy for the First Time ................................. 83
Assigning Global Policies to VPN Communities ......................... 83
Re-assigning Global Policies ....................................................... 83
Viewing the Status of Global Policy Assignments ...................... 86
Global Policy History File ............................................................. 86
Configuration ............................................................................... 87
Assigning or Installing a Global Policy ........................................... 87
Reassigning/Installing a Global Policy on Customers ...................... 87
Reinstalling a Customer Policy on Customer Gateways ................. 88
Remove a Global Policy from Multiple Customers ....................... 89
Remove a Global Policy from a Single Customer ......................... 89
Viewing the Customer’s Global Policy History File ..................... 89
Global Policies Tab ...................................................................... 89
Global Names Format ................................................................... 90
Working in the Customer’s Network ............................................... 91
Overview ...................................................................................... 91
Customer Management Add-on (CMA) ......................................... 91
Administrators ............................................................................ 92
SmartConsole Client Applications ................................................. 92
Installing and Configuring Security Gateways ............................. 92
Managing Customer Policies ....................................................... 93
UTM-1 Edge Appliances ............................................................... 93
Creating Customer Policies ......................................................... 93
Revision Control ......................................................................... 94
Working with CMAs and CLMs in the MDG ................................. 94
VPN in Provider-1 ....................................................................... 95
Overview ...................................................................................... 95
Access Control at the Network Boundary ...................................... 96
Authentication Between Gateways ................................................ 96
How VPN Works ......................................................................... 96
VPN Connectivity in Provider-1 .................................................... 97
Connections to a Customer Network ............................................ 98
Global VPN Communities ............................................................ 100
Gateway Global Names ............................................................... 100
VPN Domains in Global VPN ..................................................... 101
Access Control at the Network Boundary ..................................... 101
Joining a Gateway to a Global VPN Community ......................... 101
Configuring Global VPN Communities ........................................ 102
Enabling a Customer Gateway to Join a Global VPN Community .... 102
High Availability ....................................................................... 104
Overview ...................................................................................... 104
CMA High Availability ............................................................... 104
Active Versus Standby ............................................................... 106
Setting up a Mirror CMA ............................................................ 106
CMA Backup using Security Management Server ....................... 107
MDS High Availability ............................................................... 108
MDS Mirror Site ......................................................................... 108
MDS Managers .......................................................................... 109
Setting up a New MDS and Initiating Synchronization ............... 109
MDS: Active or Standby .............................................................. 109
The MDS Manager's Databases .................................................. 110
The MDS Container's Databases .................................................. 110
How Synchronization Works ...................................................... 111
Setting up Synchronization ........................................................ 113
Check Point Registry .......................................................... 142
Automatic Start of MDS Processes, Files in /etc/rc3.d, /etc/init.d .......... 142
Processes ........................................................................ 142
  Environment Variables................................................... 142
  MDS Level Processes..................................................... 143
  CMA Level Processes.................................................... 143
MDS Configuration Databases ............................................. 144
  Global Policy Database.................................................. 144
  MDS Database .............................................................. 144
  CMA Database .............................................................. 144
Connectivity Between Different Processes .............................. 145
  MDS Connection to CMAs .............................................. 145
  Status Collection.......................................................... 145
  Collection of Changes in Objects ..................................... 145
  Connection Between MDSs ............................................. 146
  Large Scale Management Processes ................................. 146
  UTM-1 Edge Processes ............................................... 146
  Reporting Server Processes ......................................... 146
Issues Relating to Different Platforms ................................ 146
  High Availability Scenarios ......................................... 146
  Migration Between Platforms ....................................... 146

Commands and Utilities ..................................................... 148

Cross-CMA Search ............................................................ 148
  Overview.................................................................... 148
  Performing a Search .................................................... 148
  Copying Search Results .............................................. 149
  Performing a Search in CLI ......................................... 149
P1Shell ............................................................................ 150
  Overview.................................................................... 150
  Starting P1Shell .......................................................... 150
  File Constraints for P1Shell Commands .......................... 151
  P1Shell Commands ...................................................... 151
  Audit Logging............................................................... 154
Command Line Reference .................................................... 154
  cma_migrate.............................................................. 154
  CPperfmon - Solaris only ............................................. 154
  cpquerybin ................................................................ 160
  dbedit....................................................................... 161
  export_database ......................................................... 162
  mcd bin | scripts | conf ............................................. 163
  mds_backup ............................................................... 163
  mds_restore ............................................................... 164
  mds_user_expdate ...................................................... 164
  mdsccmd................................................................. 164
  mdsenv ................................................................. 171
  mdsquerydb ............................................................. 172
  mdsstart ................................................................. 172
  mdsstat ................................................................. 173
  mdsstop ................................................................. 173
  merge_plug-in_tables .................................................. 173
  migrate_assist ......................................................... 174
  migrate_global_policies ............................................ 174

Index ............................................................................. 177
Chapter 1

Introduction

In This Chapter

The Need for Provider-1 8
The Check Point Solution 12
The Management Model 21
The Provider-1 Trust Model 25

The Need for Provider-1

Secured IT systems are a basic need for modern business environments, and large deployments face unique security challenges. A large scale enterprise must handle the challenges of disparate yet interconnected systems. The large scale enterprise often has corporate security policies that must be tailored to local branch needs, balanced with vital requirement for corporate-wide access, perhaps between branches in different countries.

Businesses with a large user base often need to monitor and control access to confidential internal sites, and to monitor communication failures. Administrators must be alerted to external attacks, not only on a company-wide basis, but also more selectively on a department by department, branch by branch basis.

Companies with many branches must face security and access challenges that small scale businesses do not. For example, an international airline needs to provide access of varying levels to ticket agents, managers, airline staff, and customers, through the Internet, intranets both local and international, and through remote dial-up; all the while preventing unauthorized access to confidential financial data.

Differentiating between levels of access permissions is critical not only for securing user transactions, but also for monitoring for attacks, abuse and load management. Task specialization amongst administrators must also be supported so that security can be centralized.

Service providers such as Data Centers and Managed Service Providers (MSPs) need to securely manage large-scale systems with many different customers and access locations. An MSP must potentially handle separate customer systems with many different LANs, each with its own security policy needs. The MSP must be able to confidentially address the security and management needs for each customer, each with their own system topology and system products. One policy is not sufficient for the needs of so many different types of customers.

A Data Center provides data storage services to customers and must handle access and storage security for many different customers, whose requirements for private and secure access to their data are of critical importance.

We will examine a few basic scenarios: the MSP, the Data Center, and the large scale enterprise.

Management Service Providers (MSP)

An MSP manages IT services, such as security and accessibility, for other companies, saving these companies the cost of an expert internal IT staff. A management system must accommodate the MSP's own business needs, deploying an IT management architecture that scales to support a rapidly growing customer base, while minimizing support procedures and dedicated hardware.

The MSP handles many different customer systems, which creates a variety of IT management needs. Home users may require basic Internet services, with security managed by UTM-1 Edge appliances. Small companies may require Internet and customized-security coverage; others want autonomy to manage their own security policies. One small company wants to protect its computers with a single gateway, a Security...
Gateway, while another requires gateways and security services for several offices and multiple networks which must communicate securely and privately.

While the MSP must have administrators that can manage the entire MSP environment, administrators or individual customers must not have access to the environments of other customers.

Let’s examine the network of a fictitious MSP, SupportMSP:

**Figure 1-1** Example of an MSP environment

Service providers need a management tool designed to specifically address the unique challenges of large-scale private-customer management. These different and unconnected customers’ systems must be centrally managed, yet the MSP must also maintain the privacy and integrity of each customer’s system.

Further, the MSP must be able to flexibly manage security policies. Customers cannot all be assigned one security policy. It may be that specialized security policies suit a set of clients with similar needs (for example, supermarkets with many branches), whereas individualized policies better suit other customers (such as independent tax accountants and dentists). Repetitive policy changes and time-intensive end-user management are a common problem if policies cannot be managed adroitly.

The MSP must also handle communication and activity logging for network troubleshooting and reporting purposes. Comprehensive logging for many different customers and disparate systems can be process and space intensive, draining system resources if not handled carefully. This creates both administration issues and unique security policy requirements.
Data Centers

The data service provider is a type of service center, a company that provides computer data storage and related services, such as backup and archiving, for other companies. For example, let's examine the network of a fictitious Data Center:

Figure 1-2 Example of a Data Center

Similar to the MSP, the Data Center manages its own environment, whereas individual customer administrators and customers cannot have access to other customers' environments.

Large Enterprises

Businesses that expand through lateral and horizontal integration, such as conglomerates or holding companies, face security policy challenges due to the diverse nature of their subsidiaries' businesses. In these complex environments, security managers need the right tools to manage multiple policies efficiently. Central management of security policy changes, which are enforced by the different Security Gateways throughout the system, ensure that the entire corporate IT architecture is adequately protected.
Let's look at a sample deployment for an automotive manufacturing concern:

**Figure 1-3** Conglomerate's network

Corporate IT departments must manage security services for a wide-spread system, with link-ups with vendors, external inventory systems, billing inputs, and reporting requirements. Different branches are geographically distributed and have independent network management. Yet the network security personnel must support a corporate-wide security policy, with rules enforcing access for appropriate users, preventing attacks, enabling secure communication and failover capabilities.

IT departments must often delegate levels of authority among administrators, so that there is a hierarchy of access even within systems support. Whereas some administrators will have global authorities to maintain the system backbone, others may handle specialized activities and only require permissions for certain parts of the system. For example, an IT support person in a manufacturing branch would not necessarily need to have total administrator privileges for the logistics headquarters network, and a vendor administrator that handles network maintenance would not need corporate-wide permissions.

IT services in large scale enterprises must often log network activity for security tracking purposes. Comprehensive logging can consume considerable system resources and slow down a corporate network, if not deployed with an appropriate solution. For enterprises with local and remote branches, centralized failover security management is another critical success factor in achieving efficient and comprehensive system security.
For Big Bank, different types of permissions and access management are required to protect internal networks and separate them from external networks accessible to users.

**Figure 1-4** Big Bank’s network

---

**The Check Point Solution**

Check Point Provider-1 is the best-of-breed security management solution designed to meet the scalability requirements of service provider and large enterprise Network Operating Center environments. A unique three-tier, multi-policy management architecture and a host of Network Operating Center oriented features automate time-consuming repetitive tasks common in Network Operating Center environments. Provider-1 meets the needs of both the enterprise and of service providers serving the enterprise market. This solution dramatically reduces the administrative cost of managing large security deployments.

The basic three-tier security architecture of the Check Point Security Gateway system, consisting of a gateway, a management console, and a GUI, delivers a robust mechanism for creating Security Gateway security policies and automatically distributing them to multiple gateways. Provider-1 supports central management for many distinct security policies simultaneously.

Companies envision horizontal growth throughout an industry, to implement economies of scale through incorporation of partner-companies and vendors. Enterprises want to manage vertical growth through product differentiation. Security management achieves a new level of customization and flexibility with Provider-1.

With Provider-1, security policies can be customized. Enterprises can, for example, tailor a security policy to enable vendor applications which tie into corporate financial networks to communicate safely and securely, yet without having access to confidential corporate data. As another example, a security policy can enable franchise companies to communicate with regional and international headquarters, yet safeguard the franchise internal network integrity.

An administrator can create policies for groups of customer Security Gateways, and/or create high-level global policies that manage all customer policies at once. The ability to set policy at every level, including both the customer and global level, delivers exceptional scalability by eliminating the need to recreate policies and policy changes, potentially to thousands of devices.
Basic Elements

The Provider-1 system is designed to manage many widely distributed gateways, for networks that may belong to different customers, different companies, or different corporate branches.

The primary element of a security system is the gateway, the Security Gateway. Administrators decide how this Security Gateway is to be managed and apply a security policy, with rules that determine how communication is handled by the Security Gateway.

A Customer Management Add-On (CMA) is a virtual customer management. The CMA manages customer Security Gateways. Through the CMA, an administrator centrally creates and deploys policies on customer gateways.

Note - You may have noticed that the term Customer is capitalized in the preceding sentence. As a convention in this guide, the term Customer will appear as capitalized whenever referring to elements of the Provider-1 system.

The Multi-Domain Server (MDS) houses the CMAs, as well as all of the Provider-1 system information. It contains the details of the Provider-1 network, its administrators, and high level customer management information.

The MDS can hold a substantial amount of customer network and policy detail on a single server, providing a powerful, centralized management node. Multiple MDSs can be linked in the Provider-1 system to manage thousands of policies in a single environment, and to provide failover capabilities.

The CMA is the functional equivalent of a standalone Security Management server. But unlike the Security Management server, the CMA is a manager, located on the MDS. Although many CMAs can be stored on the same MDS, CMAs are completely isolated from each other, providing absolute customer privacy. In a large enterprise, each CMA may manage branch or department Security Gateways, depending on the security resolution required by the corporate security policy.

CMAs are located inside the Provider-1 environment. The Security Gateway can be located in a separate network, in a separate city or country.

Example: MSP Deployment

Let’s examine the basic system components at a less granular level, looking at a start-up MSP setup with Provider-1. The service provider, Provider, has an MDS and an internal network, connected to the Internet and protected by a Security Gateway. This service provider offers security services to two customers, and manages their Security Gateways.
Each customer has a Security Gateway protecting their respective internal corporate networks. Typing.com has one network with one Security Gateway. TravelAgency has two branches, each protected by its own Security Gateway. Each Customer has its own CMA, which resides in the service provider's MDS, inside the Provider-1 network environment.

Each CMA can manage more than one Security Gateway. TravelAgency has its own private CMA, which manages both of TravelAgency's Security Gateways. Typing.Com also has its own private CMA, which manages its Security Gateway. TravelAgency cannot access information about the Typing.Com environment, nor about the service provider’s environment.

Notice that Provider also has a CMA to manage its own Security Gateway.

**Figure 1-6** How CMAs manage Security Gateways

---

**Example: Enterprise Deployment**

Whereas a service provider manages individual customer networks, a large enterprise manages branches and departments. So, let's consider a Provider-1 setup for an international accountancy firm. The firm has its corporate headquarters in London, with one branch office in Minnesota, and another in Paris. Each of the branches has Security Gateways protecting internal corporate networks. Let us say that in this corporate environment, all security management is handled through the corporate headquarters in London.
How can this corporate system be protected? The branch offices are assigned CMAs to manage their gateways. In this case, the IT department is centralized in the corporate headquarters in London. An MDS has been created in London to manage the system. The Manchester corporate branch’s Security Gateway is handled by its own CMA. The Paris and Nice branches are both managed by another CMA. Although the MDS and the gateways themselves are in different cities and countries, management is centralized and handled by the IT department in the London office.

**Figure 1-7** Enterprise deployment

---

**Multi-Domain GUI**

Provider-1 administrators use the Multi-Domain GUI (MDG) as the primary interface to handle customer security management. The MDG has many "views" tailored to display information relevant to specific tasks.
The MDG manages the entire Provider-1 environment, and provides an easy way to incorporate customers and their networks into the Provider-1 system. It is used to update Customer and gateway information, and to assign and navigate between global policies. Using the MDG, administrators can provision and monitor security through a single console, and oversee rules, policies, logs, statuses, and alerts for hundreds of customers.

Point of Presence (POP) Network Environment

Some small scale businesses may not want the expense of a network or IT maintenance staff. MSPs can provide a total IT package for these customers, using the POP network solution to provide secured, Security Gateway protected Internet service. In the standard Provider-1 configuration we have seen, all of the customer's Security Gateways are deployed on the customer's premises. In a POP-based configuration, the Security Gateways are deployed in the POP center on the service provider's premises.

Leased lines to the POP service center provide secured Internet access for customers. All Provider-1 components, such as the MDS and the MDG (the administrative GUI), are located on the service provider's premises. Customers dial-in to receive services, and connect to the Internet via the POP center. Although their usage is monitored and protected, they do not have to be involved in any of the security management.

All aspects of security and access are completely maintained by the MSP, using CMAs on the MDS to manage the gateway in the POP center. The CMAs in the MDS do this by managing the security policies for the Security Gateways that protect customer access.

Figure 1-8  A simple model of a POP configuration
For some MSPs, using VSX technology to provide customer Security Gateways is a cost-saving solution. When setting up a POP site using VSX, individual security domains can be aggregated on a single platform, substantially minimizing hardware investment. Provider-1 has special features which enable CMAs to manage the security policies for the VSX virtual gateways, protecting customer sites from intrusion. For more information, see the VSX Administration Guide.

**Figure 1-9** POP center using VSX

Managers and Containers

There are two "types" of MDS: a Manager, which contains Provider-1 system information, and a Container, which holds the CMAs. The Manager is the entry point for administrators into the Provider-1 environment, via the MDG, the Provider-1 GUI.

Provider-1 can be installed on a single computer and configured as a combined Manager/Container. It can also be installed on multiple computers, where one MDS is a standalone Manager and another is a standalone Container. There must be at least one Manager and one Container per Provider-1 system.

In an environment where there are numerous Customers, it is recommended to use several Containers to "house" the CMAs. Each CMA does the following:

- Stores and manages its respective customer's Network Object database and Security Policies
- Receives status notifications and real-time monitoring data from the customer's gateways
- Receives logs from the customer's gateways, unless the logging properties of some or all of the gateways are configured otherwise

Housing too many CMAs on a single Container can lead to performance issues. See Hardware Requirements and Recommendations (on page 39) to calculate the proper balance. Using Containers, multiple MDSs can cascade to manage thousands of CMAs in a single environment.

Multiple administrators can simultaneously access the system via the MDG by connecting to the same, or different, MDS Managers. Administrators can access the entire Provider-1 system from each of the Managers, as all system information is stored on each Manager.
Let's look at a Provider-1 environment for a service provider that handles numerous small customers, and several large-scale customers.

**Figure 1-10** Multiple MDSs in the service provider environment

This service provider needs a robust system with many Containers to handle the large amount of information stored for all of its Customers. There are two MDS Managers in this system. One is housed as a standalone Manager, whereas the other is housed with a Container on the same server. There are also two other Containers, which are managed by the MDS Managers. Another computer runs the MDG, the Provider-1 graphical management tool. Administrators can login to any Manager, and see the entire system via the MDG.

**MDS Synchronization**

Manager synchronization (for Provider-1 system information) is performed at the MDS level. MDS Managers are "mirrors" of each other. If there is more than one MDS Manager in the system, each Manager will contain all the information regarding the Provider-1 management system such as administrator hierarchy, Customer and network information.

MDS Managers contain three databases: MDS, Global Policy and ICA. The MDS Manager's MDS database (general information) is synchronized whenever changes are made. The Global Policy database is synchronized either at configurable intervals and/or events, or it is synchronized manually. Interconnected, mutually redundant MDS Managers form a robust management system providing non-stop access, without the need to deploy dedicated hardware or software redundancy.
MDG management activities can be performed using any of the MDS Managers. MDS Manager synchronization does not mirror CMA-specific data. For example, internal domains and Customer level policy rules are known only at the CMA level, so they are not synced by MDS Managers. To enable CMA failover, you must set up CMA High Availability. CMA High Availability synchronization is separate from MDS synchronization.

**Figure 1-11**  MDS Synchronization in an Enterprise network

Log Managers

**Multi-Domain Log Module**

The Multi-Domain Log Module (MLM) is an optional server that is dedicated to log collection, separating critical management activities from logging traffic. It thereby provides the infrastructure for further data-mining activities and improves performance for large deployments by offloading log processing activities from the MDS. It is recommended for systems with many CMAs or a heavy logging load.

Redundant log infrastructures can be created by designating an MLM as a primary log server and the MDS as a backup. In the event that the MLM cannot be reached, logs are redirected to the MDS. It is possible to have multiple MLMs in the Provider-1 network. The MLM is controlled by the MDG, and maintains Customer Log Modules (CLMs), with a separate log repository for each Customer.
Let's look at Big Bank. Big Bank is expanding and has opened a number of new branches. It has decided to track activity in its system to satisfy security requirements. It has created an environment with three MDS's. The system administrators have set up an MDS Manager/Container with a second Container to manage Security Gateways throughout the different bank branches. They have also set up an MLM to track activity.

Figure 1-12  A simple system with an internal MLM

**Customer Log Module**

A Customer Log Module (CLM) is a log server for a *single* Customer. Service providers can deploy CLMs to monitor specific Customer modules. Enterprises may deploy CLMs to monitor branch activity.

In the example below, Big Bank uses a specific CLM to collect information about the Paris branch's gateway activities.

Figure 1-13  CLM gets activity data from customer's Security Gateway
High Availability

CMA High Availability

CMA High Availability is implemented by using two or more CMAs to manage one Customer network, one in Active mode, and the others in Standby. Implementing management High Availability guarantees failover capability. At any given time, only one CMA is Active, while the Standby CMAs are synchronized with the Active CMA.

Data synchronization between the CMAs greatly improves fault tolerance and enables the administrator to seamlessly activate a Standby CMA when required. With High Availability, should a CMA fail for any reason, a Standby CMA can continue operation without service interruption.

The High Availability scheme requires one Primary CMA and at least one Secondary CMA, which are housed separately, on different MDS computers. Administrators make security policy changes through the Active CMA. If policy changes are made with the Active CMA, the Standby CMAs can be set up to synchronize automatically to reflect these changes.

These CMAs must be synchronized in order to maintain the same information. It is possible to configure the High Availability feature to synchronize automatically for each policy installation operation, on each policy save operation and on any other scheduled event. If the Active CMA's data has not been synchronized with the Standby CMAs, you can still use the Standby CMAs, which are updated until the moment of the last synchronization.

Security Policies in Provider-1

Security Policies are created to enforce security rules. Administrators can create security policies and rules tailored to a specific Customer, or a type of Customer. In the Provider-1 environment, administrators create Customer security policies for a specific set of gateways, using the CMA, which is the equivalent of the Security Management server in the Check Point Security Gateway model. To find details about how a Security Gateway works with security policies, see the VPN and IPS Administration Guides.

The Need for Global Policies

Besides security policies for a specific set of gateways, administrators need to create policies which apply to the entire Provider-1 environment. The separation between different levels of policies, and different types of policies, means that Customer-level security rules do not need to be reproduced throughout the entire Provider-1 environment. Policies can be created and privately maintained for each Customer, ensuring a Customer's security integrity. Global Policies enforce security for the entire Provider-1 system.

The Management Model

Introduction to the Management Model

In the Provider-1 environment, the management model has been designed so that network security managers can centrally and securely manage many distributed systems. Network security is sharpened by differentiating between different levels of security needs, and differentiating between access privileges and needs. The Provider-1 management model allows you to designate trusted users (administrators) with different access rights. It enables trusted communication both within the Provider-1 network, and with customers' network environments.

Administrators

It is important, for security purposes, that there be different types of administrative authority. Administrators with authority over the entire system are needed in order to manage the entire Provider-1 system. But there also must be a level of administration authority which only applies to the customer environment and not to the Provider-1 system.

It is inappropriate for an administrator who remotely manages a Security Gateway in a particular customer network to have authority over or access to the entire Provider-1 system. This could be a serious security
breach, as a customer's internal staff would have access to other customer networks. For example, it would not be appropriate for an MSP to allow an administrator of one of its customers to have the authority to shut down an MDS Manager or delete all the superusers from the system.

In the Provider-1 environment, four types of administrators have been designated to handle different levels of responsibility. While there is a need for administrators with the authority to create and manage the entire Provider-1 environment, not every administrator in the system has this level of complete control. The following table shows permissions by type of administrator.

<table>
<thead>
<tr>
<th>Administrator</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Provider-1 Superuser</strong></td>
<td><strong>Provider-1 Superusers</strong> manage the entire Provider-1 system and can oversee all the networks of all Customers in the Provider-1 system. They can use all MDG tools relating to Customer and MDS management, and can manage all other administrators. <strong>Provider-1 Superusers</strong> have sole permission to manage and change the MDSs. They can:</td>
</tr>
<tr>
<td></td>
<td>• Add, edit or delete MDSs, including manager servers, containers, High-Availability servers, logging servers, etc.</td>
</tr>
<tr>
<td></td>
<td>• Enable or disable a computer's permission to access the MDG.</td>
</tr>
<tr>
<td><strong>Customer Superuser</strong></td>
<td><strong>Customer Superusers</strong> can manage the networks of all Customers in the system, using the MDG and SmartConsole tools. They can use all MDG tools relating to Customer management; create, edit and delete Customers; and see all the network objects for all of the Customers. <strong>Customer Superusers</strong> can manage <strong>Customer Managers</strong> and <strong>None</strong> Administrators. However, they cannot manage or change the MDS environment or manage <strong>Provider-1 Superusers</strong>.</td>
</tr>
<tr>
<td><strong>Global Manager</strong></td>
<td><strong>Global Managers</strong> can access Global SmartDashboard and, if so configured, manage Global Policies and Global Objects. <strong>Global Managers</strong> can also manage their assigned set of Customer networks from within the Provider-1 environment. They can:</td>
</tr>
<tr>
<td></td>
<td>• Access the General, Global Policies, High Availability and Connected Administrators Views.</td>
</tr>
<tr>
<td></td>
<td>• See and manage (add, edit and delete) the network objects of their Customers.</td>
</tr>
<tr>
<td></td>
<td>If <strong>Global Managers</strong> are assigned Read/Write/All permissions, they can:</td>
</tr>
<tr>
<td></td>
<td>• Edit their Customers.</td>
</tr>
<tr>
<td></td>
<td>• Add, edit and delete their Customer's CMAs and CLMs.</td>
</tr>
<tr>
<td></td>
<td>• Start or stop their Customer's CMAs and CLMs.</td>
</tr>
<tr>
<td></td>
<td>• Import their Customer's CMAs to another MDS.</td>
</tr>
<tr>
<td></td>
<td>• Create <strong>Customer Manager</strong> or <strong>None</strong> administrators for their Customers.</td>
</tr>
<tr>
<td></td>
<td><strong>Global Managers</strong> have fewer permissions than <strong>Customer Superusers</strong>:</td>
</tr>
<tr>
<td></td>
<td>• They cannot see the Network Objects of Customers to which they are not assigned.</td>
</tr>
<tr>
<td></td>
<td>• They cannot create new Customers.</td>
</tr>
<tr>
<td><strong>Customer Manager</strong></td>
<td><strong>Customer Managers</strong>, similar to <strong>Global Managers</strong>, can manage their assigned sets of Customer networks. However, they cannot access the Global SmartDashboard, meaning they cannot edit Global Objects or Global Policies.</td>
</tr>
<tr>
<td><strong>None</strong></td>
<td><strong>None</strong> administrators manage their Customers according to their assigned permissions. They are outside of the Provider-1 management environment. They manage their internal networks using the SmartConsole tools, e.g., SmartDashboard. They do not have access to the Provider-1 system, and cannot open an MDG.</td>
</tr>
</tbody>
</table>
Management Tools

**Multi-Domain GUI**

Administrators use the Multi-Domain GUI (MDG), the interface through which Provider-1 administrators handle Customer security management. The general view is shown below:

![Multi-Domain GUI](image)

Administrators use the MDG to manage the Provider-1 environment and monitor Customers’ networks. This tool provides an easy way to add Customers and their networks to the Provider-1 management system. Administrators can create, update, change and delete Customers, CMAs information; assign licenses; view and assign policy policies, which are stored centrally on the MDS. Through a single console, administrators can provision and monitor security, by assigning and overseeing rules, policies and logging setups, as well as monitoring logs, statuses, and alerts for hundreds of customers.

The MDG also is used to create administrators of all four types and assign their permissions. The MDG can even be used to designate which other computers can be entrusted to run the MDG. Administrators can create a logging setup by adding an MLM (Log Containers) to the Provider-1 management system, and designating a dedicated customer's server as a CLM for that customer. Further, it is possible to update Check Point software installed on all Provider-1 computers and Customer network computers using SmartUpdate, via the MDG.

From the MDG, an administrator can launch Global SmartDashboard to create Global Policies, or the administrator can launch SmartConsole Clients for each of the Customers. Outside of the Provider-1 environment, local administrators can also run SmartConsole Client applications for each of the Customers.

**SmartConsole Client Applications**

SmartConsole Clients are the Check Point tools used to design, manage, monitor and log the Security Gateway enforcement policies. SmartConsole Clients include all the following:

- **SmartDashboard** is used by the system administrator to define and manage the Security Policy. From this SmartConsole you can access many Check Point features and add-ons.

- **SmartView Tracker** is used for managing and tracking logs throughout the system.

- **SmartUpdate** is used to manage and maintain a license repository, as well as to facilitate upgrading Check Point software.

- **SecureClient Packaging Tool** is used to define user profiles for SecuRemote/SecureClient clients.

- **SmartView Monitor** is used to monitor and generate reports on traffic on interfaces, Provider-1 and QoS gateways, as well as on other Check Point System counters. It is also is used for managing, viewing alerts and testing the status of various Check Point components throughout the system.
- *SmartReporter* is used to generate reports for different aspects of network activity.
- *SmartProvisioning* is used for managing large numbers of SmartLSM Security Gateways via the Security Management server or Provider-1 CMA.

**Sample Deployment - Administrator Setups**

Let's examine a sample deployment, in which a service provider has an MDG console set up within the Provider-1 environment, and customers have their own consoles within their internal networks.

The service provider's **Provider-1 Superuser** administrator, Rosa, uses the installation CD and command line utilities to configure and set up the entire Provider-1 environment. Then, she uses the MDG and the Global SmartDashboard to manage the global policies. As a **Provider-1 Superuser**, Rosa is responsible for everything to do with the physical layout of the service provider's environment, and managing all the highest level security authorizations.

**Figure 1-14**  
Rosa sets up the Provider-1 environment

Rosa knows that her Provider-1 environment will run a large system, with hundreds of Customers, and it will not be possible for one administrator to handle all the activity. It is time to start considering staffing issues. **Customer Superusers** can handle all Customer specific management activities. They can create/delete/edit Customers and create edit or delete CMAs. Rosa authorizes Martin to be a **Customer Superuser**. Now Martin can add customers to the system.

**Figure 1-15**  
Martin adds customers to the Provider-1 environment

Martin starts adding customers into the system. Each customer needs a security policy to monitor the customer network's gateway, the Security Gateway. The work is really piling up! Now that the customer base is expanding, it is time for Martin, as a **Customer Superuser**, to add more customer administrators.
Martin authorizes Tony to be a **Customer Manager** for the customers Accountant and Pharmacy2Go. **Customer Managers** can handle many Customer specific management activities. They can add, edit or delete their Customer's CMAs. They can start or stop their Customer's CMAs and CLMs. They can also import their Customer's CMAs to another server, and create customer security rules. It's time for Tony to create security policies for Pharmacy2Go and for Accountant.

**Figure 1-16**  Tony creates security rules for customers

The company Pharmacy2Go has a resident IT manager, Sandrine, who handles local network maintenance and security. Tony works with Sandrine to ensure that Pharmacy2Go's network is running securely and safely.

As a **Customer Manager**, Tony can authorize **None** administrators, who are outside of the Provider-1 management environment, but may administer customer Security Gateways themselves. Tony adds Sandrine to the list of administrators as a **None** administrator, so that she can use SmartConsole applications to monitor and track activity in Pharmacy2Go's network.

Sandrine can run SmartConsole Client applications for Pharmacy2Go’s network, now that she has been made a **None** administrator. Remember, **None** administrators manage their own internal networks via the CMA. They do not have access to other elements in the Provider-1 environment.

Notice that the Provider-1 network itself needs to maintain its own security, protecting the confidentially of critical information regarding customer networks, administrators, and access details, as well as for its own network! It can use a stand-alone Security Gateway, or define a CMA to manage its gateway. If the gateway is standalone, Rosa can manage it through its own Security Management server. If maintained by the MDS, it is managed with a CMA.

---

**The Provider-1 Trust Model**

**Introduction to the Trust Model**

The Provider-1 system provides a method for MDSs and CMAs to establish secure, trusted and private communication between Check Point gateways while ensuring data integrity. This is a critical component in ensuring that system management commands and system information are delivered securely.

Provider-1 systems must establish safe process communication between MDSs, between MDSs and CMAs, between CMAs and the Customers' Gateways that they are managing, and between administrators and CMAs. To ensure secure and private communication, Secure Internal Communication is used.
Secure Internal Communication (SIC)

Secure Internal Communication (SIC) is used to establish trust between each of the computers and components in the Provider-1 system that must communicate with each other. A basic explanation of how SIC works appears in the Security Management Administration Guide.

Safe communication ensures that the system can receive all the necessary information it needs to run correctly. Although information must be allowed to pass freely, it also has to pass securely. This means that all communication must be encrypted so that an imposter cannot send, receive or intercept communication meant for someone else, be authenticated, so there can be no doubt as to the identity of the communicating peers, and have data integrity, not have been altered or distorted in any way. Of course, it is helpful if it is also user-friendly.

The SIC model incorporates PKI. Certificates are issued to trusted communicating parties by an Internal Certificate Authority. These certificates are then used to authenticate every communication established between the communicating parties.

The following security measures are taken to ensure the safety of SIC:

- Certificates for authentication.
- Standards-based SSL for the creation of the secure channel.
- 3DES for encryption.

Trust Between a CMA and its Customer Network

In order to ensure authenticated communication between the Provider-1 environment and the Customer network environment, each CMA also has its own Internal Certificate Authority (ICA), which is responsible for issuing certificates to the CMA's Customer gateways. The CMA ICA is part of the CMA data residing in the MDS Container. Each CMA ICA is associated with a specific Customer. A Customer's secondary CMA shares the same Internal Certificate Authority as the primary CMA.

The ICA of each CMA issues a certificate to Security Gateways in the Customer network. SIC can then be established between the CMA and each of its Customer's Security Gateways.
Different CMAs have different ICAs to ensure that a CMA establishes secure communication with its own Customer's gateways, but that different Customer CMAs cannot penetrate each other's internal networks and establish communication with another Customer's gateways.

**Figure 1-17** SIC between CMA and Customer gateway

**Trust Between a CLM and its Customer Network**

The CLM (Customer Log Manager) also receives a certificate from the CMA's ICA. This is so that the Customer's Security Gateways can establish communication with the CLM, for tracking and logging purposes. The gateways and CLM must be able to trust their communication with each other, but only if they belong to the same customer. Otherwise, different customers could monitor each other, which would be a security breach.

**MDS Communication with CMAs**

Every MDS Container communicates with the CMAs that it houses locally and securely through a protocol called SIC local. This type of authentication, SIC local, is managed by the Provider-1 environment and allows internal MDS communication to be trusted.

SIC is used for remote (not on the same host) communication, whereas SIC local is used for a host's internal communication. SIC local communication does not make use of certificates.
Trust Between MDS to MDS

The primary MDS Manager, the first Manager created, has its own Internal Certificate Authority. This ICA issues certificates to all other MDSs, so that trusted communication can be authenticated and secure between MDSs. All MDSs share one Internal Certificate Authority.

Figure 1-18  SIC between MDSs

The ICA creates certificates for all other MDSs, and for Provider-1 administrators. Administrators also need to establish trusted communication with the MDSs.

Authenticate the Administrator

Administrators are authenticated to access the MDS via the MDG either by using a User Name and Password combination (which is considered only semi-secure) or by using a certificate issued by the MDS ICA (far more secure).

Figure 1-19  SIC between Administrator and MDS

For management purposes, administrators use the certificates provided by the MDS ICA to establish trusted communication to manage the CMAs. This is because every CMA also trusts the MDS ICA for administrator management activities using a communication medium, CPMI. This means that administrators do not need to have certificates issued to them for every CMA that they communicate with.

Figure 1-20  SIC between administrators and a customer CMA
Authenticating via External Authentication Servers

Provider-1 supports authentication using an external server that contains a database of user login information (for example, user name, password and attributes). When a Provider-1 administrator is set to authenticate using one of these external servers, all authentication requests are forwarded to the authentication server. The external server authenticates and authorizes the user and sends a reply to the MDS. Only if the administrator is authenticated and verified will the MDS allow the administrator to connect to the MDS or the CMA.

Provider-1 supports the following external authentication servers:

- RADIUS
- TACACS
- RSA SecurID ACE/Server

The following diagram depicts an authentication process in which administrators use external authentication:

Figure 1-21 Authentication using an External Authentication server

TACACS and RADIUS authentication methods, when authenticating an administrator connecting to a CMA, use the MDS as a proxy between the CMA and the external authentication server. Therefore, each MDS container should be defined on the authentication server, and the authentication server should be defined in the global database. In addition, if the MDS is down, the CMA will not be able to authenticate administrators.

Setting up External Authentication

To set up External Authentication:

To authenticate using an authentication server, the MDS must know which administrators should be authenticated. Administrator authentication is performed through the MDG as follows:

1. Open MDG > Administrators.
2. Create a new administrator.
3. In the General tab, enter the same user name that was created on the authentication server.
4. Mark the administrator’s permission.
5. On the Authentication tab, select the Authentication Scheme. If using RADIUS or TACACS, choose the appropriate server that was configured in Global SmartDashboard.
6. If using SecurID, do the following:
   a) Generate the file sdconf.rec on the ACE/Server, and configure the user to use Tokencode only.
   b) Copy sdconf.rec to /var/ace/ on each MDS.
   c) Edit the file /etc/services and add the following lines:
      
      securid 5500/udp
securidprop 5510/tcp

d) Reboot the MDS machines.

Alternatively, instructions 3, 4, and 5 can be performed from the command line interface (CLI) with the following syntax:

```
mdscmd setadminauth <administrator name>
<undefined | os | fw1 | securid | tacacs | radius> [authentication server name]
[-m mds -u user -p password]
```

Re-authenticating when using SmartConsole Clients

When a SmartConsole Client is launched from another open SmartConsole Client, the system by default reapplies the credentials entered when the administrator logged into the first Client.

However, there are cases where it is useful to compel administrators to re-authenticate for each SmartConsole Client they launch. When using RSA SecurID to authenticate Provider-1 administrators, for instance, it is common to require re-authentication when SmartConsole Clients connect to MDSs or CMAs.

You can compel administrators to re-authenticate every time a new GUI client is launched and connects to:

- a specific CMA
- all CMAs created on this system in the future
- this MDS or MLM

The instructions for each are listed below.

...When Connecting to a Specific CMA

The following commands need to be executed in a root shell on the MDS machine hosting the CMA:

```
dbedit -s <CMA IP> -u <name of administrator with edit permissions for this CMA> -p < administrator password>
modify properties firewall_properties fwm_ticket_ttl 0
update properties firewall_properties
quit
```

If the relevant Customer has more than one CMA, synchronize the CMAs for the change to take effect on both. If the Customer owns one or more CLMs, the Install Database operation should be performed on each CLM for the change to take effect.

...When Connecting to all CMAs Created on This System in the Future

The following steps need to be executed in a root shell of every MDS Container machine:

Run the command mdsenv.

Edit the file $MDS_TEMPLATE/conf/objects_5_0.C

Find the line containing: fwm_ticket_ttl

Replace it with the line: fwm_ticket_ttl (0)

...When Connecting to this MDS or MLM

The following commands need to be executed in a root shell on the MDS machine hosting the CMA:

```
dbedit -s <IP of the MDS or MLM> -u <name of the administrator with edit permissions for the Global Policy of the MDS> -p <password of the administrator>
modify properties firewall_properties fwm_ticket_ttl 0
update properties firewall_properties
quit
```
If the Provider-1 configuration consists of more than one MDS Container server or MLM, synchronize the Global Policy for the change to take effect on all MDS Container servers or MLMs.

**CPMI Protocol**

The CPMI (Check Point Management Interface) protocol is a generic open protocol that allows third party vendors to interoperate with Check Point management products. The client side of CPMI is included in the OPSEC SDK documentation, so third-party products can integrate with the CMAs. For more information on CPMI, see the *CPMI* guide in the OPSEC SDK documentation.
Chapter 2

Planning the Provider-1 Environment

This chapter deals with different aspects required in order to plan and prepare for setting a first time deployment with Provider-1. In every first time setup there are general questions that you need to ask yourself, such as

- What do you need to know about the basic components that need to be installed?
- How should the basic components be deployed and in what order should they be installed?
- What are the hardware requirements that need to be considered?
- What licenses need to be obtained in order to run the product?
- What are other additional requirements that may influence the performance, strength or security of the environment?

In this chapter, we will deal with many of the questions that you need to consider when planning your Provider-1 environment.

In This Chapter

- Asking yourself the right questions
- Consider the Following Scenario
- Protecting Provider-1 Networks
- MDS Managers and Containers
- Setting up the Provider-1 Environment
- Hardware Requirements and Recommendations
- Provider-1 Order of Installation
- Licensing and Deployment
- Miscellaneous Issues

Asking yourself the right questions...

There are many factors to consider when planning your Provider-1 environment. This section discusses a few of these issues in general terms. Specific details are discussed at a later stage.

Safety comes first

Whatever deployment you choose to implement, first and foremost, must protect your networks. You must also install an <tp_sgate > to protect the Provider-1 environment itself. For more information, see Protecting Provider-1 Networks (on page 34).

MDS Managers & Containers - How Many Do You Need?

Every Provider-1 management network requires at least one MDS Manager (where Provider-1 system information is stored and MDG clients can connect to it to monitor and control the Provider-1 system), and one MDS Container (where CMA/CLM data is stored per Customer,) and more important, The MDS Manager and MDS Container can be installed together on one computer.

Take note that the greater your Customer base the more Containers will be necessary in the system to support the database load for these Customers. For more information, see MDS Managers and Containers (on page 35).
Choosing the Right Environment

Choose the deployment that best suits your need, amongst the options you can deploy a standalone or a distributed environment. For more information, see Setting up the Provider-1 Environment (on page 36).

Choosing the Right Platform

- When choosing between a Linux or SecurePlatform Operating System, remember that all the MDSs in the system must all be of the same platform.
- The Provider-1 MDG runs only on Windows platforms.

High Availability

If you are supporting many complex Customer networks, you may decide to implement failover/recovery capabilities:

- For CMA High Availability, you need at least two container MDSs. By creating two or more containers, you then create two or more CMAs for each Customer. These CMAs serve as Active and Standby Management servers for the customer gateways.
- For MDS High Availability, where there are multiple entry points to the system, you need at least two Manager MDSs in order ensure MDG access even when one of the manager MDSs is not available.

Logging & Tracking

If you decide to implement logging for tracking and troubleshooting purposes, for a very large system where many different services and activities are being tracked, it is recommended that you have one or more dedicated log servers (MLM).

Migrating in a Standalone Environment

If you want to migrate standalone Security Management server management components into Provider-1 CMAs, ensure that you are thoroughly acquainted with the procedure. Before you begin, consult the Upgrade Guide. Choose a method and ensure a setup that supports your migration strategy.

Routing Issues in a Distributed Environment

If you have a distributed system, with MDS servers located remotely, ensure that you have considered routing issues. Routing must enable all MDS components of the Provider-1 system to communicate with each other, and for CMAs to communicate with Customer networks. For more information, see IP Allocation & Routing (on page 43).

Platform & Performance Issues

Check Provider-1 system hardware and platform requirements, and ensure that you have the needed platform patches installed. If you have an MDS with multiple interfaces, ensure that the total load for each MDS computer conforms to performance load recommendations. For more information, see Hardware Requirements and Recommendations (on page 39).

Setting Up Administrators

Consider which computers administrators will manage the system, and the administration hierarchy that you want to establish.

Licensing

Once you have determined what sort of server/computer configuration you need, you will want to ensure that you have the appropriate licenses. For more information, see Licensing and Deployment (on page 40).

Consider the Following Scenario...

The following scenario outlines a typical example of the basic components and features that can be implemented that need to be taken into consideration when planning.

Environment: Distributed with High Availability
Consider the following: a medical supplies firm has several branch locations, and requires failover capabilities. MDSs are installed in three branches: Kansas, Osaka, and Montenegro. Each MDS has a mix of primary and secondary CMAs.

**Security: Security Gateway**

Critical to comprehensive security, each MDS is protected by a Security Gateway. This gateway should be managed by a CMA or by a standalone Security Management server.

The gateway must have a security policy that adequately protects the network and which allows secure communication between Provider-1 components and external customer networks.

The gateway must have security rules that allow CMAs to communicate with customer gateways, and that allow external customer administrators to access CMAs.

---

**Requirement: Logging and Tracking**

Most enterprise systems and MSPs require event logging and tracking. Accountability requirements can lead to sizable log maintenance. By default, logs will be stored on the Customer's CMA that manages the gateway which is generating the logs in the Provider-1 management network. For most systems, in terms of licensing, it is more cost-effective to dedicate an MLM server to store logs rather than purchase extra Managers for this purpose. It is recommended that you implement one or more dedicated log servers (MLMs), depending on the activity tracking load in the system Provider-1 manages.

For more information about logging, see Logging in Provider-1 (on page 119).

**Requirement: GUI Clients & their Platforms**

Finally, consider the platforms that will be used to run the GUI tools used to manage the Provider-1 and Customer environments. The Provider-1 system is monitored using the MDG and SmartConsole Client applications. GUI Clients should be deployed either inside or outside of the Provider-1 network to enable administrators to access the Provider-1 system. The MDG runs only on Windows platforms but supports MDS's and their CMAs on any supported platform.

**Requirement: Routing & Communication**

If GUI Clients are located outside of the Provider-1 network, communication between these computers and the MDS Manager(s) must be allowed. If MDSs are in different remote locations, and there is more than one Provider-1 network, communication between the remote MDSs and the local MDSs must be allowed. Also ensure appropriate routing to support communication between computers and servers.

---

**Protecting Provider-1 Networks**

No matter how you deploy your Provider-1 environment, each Network Operation Center (NOC) must be protected by a Security Gateway. This gateway is managed either by a CMA or by a standalone Security Management server.

This gateway must have a security policy that adequately protects the NOC and which allows secure communication between Provider-1 components and external customer networks. This is essential to ensure continued open communication between all the components, enabling MDSs to communicate with
each other, and management servers (CMAs, CLMs, CMA-HAs) to communicate with customer networks. It must support proper routing. At the same time while the lines of communication must be open and free, they must also be secure.

The gateway must have security rules that allow CMAs to communicate with customer gateways, and that allow external customer administrators to access CMAs.

# MDS Managers and Containers

Every Provider-1 environment requires at least one MDS Manager and one MDS Container. Beyond the minimum requirements, to determine how many MDSs your environment requires, consider the functionality of the different types of MDSs.

## MDS Managers

Use the MDG to connect to the MDS Managers in order to monitor and control the Provider-1 environment. If more than one MDS Manager is deployed:

- They can provide mutually redundant failover capabilities.
- They can be configured to synchronize global policy data either automatically or manually.

## MDS Containers

MDS Containers contain and manage Customer data such as the Customer’s network objects’ database and security policies. This data is private (per Customer) and therefore it is not shared. Consider the following:

- MDS Containers and High Availability (on page 35)
- MDS Containers and Performance Issues (on page 35)

## MDS Containers and High Availability

Customer data can only be maintained in a redundancy scenario, that is, if High Availability has been enabled for the Customer. This is called CMA-High Availability, or CMA-HA. Data sharing is on a Customer by Customer basis, and is synchronized between the CMA and CMA-HA. At least two Containers are required for CMA High Availability because the Customer's CMA-HA must be set up on a different Container than the CMA (see High Availability (on page 104)). The Customer's Primary CMA should reside on one Container and each Secondary CMA should reside on another.

## MDS Containers and Performance Issues

The Container load depends on the complexity of the Customer’s policies and setups. Multiple Containers can cascade to manage thousands of CMAs in a single environment. In general, to support numerous Customers who have complex networks, it is advisable to deploy several Containers, since a Container with an overload of CMAs can suffer performance-wise.

# Choosing your deployment for MDS Managers and Containers

You can set up your MDS Managers and Containers in Mirror Sites, or in a Distributed Environment.

## Setting up MDS Managers and Containers in Mirror Sites

Service providers usually need a robust system with many Containers to handle the large amount of data and rules used to manage their customers’ networks. An MSP may implement a remote mirror site for disaster recovery. For example, an MSP can create a Provider-1 management network containing a Manager, with several Containers housing Customers’ CMAs. The MSP can also maintain a mirror site in another city, comprising of a secondary Manager, with several Containers storing CMA-HAs.
**MDS Managers and Containers in a Distributed Environment**

An enterprise system can centralize the Provider-1 management network at one branch yet have one or more backup MDSs at other locations. (For more information about failover options, see High Availability (on page 104).)

For example, a corporate bank with several international branches locates the "primary" Provider-1 management network in their headquarters. But, to support Active CMAs for the different local branches, they maintain an MDS Container per region, at a central regional branch. The CMA-HAs can be maintained for failover capabilities in the Provider-1 management network MDSs in the headquarters, or distributed to the local MDS Containers. If a central regional branch contains an MDS Manager as well, the whole MDS environment can be accessed by connecting the MDG GUI client to that server.

![CMA High Availability in an Enterprise Network](image)

**MDS Clock Synchronization**

For MDSs to be able to properly synchronize, all MDSs' system clocks must be synchronized. If there is more than one MDS computer in the system, before installing any new MDS, first synchronize the computer clock with other MDSs in the system.

The time of modification is written using UTC (Coordinated Universal Time), used by MDSs' system clocks. Synchronize MDS clocks using any synchronization utility. It is recommended that you reset regularly to compensate for clock drift. Correct database operation requires that the MDS clocks are synchronized to the second. It is recommended that MDS clocks be synchronized automatically at least once a day.

**Setting up the Provider-1 Environment**

The Provider-1 topology depends on system and business requirements. A number of simplified basic scenarios for enterprises are discussed in this section. Provider-1 is designed to flexibly support many different types of management network and customer network configurations. These include:

- A Typical Scenario (on page 37)
- A Standalone Provider-1 Network (on page 37)
- A Distributed Provider-1 Network (on page 38)
- Provider-1 Network with Point of Presence (POP) Center (on page 38)
A Typical Scenario

Enterprises usually choose to put the Provider-1 management network in its own segment, separated from the main enterprise network by a gateway.

Figure 2-24 Separate and Protect Network Segments

Provider-1 servers are often separated from support servers such as Radius, LDAP, and anti-virus servers. This is not by any means a requirement.

Figure 2-25 Separate Support Segments

A Standalone Provider-1 Network

The Provider-1 management system can be set up in one network location, with all the MDSs located in the same local network. Failover capabilities are enabled by having at least two Manager/Container MDSs. Management and maintenance are centralized through the Provider-1 network segment. The advantage of this setup is that routing complexity is considerably reduced.
Logs can be stored centrally on the MLM server (per Customer in different CLMs) and accessed via SmartView Tracker.

**Figure 2-26** Separate Provider-1 Segment with Remote Logging

A Distributed Provider-1 Network

The Provider-1 management system can be distributed over different geographical locations to provide disaster recovery capabilities and to minimize the overhead of logging traffic. In such a deployment, MDS managers and containers exist on both the local network and other remote networks. An MLM may also be set up at a remote location as a way of "outsourcing" logging traffic. Routing must ensure that local and remote MDSs can communicate with each other to maintain MDS synchronization. Each Provider-1 network segment must have adequate protection, by a Security Gateway.

**Figure 2-27** Separate Provider-1 Segments for Disaster Recovery/Logging

Provider-1 Network with Point of Presence (POP) Center

Provider-1 can be configured to manage a POP center which allows branch offices to receive service and secured Internet access via leased lines to the POP service center. All Provider-1 components, such as the MDS and the MDG (the management console), are located in one network location. Customers or corporate users dial-in to receive services, and connect to the Internet via the POP center.
Usage is monitored and protected via the Provider-1 management network, and branches do not have to be involved in any of the security management. All aspects of security and access are completely maintained using CMAs on the MDS to manage the gateway in the POP center. The CMAs in the MDS do this by managing the security policies for the Security Gateways in the POP center.

Figure 2-28  A Simple Model of a POP Configuration

Hardware Requirements and Recommendations

The Provider-1 disk space requirements are as follows:

- For basic MDS installation: 800MB.
- For each CMA: 50MB for the CMA directory.

When considering disk space, it is recommended to use volume management software.

Provider-1 Order of Installation

For each MDS component's setup to be stable and workable, it is important to conduct setup/installation in the following order:

1. Install the Operating System (OS).
2. Conduct OS hardening. It is advisable to remove unnecessary applications, scripts or libraries that are not needed as they are not necessarily secure. It is advisable to limit resident libraries and applications to those needed for system functionality.
3. Install the OS patches.
4. Install Check Point products.
5. Install Check Point patches.
6. Install Check Point hotfixes.

The appropriate OS patches, and the Provider-1 installation procedure are discussed in Provisioning Provider-1 (on page 46).
Licensing and Deployment

The Trial Period

All purchased Check Point products have a 15 day trial period. During this period the software is fully functional and all features are available without a license. After that period, a permanent license must be installed in order to continue using the software. Alternatively, an evaluation license must be obtained.

The starting point of this trial period is defined differently for different products. The Provider-1 trial period begins as soon as the MDS is installed (regardless of its type). The trial license is for an MDS Manager maintaining up to 200 CMAs. Each CMA you create during the trial period receives its own trial license for a Primary CMA managing an unlimited number of gateways. The license supports the Check Point SmartUpdate & SmartMap features and expires on the same day as the MDS's trial license.

Considerations

Provider-1 Components Installed at the NOC

The following components are deployed at the Network Operation Center:

- Multi Domain GUIs (MDG)
- Multi Domain Servers (MDS), including Multi Customer Log Modules (MLM)
- Customer Management Add-on (CMA)
- Customer Log Module (CLM)

Selecting MDS and CMA Licenses

Similar MDS components must be installed on different computers. Two Managers cannot share the same computer. Each Container must also be on a separate computer. However, a Manager/Container combination can be housed on the same computer. Licenses are available separately or combined for the MDS components.

When considering which licenses to buy, a second MDS Manager is recommended for disaster recovery. A standalone MDS Manager is available to be used for management purposes only, serving as an entry point to the system.

If many CMAs will be supported by the system, or if the CMA load increases, more MDS Containers are needed, not Managers. CMAs are maintained only on Containers. Licenses for MLMs (dedicated log servers) are inexpensive, so they are a cost effective alternative to storing logs by default on Managers/Containers.

The MDS license is per IP, and is based on the following factors:

- The MDS type, whether Manager, Container, combined, or Log Manager (MLM).
- For Containers, the MDS license depends on the number of CMAs managed.

Provider-1's licensing is geared to match its scalable architecture. Licenses are matched to needs, and can be purchased to accommodate a growing Customer base. Components are licensed according to the number of CMAs and Security Gateways. New CMAs can be seamlessly integrated, by upgrading to a larger license.

Each CMA requires its own CMA-level license. These are obtained per CMA's IP address. The exceptions to this are the VSX Bundle license (see VSX Bundle License on page 42)). Pro Add-ons for multiple CMAs are purchased in a bundled product, called Pro Add-ons for MDS. The way to generate the CMA Pro Add-on licenses in UserCenter is as follows: Perform the "Activate License" operation on the bundled product, using the IP address of the first CMA, to generate the license for this CMA. For each additional CMA, perform the "Change IP" operation on the bundled product, and change to the IP address of this CMA.

Install the generated licenses at the respective CMA level.

The MLM license is comprehensive so there is no need for separate licenses per CLM. A single license installed on the MLM applies to both the MLM and the CLMs it maintains. CLMs are per Customer and can
receive logs from all of the Customer's gateways, regardless of their number. The number of gateways that report to the same MLM is unlimited.

The MDG does not require a license.

**Provider-1 Enterprise Edition**

Provider-1 supports the new licenses for Provider-1 Enterprise Edition Products. The new licenses enable an MDS with 3 or 5 CMAs (depends on the license purchased). Each CMA has a Pro license level and can manage an unlimited number of gateways.

**Managing Licenses**

Provider-1 uses SmartUpdate to incorporate newer versions and licenses. Required components and licenses can easily be upgraded using the SmartUpdate view in the MDG.

Licenses are additive. For example, an MDS Container license for 50 CMAs and an MDS Container license for 25 CMAs add up to 75 hosted CMAs.

**Further Licensing Detail**

**Licensing the Multi-Domain Server (MDS)**

There are two basic MDS components: Containers and Manager. Containers hold CMAs, whereas Managers manage the Provider-1 environment and provide entry points for the MDG GUI Clients.

**Multi-Customer Log Module (MLM) Licenses**

An MLM is installed as a Container. In order to simplify the deployment process, a single license installed on the MLM applies to both the MLM and the CLMs it maintains. A customer's CLM can receive logs from all of the customer's gateways, regardless of how many there are. See Logging in Provider-1 (on page 119) for more details.

**Customer Management Add-on (CMA) Licenses**

The CMA is a Check Point Security Management Server. Each CMA manages a single customer's network and requires a dedicated CMA license. While each CMA belongs to a single Customer, each Customer can have up to multiple CMAs, for High Availability purposes. Each CMA must be maintained on a different MDS.

CMAs are licensed according to the number of gateways they manage. There are four levels of CMA licenses to enable scalable, cost effective deployment:

- **CMA-1** — suitable for a Customer with one gateway.
- **CMA-2** — suitable for a Customer with up to two gateways.
- **CMA-4** — suitable for a Customer with up to four gateways.
- **CMA-U** — suitable for a Customer with an unlimited number of gateways.

You do not have to install additional software when you create a CMA in the Provider-1 network. To add a new CMA, you only need add the CMA's license, which is ordered per CMA IP. The number of QoS gateways managed by a CMA is unlimited and requires no special license.

The CMA manages any of the following:

- Security Gateways on a variety of platforms (Linux, Nokia, AIX, HP, NT, Win2K)
- UTM-1 Edge Gateways
- Bay Networks devices
Customer Log Module (CLM) Licenses

If you want to host a CLM on a non-MLM MDS, you must install a CLM license. There is no limit to the number of CLMs that can be defined for a single Provider-1 Customer; however, each CLM must be created on a separate MDS.

Gateway Licenses

A Customer's gateways require licenses. Gateways are licensed according to the number of nodes at a site. A node is any computing device with an IP address connected to the protected network. Provider-1 also supports Quality of Service (QoS) gateways.

VSX Bundle License

The VSX Bundle License provides licensing for managing VSs and CMAs, located on an MDS server. The bundle license is installed on the MDS server and permits a specific number of VSs to be managed. The number of CMAs that can be defined on an MDS equals the number of VSs permitted plus one. The additional CMA is used for the CMA with VSX Box. The VSX bundle, however, does not limit the number of Virtual Systems or Virtual Routers.

CMAs without a CMA-level license use the bundle license. If a CMA-level license is installed on a specific CMA to allow the management of a regular gateway, then that CMA stops using the bundle license, and the VSs located on it are not counted off the bundle license. When a CMA is managing a non-VSX gateway, both a CMA-level license and container license on the MDS is required.

VSX Bundle License for HA CMAs

The VSX HA CMA Bundle License is used for HA CMAs on a primary or backup MDS for High Availability. HA CMAs can use the regular bundle, but Primary CMAs cannot use the HA bundle.

License Violations

When a license violation is detected, syslog messages are sent, pop-up alerts in the MDG, and audit entries in the SmartView Tracker stating the nature of the violation, are generated. In addition, an indication about the license violation appears on the status bar of the MDG.

While the MDS is in violation, new CMAs, Virtual Systems, VSs or Virtual routers cannot be added to the MDS.

Replacing the Trial Period License

After the trial period expires, a permanent license must be installed. Before installing a new license, make sure the amount of CMAs and VSs do not exceed the amount permitted by the new license. Installing a new license that allows less CMAs or VSs than were configured during the trial period is a violation. As a result, the MDS will not start.

During the trial license, up to 200 CMAs and up to five VSs per CMA are permitted to be configured. In order to configure more than five VSs per CMA, a bundle license or CMA-level license would need to be installed. In order to successfully install a bundle license before the trial license expires, the trial license must be disabled from the CMA. The command for disabling the trial period license on a CMA before the license expires is:

cpprod_util CPPROD_SetPnPDisable 1

This command needs to be executed on each CMA separately and will only take effect after restarting the CMA.

The license violation mechanism is enforced separately for each MDS meaning that if one MDS is in license violation, the other MDSs will continue to function.
Installing the VSX Bundle License

Installing the VSX Bundle license is similar to installing any other MDS level license. The installation can take place on the MDG from the MDS properties view or from the command line, using the "cplic put" command.

Miscellaneous Issues

IP Allocation & Routing

Provider-1 uses a single public IP interface address to implement many private "virtual" addresses. The MDS Container uses virtual IPs to provide CMAs, CMA-HAs and CLMs, which reside on a Container, with IP addresses.

Each MDS Container has an interface with an IP address, which is routable. Behind the interface's IP address the CMAs have a range of virtual IP addresses, which must be routable as well in order for the gateways and the SmartConsole clients to be able to connect to the CMAs. It is possible to use either public or private IPs.

When setting up route tables, ensure that you enable the following communication paths:

- The Customer's gateways to the Customer's CLM(s).
- A Customer's CMA to CLM(s).
- A Customer's CMA to CMA-HA.
- A CMA-HA to CMA.
- The CMA and CMA-HA to the Customer's gateways.
- The Customer's gateways to the CMA and CMA-HA.

Virtual IP Limitations and Multiple Interfaces on an MDS

There is a limitation of 250 Virtual IPs per interface for Solaris-platform MDS Containers. As each CMA, CMA-HA and CLM receives its own Virtual IP, this puts a cap of 250 CMAs or CLMs per Solaris Container.

If you have more than one interface per MDS, you must specify which will be the leading interface. This interface will be used by MDSs to communicate with each other and perform database synchronization. During MDS installation, you will be prompted to choose the leading interface by the mdsconfig configuration script.

Ensure that interfaces are routable. CMAs and CMA-HA must be able to communicate with their Customer's gateways, and CLMs to their Customer's gateways.

Multiple Interfaces on an MDS

If you have more than one interface per MDS, you must specify which will be the leading interface. This interface will be used by MDSs to communicate with each other and perform database synchronization. During MDS installation, you will be prompted to choose the leading interface by the configuration script mdsconfig.

Ensure that interfaces are routable. CMAs and CMA-HA must be able to communicate with their Customer's gateways, and CLMs to their Customer's gateways.

Network Address Translation (NAT)

To examine how NAT works, let us consider an example in which a Customer has three Security Gateways connected to a router. Public IP addresses are used for the connection from the gateway to the router and through to the Internet. Internal IP addresses are used for the connection from the gateways to the local networks.
Private IP addresses are used in the local networks. Using Network Address Translation (NAT), overlapping internal IP addresses can be used, as shown in the example.

**Figure 2-29**  Physical Security Gateway Deployment Using Private IP Addresses

In this example, IP addresses starting 192.168.x.x denote public IP addresses. This does not reflect real IP addresses that could be in actual use.

In the next example, the same configuration uses public IP addresses in the local network. In this configuration NAT is not required, as there is no overlapping of IP addresses and real IP addresses are used.

**Figure 2-30**  Basic Security Gateway Deployment Using Public IP Addresses

Provider-1 supports two kinds of NAT:

- **Static NAT**, where each private address is translated to a corresponding public address. In a Static NAT scenario with a number of CMAs in an internal network, the address of each CMA is translated to a different public IP address. It is a many-to-many translation. Static NAT allows computers on both sides of the Security Gateway to initiate connections, so that, for example, internal servers can be made available externally.

- **Hide NAT**, where a single public address is used to represent multiple computers/CMAs on the internal network with private addresses. Hide NAT is a many-to-one translation. Hide NAT allows connections to be initiated only from the protected side of the Security Gateway.

NAT is thoroughly explained in the *IPS Administration Guide*.

**Enabling OPSEC**

Provider-1 supports OPSEC APIs on the following levels:

- **Gateway level** — Gateways managed by Provider-1 support all OPSEC APIs (such as CVP, UFP, SAM etc.)
- **CMA level** — CMAs support all OPSEC Management APIs. This includes CPMI, ELA, LEA and SAM.
- CLM level— CLMs (hosted on MLMs) and stand alone Log servers support all logging OPSEC APIs. This includes ELA and LEA.
Overview

A successful deployment of Provider-1 depends on careful planning before you begin to install the product. There are many different questions that you should be able to answer in order to set up a system that can accomplish the management tasks that you want it to perform. Refer to Planning the Provider-1 Environment (on page 32) to help you understand your deployment needs and map out a layout for your network. Once you have planned your network, it is time to set it up. In this chapter we will go through the steps to set up and configure your management network.

Bear in mind that a good system setup needs to be robust, flexible and scalable, so that it can expand as your business grows. Your deployment should enable you to add further MDSs using the MDG, or command line utilities. You should also be able to add administrators, customers, and GUI Clients (computers which are allowed to run the MDG) at any given time.

Provisioning Process Overview

The following list presents an overview of the Provider-1 provisioning process. Many of these procedures are described in greater detail in this chapter.

1. **Setup network topology and verify connectivity.** It is essential that you configure routing and ensure connectivity between all network components, such as MDSs, CMAs and customer gateways. Thoroughly test connectivity between all components and nodes. Make certain that your that you configure and test connectivity when adding new MDSs, CMAs and customer gateways to the Provider-1 system.

2. **Install and create the Primary MDS.** If you have only one MDS, it must be both a Container and a Manager. Configure administrators and GUI Clients at this time. For more information, see the High End Security Products Installation and Upgrade Guide.

3. **Install MDG and SmartConsole Clients.** For more information, see Using the MDG for the First Time (on page 47).

4. **Install the MDS license.** If you have a trial license, this step can be postponed until before the trial period ends in 15 days. For more information, see Adding Licenses using the MDG (on page 48).

5. Install and configure MLMs and additional MDSs as required. For more information, see Multiple MDS Deployments (on page 50).

6. Install and configure Security Gateways to protect your Provider-1 network. Define and install the security policy. For more information, see Protecting the Provider-1 Environment (on page 53).
Setting Up Your Network Topology

The MDS and customer Security Gateways should be TCP/IP ready. An MDS server should contain at least one interface with a routable IP address and should be able to query a DNS server in order to resolve the IP addresses of other machine names.

As applicable, ensure that routing is properly configured to allow IP communication between:

- The CMA/CLM and its managed gateways.
- An MDS and other MDSs in the system.
- A CMA and CLMs of the same customer.
- A CMA and its high availability CMA peer.
- A GUI client and MDS managers.
- A GUI client and CMAs/CLMs.

Creating a Primary MDS Manager

Use the distribution CD or the MDS installation utility to perform either of the following installation types:

- Fresh installations.
- MDS upgrades from previous versions of Provider-1.

All MDS types, whether Manager, Container or MLM, are created using the same installation process.

To install or upgrade the primary MDS manager, follow the instructions in the High End Security Products Installation and Upgrade Guide.

Using the MDG for the First Time

Once you have set up your primary MDS, use the MDG to configure and manage the Provider-1 deployment. Ensure that you have installed the MDG software on your computer and that your computer is a trusted GUI Client. You must be an administrator with appropriate privileges (Superuser, Global Manager, or Customer Manager) to run the MDG.

Launching the MDG

To start the MDG:
1. Select: Start > Programs > Check Point SmartConsole > Provider-1.
2. Enter your User Name and Password or browse to your Certificate and enter the password to open the certificate file.
3. Enter the MDS Manager computer name or IP address to which you intend to connect.
4. After a brief delay, the MDG opens, showing those network objects and menu commands accessible according to your Provider-1 permissions.
Adding Licenses using the MDG

To add a license to an MDS or MLM using the MDG:

1. In the MDG, Select the General View and the MDS Contents page.

2. Double-click on an MDS or MLM. The MDS Configuration window opens.
3. Select the **License** tab.

![License tab](image)

4. Install licenses using one of the following methods:

   **Fetch License File**
   
   a) Click **Fetch From File**.
   
   b) In the **Open** window, browse to and double-click the desired license file.

   **Add License Information Manually**
   
   a) Click **Add**.
   
   b) In the email message that you received from Check Point, select the entire license string (starting with `cplic putlic...` and ending with the last SKU/Feature) and copy it to the clipboard.
   
   c) In the **Add License** window, click **Paste License** to paste the license details you have saved on the clipboard into the **Add License** window.

   ![Add License window](image)

   d) Click **Calculate** to display your **Validation Code**. Compare this value with the validation code that you received in your email. If validation fails, contact the Check Point licensing center, providing them with both the validation code contained in the email and the one displayed in this window.
Multiple MDS Deployments

In Provider-1 systems where more than one MDS is installed, you need to take various configuration factors into account. The following section describes what in detail you need to know.

Synchronizing Clocks

All MDS system clocks must be synchronized to the second to ensure proper operation. Before creating a new MDS, you must first synchronize the new computer clock with other MDS platforms in the system.

You can synchronize MDS clocks using any synchronization utility. It is recommended that all the MDS clocks be synchronized automatically at least once a day do compensate for clock drift.

Adding a New MDS or MLM

Before you begin:
- If you are installing an MDS or MLM on a Linux or Solaris platform, you must synchronize the new platform clock with all other MDS platform in your deployment before starting the installation and configuration process. For Secure Platform installations, you synchronize the clocks after completing the installation routine and rebooting the computer.
- Make certain that you are logged on with superuser permissions.

To create a new MDS or MLM:
1. Install MDS or MLM on SecurePlatform or Linux computers as described in the High End Security Products Installation and Upgrade Guide. You install MLMs in the same manner as MDSs (Containers and Managers).
2. If you are installing to a Secure Platform computer, synchronize all MDS clocks at this time. For Linux and Solaris platforms, you should have synchronized the clocks prior to starting the installation.
3. In the Primary MDG General View, select the MDS Contents Mode from the View menu.
4. Select New Multi Domain Server from the Manage menu, or right-click the Provider-1 root of the MDS Contents tree and select New Multi Domain Server.

5. In the Multi Domain Server Configuration window, enter the following information:
   - MDS Name: MDS computer name
   - MDS IP Address: MDS Management IP address
   - CMA IP address Range: Range of valid IP addresses for CMAs
   - Status Checking Interval: Time in seconds between MDS status updates
6. Click **Communication** to establish SIC trust. Enter the **Activation Key** that you specified while installing the MDS or MLM computer.

![Communication Dialog](image)

7. Click **Initialize**. If SIC trust succeeds, the **Trust State** field displays **Trust established**.

![Communication Dialog](image)

If you are setting up a high availability deployment, a prompt appears asking you to perform an **Initial synchronization** for this MDS. This operation synchronizes the primary and secondary MDSs.

8. Click **Yes** to perform the synchronization. When the synchronization finishes, click **OK** to continue.

9. If you created a new MDS Manager, you can now connect directly to it. Log on the new MDS using the MDG.

**MLM Configuration - Additional Step**

If you created an MLM, set up your CLMs for customer activity logging. Refer to Logging in Provider-1 (on page 119) for details.
Modifying an Existing MDS

To modify an existing MDS:

1. In the MDG General view MDS Contents mode, select an MDS and choose Manage > Configure, or double-click the MDS, or right-click the MDS and select Configure Multi Domain Server.

2. In the Multi Domain Server Configuration window, enter or modify the following information as required:
   - **MDS Name**: MDS computer name
   - **MDS IP Address**: MDS Management IP address
   - **CMA IP address Range**: Range of valid IP addresses for CMAs
   - **Status Checking Interval**: Time in seconds between MDS status updates

3. If you wish to re-establish SIC trust, perform the following steps:
   a) From the MDS command line, execute the `mdsconfig` utility. Select (5) from the Configuration Options menu and follow the instructions on the screen to re-initialize SIC communication.
   b) In the MDG Multi Domain Server Configuration window, click Communication.
   c) In the Communication window, click Reset.
   d) Enter the Activation Key that you specified with the `mdsconfig` utility.

4. Click Initialize. If SIC trust succeeds, the Trust State field displays Trust established.

5. In the Multi Domain Server Configuration window, click OK.
Deleting an MDS

If you want to delete the MDS, do so only if you are certain that you no longer need it. If you delete an MDS in error, you will have to reconfigure it from scratch (including its CMAs and gateways).

**To delete an MDS:**
1. In the MDG **General** view **MDS Contents** mode, right click an MDS and select **Delete Multi Domain Server**.
2. Confirm the deletion and click **OK**.

Protecting the Provider-1 Environment

You should always deploy a Check Point Security Gateway to protect your Provider-1 network, including your MDS, MLM and management platforms. This section presents the procedures for installing and defining Check Point Security Gateways to protect your Provider-1 network. You can manage your Security Gateway using either a Security Management server (configured as a standalone gateway/Security Management combination) or a Provider-1 CMA and the MDG.

Standalone Gateway/Security Management

In this scenario the Security Gateway that protects your Provider-1 deployment and a Security Management server are installed on a single Linux or SecurePlatform computer.

**To deploy a Security Gateway/Security Management standalone installation:**
1. Install and configure a Check Point Security Gateway and Security Management server on a single computer as described in the *Internet Security product Installation and Upgrade Guide*.
2. Verify connectivity between the Security Gateway/Security Management server, the MDS, the SmartDashboard client and any other Provider-1 network components.
3. Verify that SIC trust has been successfully established.
4. Log on to SmartDashboard.
5. Create and configure the Security Gateway object to protect your Provider-1 deployment.

Provider-1 CMA and MDG Management

In this scenario, the Security Gateway that protects your Provider-1 deployment is installed on a SecurePlatform or Linux computer and is managed by CMA on the MDS itself.

1. Install Check Point Security Gateway on a SecurePlatform or Linux computer, without the Security Management server, as described in the *Internet Security product Installation and Upgrade Guide*.
2. Verify connectivity with the MDS.
3. Launch the MDG and log into the MDS.
4. Define a customer for the gateway and create a CMA for this customer. For more information, refer to Configuring a New Customer (on page 66).
5. In the MDG, launch SmartDashboard from the CMA and create the network object representing the Security Gateway on the CMA.
   a) Right-click the **Network Objects** icon, and from the drop-down menu select **New > Check Point > Gateway**.
   b) Enter configuration details for the gateway, including an IP address. The external gateway should have a routable IP address.
   c) The products installed on this computer should be **Firewall** and **SVN Foundation**. You can install additional products as required.
6. Establish SIC trust with the gateway.
7. Define and install a Security Policy for the gateway.
Defining a Security Policy for the Gateway

The Provider-1 gateway must have a Security Policy that allows connections between:

- the CMA & CMA-HA and their Customer gateways.
- a Customer's gateways to the Customer's CMA & CMA-HA.
- Log transfers between Customer gateways and CLMs.
- GUI Clients and Customer gateways, according to which GUI Clients are assigned to which Customer.
- GUI Clients and the CMAs & CMA-HAs, according to which GUI Clients are assigned to which Customer.

![Figure 3-31](image)

Allowing Communication between CMAs and the Gateway

The Security Policy must also allow connections between:

- The Provider-1 management network CMA and the Provider-1 management network gateway.
- Between MDSs, if they are distributed between several Provider-1 management networks.
- GUI Clients and the MDS Managers, according to which GUI Clients are allowed MDG access.

For general information regarding creating Security Policies using SmartDashboard, see the Security Management Administration Guide.

Enabling Connections Between Different Components of the System

To enable secure communication and proper access between different system components:

1. Launch SmartDashboard and connect to the CMA. Create objects to represent each Customer's CMA, CMA-HAs, CLMs, and the Customer's gateways.
2. Examine the implied rules for the CMA. These rules are created to allow CLM and CMA communication with gateways for specialized services specific to the type of CPMI communication each management uses to communicate with the Customer's gateways. Rules must be created to permit the Security Gateway to these specialized CPMI communication services between a specific Customer's CMAs and CLMs and the Customer's gateways.
3. Using the implied rules as a template, create rules for each customer permitting services from the source CMAs/CLMs to the Customer gateways, and from Customer gateways to CMAs/CLMs.
4. Examine your network deployment and decide which components should be used in rules in order to enable communications, perform status collections and push/pull certificates. For instance, if the Provider-1 network is distributed, with different MDSs in remote locations and Security Gateways protecting a remote Provider-1 network, rules must be defined to enable the MDSs to communicate with one another. In such a rule the MDSs need to appear in both the Source and Destination column of the rule. Use the table below to examine how to create rules that allows connections between specified components.

<table>
<thead>
<tr>
<th>Description</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable connections between the MDG and the MDS Manager</td>
<td>GUI Client</td>
<td>MDS Manager</td>
</tr>
<tr>
<td>Enable connections between an MDS to all other MDSs (for all MDSs with the same ICA). The connection is bi-directional, i.e. each MDS must be able to connect to all other MDSs. This includes Managers and Containers.</td>
<td>MDSs</td>
<td>MDSs</td>
</tr>
<tr>
<td>CMA status collection. Each CMA collects different status information from its Customer's gateways. If a Customer has two or more CMAs, the first CMA collects statuses from the peer (&quot;Mirror&quot;) CMAs as well.</td>
<td>Customer's CMA, CMA-HA</td>
<td>Security Gateway CMA-HA</td>
</tr>
<tr>
<td>MDS-level status data collection. In a system with more than one MDS, each Manager collects statuses from the other MDSs in the system (Managers and Containers)</td>
<td>MDSs</td>
<td>MDSs</td>
</tr>
<tr>
<td>Enable passing a certificate to an MDS. When creating a new MDS in the system, it must be supplied with a SIC certificate created by the ICA of the primary Manager.</td>
<td>MDSs</td>
<td>MDSs</td>
</tr>
<tr>
<td>Push a certificate to a CMA. When defining a Mirror CMA for a Customer, it must receive a certificate. Usually this is a one-time operation, unless you decide to supply the CMA with a new certificate.</td>
<td>CMA</td>
<td>CMA-HA</td>
</tr>
<tr>
<td>Customer level High Availability synchronization protocol. When creating a Mirror CMA and later when synchronizing CMAs (of the same Customer).</td>
<td>CMA CMA-HA</td>
<td>CMA-HA CMA</td>
</tr>
</tbody>
</table>
Chapter 4
Customer Management

In This Chapter

Overview
Creating Customers: A Sample Deployment
Setup Considerations
Management Plug-ins
Configuration

Overview

Once the Provider-1 Superuser has set up the MDSs and the Provider-1 system has been protected with a Security Gateway, it is time to start designating networking technicians, administrators and resources to manage customers/branches and their network environments. Customers can now be introduced into the framework. Here are some considerations that it can be useful to address when creating a customer:

• What type of services does the customer/branch require? Will customer administrators manage local network security or will security be handled completely by the Provider-1 environment? Will the Security Gateways be at the customer location or in a POP center in the Provider-1 environment?

• How complex is the customer's network environment? How many gateways, routers, computers, hosts, servers and users?

• What security does the customer require? What level of activity tracking?

• Does the customer require failover security management capabilities?

The first step is to create a new "Customer." The Customer is an entity that is used to represent a unique set of network objects, policies, logs and other definitions in the Provider-1 system. Usually, the "Customer" object belongs to either:

• an actual customer, or

• an enterprise branch.

This Customer must be provided with a management server (a CMA), for the Customer's physical gateways, routers, and servers. Provider-1 administrators may find it useful to have contact information, a phone number, email, and host address, so as to establish contact with Customer staff that know their system.

Building a customer setup allows the administrator assigned to the customer to bridge the gap between the virtual representation of "the Customer" in the Provider-1 system, and the actual customer/branch network requiring security and services.

The Customer needs a CMA, created to actually manage the customer's Security Gateways and networks. The CMA is put on an MDS Container, which should be chosen with an eye towards performance considerations. A customer may have a very complex network with many computers and users. It is better to create this Customer on an MDS Container without a heavy load of CMAs and policies.

Administrators must be selected and assigned to handle "Customer" maintenance within the Provider-1 environment; and to manage activities within the customer's internal network.

The internal network must be mapped into SmartDashboard, with security rules created for it. The network mapping in SmartDashboard must be updated as necessary to address changes in network structure. These customer network activities are handled with applications managing the customer network environment. They are addressed separately in Working in the Customer's Network (on page 91) and in further detail in the Security Management Administration Guide.
If failover management abilities are critical to the customer, one or more secondary CMAs must be created. For further details about CMA High Availability, see High Availability (on page 104).

Customer can be assigned CLMs, servers that are dedicated to collecting a customer's logs. For more information about customer activity logging, see Logging in Provider-1 (on page 119).

When a Provider-1 environment has many customers, it is wise to create security policy templates (Global Policies). Global policies are created using the Global SmartDashboard; this is described in more detail in Global Policy Management (on page 72).

Creating Customers: A Sample Deployment

Introduction to Creating Customers: A Sample Deployment

How does a real customer become a Customer? Let's look at a service provider deployment, in which a service provider's network has already been created, with two MDS Managers/Containers and an MLM. The first customer will now be introduced into the Provider-1 framework.

Figure 4-32  Initial customer setup in Provider-1 environment

The **Provider-1 Superuser** administrator Rajan wants to create a customer named "GasCompany." This company will be managed by an administrator named Sally. Rajan was given **Provider-1 Superuser** administrator during MDS installation. Now Rajan launches the MDG.
The MDG is the interface to the Provider-1 system, via the MDS Manager. Initial creation of the Customer takes place through the MDG. Provider-1 has an Add Customer Wizard which takes Rajan step by step through the process of creating "GasCompany."

Rajan inputs details about GasCompany: name, location, contact details. Carmen Sanchez is the Customer's IT manager on-site who is responsible for GasCompany's network in Texas, so Rajan inputs Carmen's contact details. Sally, the administrator who works just down the hall from Rajan, will want to have them handy. Rajan, as a Provider-1 Superuser, is automatically an administrator for GasCompany. He now adds Sally as an administrator. Now Rajan must choose which type of authorizations to give to Sally.

**What Type of Administrator?**

What sort of administrator should Sally be? Sally is going to be handling many different aspects of customer management within the Provider-1 environment, but she does not need to create new Customers or be a Superuser. On the other hand, she needs to be able to start and stop the CMA for maintenance or updates. So Rajan assigns her **Customer Manager** permissions. Rajan also assigns Read/Write permissions for GasCompany to Sally.

**What Type of Authentication?**

Rajan must choose an authentication scheme for Sally: either provide a user name and password (less secure) or use a certificate (recommended). Rajan chooses authentication via certificate, and generates a certificate for Sally. When Sally logs into the system, she will use this certificate to be authenticated and establish trusted communication. Otherwise, the Provider-1 system will not let her in.
Assigning a Computer

Using the comprehensive Add Customer Wizard, Rajan assigns permission to Sally to use her computer to launch SmartConsole applications and the MDG, in order to manage GasCompany's network. Rajan does not want every computer to be able to launch applications for this customer: it would be a security breach.

Figure 4-33 Sally is now a Customer Manager

Assigning a CMA

Rajan names the first CMA GasCompany_CMA. The CMA is a virtual Security Management server. Rajan chooses an MDS Manager/Container in the service provider site to "house" the CMA. Even if there were many other customers, GasCompany does not have a very complex environment, so Rajan is not worried about putting the Customer on any MDS in the system. Of course, if the system was full of Customers with major accounts and thousands of supported gateways, Rajan would think twice about which MDS to use!

To provide it with a virtual IP, which is mapped to the MDS interface, Rajan has already entered a range of virtual IP addresses for the MDS interface in the MDS configuration window. The Provider-1 system automatically maps this range to the MDS interface. Now, using the Add Customer Wizard, Rajan creates the CMA and uses the Get Automatic IP Address option. The Provider-1 system assigns the first available virtual IP address to GasCompany_CMA.

The CMA license is already on-hand: Rajan ordered it in advance. Using the Add Customer Wizard, Rajan imports licensing data and creates the CMA.

GasCompany wants failover security, so Rajan uses the Add Customer Wizard to create a mirror (secondary) CMA named GasCompany_CMA_HA on a different MDS Container. (The mirror CMA must be created on an MDS other than the one hosting the primary CMA).
The CMAs are now up and running; they have been "started" by the system.

**Figure 4-34** A 'started' CMA can begin managing GasCompany's network

Rajan has completed the basic steps involved in introducing a customer into the Provider-1 setup.

Having created a customer's CMA, it is time to establish a connection between the Active CMA and the Security Gateways it will manage.

There are two processes involved. Sally, the **Customer Manager** will launch SmartDashboard from the CMA and create a gateway object with the IP address of the gateway. Additionally, the gateway managing the Provider-1 management network must allow communication between the CMA and the customer's gateways. This is described further in Working in the Customer's Network (on page 91).

Then Rajan, the **Provider-1 Superuser**, creates appropriate security rules for the Provider-1 management network gateway to allow communication between the CMA and the customer's gateways. This is described briefly in Provisioning Provider-1 (on page 46).

**Connecting to a Customer Network**

The Customer network is defined not at the Provider-1 setup level but rather at the customer level, through SmartDashboard. Now Sally is ready to take over. GasCompany's actual network components are defined in SmartDashboard, which is launched from the CMA. Sally configures the customer/branch's network by creating objects for the gateways, routers, hosts, users, user groups, servers, and other network components, using SmartDashboard. These activities, which relate exclusively to a specific customer's network, are addressed in Working in the Customer's Network (on page 91), and in further detail in the Security Management Administration Guide.

Communication must also be permitted between the Provider-1 network and the customer's gateways. Rajan inserts appropriate rules permitting the CMAs to communicate from the Provider-1 network with the customer's Security Gateways.

Once Sally defines gateways and links them to the GasCompany_CMAs, these gateways are displayed in the MDG. However, information about different individual customer networks is isolated securely and privately from other customer networks. The customer network's details are stored in CMA databases which are isolated from each other. Only a CMA's secondary (High Availability) CMA will share access to the CMA's customer network information.
Creating more Customers

As more customers/branches are added in the Provider-1 setup, the same procedure is followed. A new customer/branch is defined, assigned an administrator and a GUI Client, and a CMA is created for the customer/branch. Rajan assigns two more new Customers to Sally, then another one to Monisha. The Provider-1 network is now connected to four customer sites. And it’s just the beginning.

Figure 4-35  Creating more customers/branches
Creating more MDSs

At some point the service provider’s MDS Container will be handling a heavy load, with many CMAs supporting a large number of Security Gateways, network objects, and users. It will be a good idea to start creating any new customers on a different MDS Container, perhaps adding a Container to handle the load. Once the new Container is setup, the process for creating new customers is the same. A new customer/branch is defined, assigned an administrator and a GUI Client, and a CMA is created for the customer/branch.

Setup Considerations

IP Allocation for CMAs

Each CMA must have a routable IP address. Every time a CMA is started, a Virtual network interface for CMA’s virtual IP is created. By default, the virtual network interface will be created on the MDS primary network interface.

During MDS configuration, you may specify a range of virtual addresses for a Container interface. Then, as you create each CMA, the Provider-1 system can automatically fetch the next available virtual IP and assign it to the CMA. Alternatively, rather than fetch from a range, you can designate a particular virtual IP to a CMA. Keep the CMAs IPs in mind for routing purposes, as you will need to ensure that your route tables allow communication between CMAs and their customer gateways.

You do not need to create any of the actual virtual IP interfaces on the server. If you would like to host the CMA’s IP address on a different network interface, you can do so by stopping the CMA, removing its virtual IP address definition and modifying the CMA file vip_index.conf.

Assigning Groups

In some cases, the same operation (such as assigning an administrator or policy) must be performed to many customers with similar security policy needs. By default, each time you select customers to apply an operation, you must go through the entire customers list and check them one by one.

To avoid this time-consuming process and facilitate customer selection, it is recommended that you use customer selection groups, which easily identify customers that can be handled simultaneously. Provider-1 has two types of selection groups: customer groups and administrator groups. As opposed to groups
created through SmartDashboard, these selection groups are not network objects. Their sole purpose is to facilitate customer or administrator selection.

For details on configuring groups, see Configuration (on page 66).

Management Plug-ins

Introducing Management Plug-ins

Management Plug-ins allow administrators to manage certain new features without performing a complete management upgrade. The Management Plug-in package (referred to from this point simply as "Plug-in") consists of only the components necessary to manage the new features.

In the Provider-1 environment, Plug-ins are installed on the MDS, and then "activated" from the MDG for relevant Customers. Each Plug-in can be activated for all Customers, or for specific Customers only. Different Plug-ins can be installed on different Customers.

When a Plug-in is activated for a Customer, various types of operations become available via the SmartDashboard of the Customer, such as creating new types of objects, modifying objects, etc. The operations are dependent on the characteristics of the individual Plug-in.

To summarize, the components of the Provider-1 environment relate to Management Plug-ins in the following ways:

- MDSs - Plug-ins are installed on them
- MDG - used to activate and deactivate Plug-ins, review their status, and see basic information regarding the new types of objects
- SmartDashboard for a CMA - used to manage the new Plug-in objects and handle the new features provided by an installed and activated Plug-in

Installing Plug-ins

Management Plug-ins are installed on the MDS from the command line. See the accompanying documentation for the Plug-in for specific installation instructions.

After installing a Plug-in to each relevant MDS, the MDS(s) must then be restarted using the commands mdsstop -m/mdsstart -m. At this point the Plug-ins are available for activation on Customers.

Activating Plug-ins

Plug-ins are activated per Customer from the MDG in the following ways:
- From the **Customer Configuration** window, when creating a new or modifying an existing Customer

![Customer Configuration Window](image1)

- From the **Management Plug-ins View**, by right-clicking in the cross-section of the desired Plug-in and Customer, and selecting **Activate this Plug-in**

![Management Plug-ins View](image2)

When a Plug-in is activated for a Customer, if one or more of the Customer's CMAs are running, the MDS restarts those CMAs.

If a Plug-in is activated for a Customer with a single CMA, and a second CMA is added later, the Plug-in will be activated automatically on the new CMA.

In the rare event where a Plug-in is activated for a Customer and it succeeds on one CMA and not on another, synchronization between the CMAs will fail. In this condition, the MDG displays an error message with a recommendation of what needs to be done. The MDG also displays the icon **Needs Attention** in the **Management Plug-ins View**. In many cases this situation can be resolved by selecting **Reactivate All Plug-ins** from the **Plug-in menu**.
Plug-ins can also be deactivated. Once a Plug-in has been activated for a Customer, and objects have been created, the Plug-in cannot be deactivated until those objects are removed.

**Plug-in Status**

Once a Plug-in is installed on the MDS, it appears in the Management Plug-ins View of the MDG. This View indicates whether a Plug-in is Activated or Not Activated per Customer, and displays an alert notification of Needs Attention for any Plug-in that has not been activated properly. For a Plug-in to appear in this View, it must be installed on at least one MDS.

**High Availability Mode**

In High Availability (HA) mode, each Plug-in to be used must be installed on all MDSs in the Provider-1 environment. As in non-HA environments, MDSs must be restarted before the Plug-ins are available for use. It is therefore possible to install the Plug-ins to disparate MDSs at the time of your choosing, and then restart them all at the same time for synchronization compatibility. If there is a delay in restarting any of the MDSs, those MDSs that have not been restarted will not be able to communicate with those that have been. This is referred to as a Plug-in Mismatch. See Plug-in Mismatches on page 65 below for details.

For deployments using a Security Management Backup server, Plug-in packages must be installed to the Security Management Backup server from the command line, as they are for the MDS. The Security Management Backup server should be restarted with the other HA MDSs.

**Plug-in Mismatches**

A Plug-in Mismatch occurs in a Provider-1 HA environment under the following conditions:

- The Plug-in is not installed on every MDS
- The Plug-in is installed on every MDS, but not every MDS was restarted afterwards.

Plug-in Mismatches are indicated in two places on the MDG. The General View - MDS Contents mode will display a Plug-in Mismatch on the relevant MDS under the Status column.
The **Plug-ins View** will display the **MDS Plug-ins Mismatches** pane, where the install status of each Plug-in on each MDS is reported.

**Note** - The **MDS Plug-in Mismatches** pane appears only if a Plug-in mismatch exists.

To resolve a Plug-in Mismatch, from the **MDS Plug-ins Mismatches** pane, review the situation and decide whether you want to:

- Install the Plug-in to any MDSs that display the icon (add graphic), and then restart those MDSs
- Remove the Plug-in from each MDS that displays the icon (add graphic)

### Configuration

#### Configuring a New Customer

New Customers are created through the **Add Customer Wizard**, which takes the administrator through all the steps needed to create a customer, assign an administrator and a GUI Client, and create the CMA.

**Start the Add Customer Wizard**

In the **MDG Customer Contents** Mode (the view to which the MDG first opens).

To create a customer, click the **New Customer** tool in the toolbar, or from the **Manage**, choose **New Customer...**, or right-click the **Provider-1** root and choose **New Customer...** from the drop-down menu. The **Add Customer Wizard** will then guide you through the definition of the new customer and the customer's CMA(s). You can create a primary and secondary CMA for the customer at the same time.

**Name the Customer and Enable QoS**

Give the Customer a name and enable QoS if desired.
**Customer Details**

Assign Customer Properties, for example, a contact person, contact e-mail, and contact phone-number.

You can add or delete these information fields via the Manage > Provider-1 Properties, in the Customer Fields tab.

**Assign Global Policy**

1. Set whether the Customer should be assigned all Global Objects or only those used in the Global Policy to which it is assigned.
   
   Also, if you want the Customer to receive the Global IPS policy, defined in Global SmartDashboard, do the following:
   
   a) Enable the **Subscribe Customer to IPS service** property. Once a Customer is subscribed to the IPS service, whenever Global Policy is assigned, changes to Global IPS are assigned and ready to be installed to the Customer as well.
   
   b) Set the **Assign Mode**:
      
      - Set to **Merge** if you want to allow the Customer Administrator to make permanent changes to the IPS policy assigned.
      - Set to **Override**, if you do not want to allow the Customer Administrator to make permanent changes to the IPS policy assigned.
   
   c) **Create a database version** if you want to allow Customer Administrators the ability to roll back to previously installed policy versions.

2. For details regarding Global IPS, see Global IPS (on page 79).

**Assign Administrators to the Customer**

1. The wizard next prompts you to select administrators. To assign an administrator to a customer, select the administrator from the **Not Assigned** column and click **Add**. You can create administrator groups to facilitate administrator assignment. All members of the group you choose are automatically selected, allowing you to **Add** or **Remove** them as a group. To create a new administrator, click **New Admin...**. Then define the new administrator as follows:
   
   a) If you have a Provider-1 **Superuser** permission, you can choose the Administrator's Provider-1 Permission as well.
   
   b) In the **Authentication** tab, select the administrator's authentication scheme: password (less secure) or certificate (recommended). If you choose authentication via certificate, in the **Certificates** tab, create a certificate. It is generated into a file and should be given to the administrator.
   
   c) Define permissions: Read/Write or a Read Only permission to the customer's network objects and policies. These permissions should also be specified when configuring the customer's gateways. An **Edit Administrator Permissions** window, corresponding to the **cpconfig** tab, can be displayed through the **Administrators** window in two ways: automatically, when you click **Add** to assign an Administrator to a customer, or manually, by selecting an Administrator from the **Assigned** list and clicking **Permissions...**

**Assign Computers on which Administrators use the MDG**

Specify the **GUI Client** (computer) from which administrators are authorized to use the MDG and/or SmartConsole application.

**Activate Management Plug-ins**

Select the Management Plug-ins necessary for this Customer. Management Plug-ins extend the MDG's ability to view and manage certain objects without the updating the management version.
Create the CMA

1. Decide to create one, two, or more Customer Management Add-ons (CMAs). Create two or more CMAs if you want to enable High Availability. All mirror (secondary) CMAs must be created on a different MDS Container from the one housing the primary CMA, so you must have at least two Containers in the system to created CMA High Availability. If you create multiple CMAs, steps 7 to 9 apply for each CMA.

2. Define the CMA. Select the Container MDS on which this CMA will be maintained. You can provide a virtual IP address for the CMA, or the Provider-1 system can also produce a virtual IP from a range that you specify per MDS. You can fetch an IP address (for the MDS) by using the Get Automatic IP Address button. If you have already set up a host table specifying a name and virtual IP for the CMA, you can Resolve by Name, fetching the IP address matching the name of the CMA.

Add CMA License Details

1. Next, fill in the license information. When you request a license from the Check Point licensing center, you receive a file that includes the license string. You can import the file with the license by clicking the Fetch from file... button.

Or, you can click Add to access the Add License window. Then, you can quickly and easily enter the license string data from the email application into the Add License window, as follows:

   a) In the file, highlight the entire license string (that starts with cplic... and ends with the last SKU/Feature) to the clipboard. Choose Copy from the Edit menu of your email application.

   b) In the Add License window, click Paste License to paste the license details you have saved on the clipboard into the Add License window. The license details will be inserted into the appropriate fields, described below.

To validate your license, click Calculate to figure out your Validation Code, and compare with the validation code received from the User Center.

2. For further license management use the following, click Fetch From File to import one or more licenses from a license file. In the Open window, browse to the license file, select it and click Open. The license that belongs to this host is added. The Licenses list displays the details of the CMA's license entered through the Add License window.

3. To define a mirror CMA, repeat the instructions for adding the first CMA, steps 6 and 7. The mirror (secondary) CMA must be created on a different MDS from the one housing the primary CMA. See High Availability (on page 104).

4. The new customer appears in the customer tree.

Creating Administrator and Customer Groups

Creating Customer Selection Groups

To create a customer selection group in any MDG View, select Manage > Selection Groups > Customer Groups... from the menu. Click Add to add a group, then name the group, and select members. To add customers to the selection group, select them in the Not in Group list and click Add. To remove customers click Remove.

Creating Administrator Selection Groups

To create a customer selection group in any MDG View, select Manage > Selection Groups > Administrator Groups... from the menu. Click Add to add a group, then name the group, and select members. To add administrators to the selection group, select them in the Not in Group list and click Add. To remove administrators click Remove.
Changing Administrators

To add/delete/edit a customer's administrators, change administrator permissions, or edit an administrator's password, you can open the Administrators view and perform these specialized activities relating to administrators.

To make various changes to an administrator, select an administrator and from the right-click drop down menu choose an action.

To create a new administrator, select New Administrator... from the Manage or right-click the Provider-1 root and select Add Administrator. Step through the procedures, which are the same as in the Add Customer Wizard. See Assign Administrators to the Customer (on page 67).

Modifying a Customer's Configuration

To modify a customer, select the customer and then choose Configure... from the Manage, or click the configure tool, or double-click the customer. The Customer Configuration window allows you to change all the basic customer settings.
Changing GUI Clients

To add/edit/switch/delete the GUI Client that a Customer is managed from, you can open the GUI Client view and reassign the Customer to a different GUI Client:

Select a GUI Client, and from the right click menu, choose an action.

To create a new GUI Client, select New GUI Client... from the Manage or right-click the Provider-1 root and select New GUI Client. Step through the procedures, which are the same as in the Add Customer Wizard. See Assign Computers on which Administrators use the MDG (on page 67).

Deleting a Customer

To delete a customer, select it in the Customer Contents Tree and then choose Delete from the Manage from the menu, or click the delete tool, or right-click the customer and select Delete Customer from the right-click menu.

Configuring a CMA

To configure a CMA, select it in the Objects Tree (in either one of the General View Modes), and select Manage > Configure, or double-click the CMA you wish to edit, or right-click the CMA and select Configure Customer Management Add-on/Configure Customer Log Module.

While the Name, Multi Domain Server and IP Address of the CMA cannot be changed, its Licenses are available for configuration.

Starting or Stopping a CMA

To start or stop a CMA:

1. Select the CMA.
2. From the Manage, choose Start Customer Management/Start Customer Log Module or Stop Customer Management/Stop Customer Log Module as appropriate, or select Start or Stop from the toolbar. The run status of the CMA will change accordingly, and the change will be reflected in the Status column.
An alternative way to start or stop a CMA is from the MDS command line, by using the `mdsstart_customer` and `mdsstop_customer` commands.

### Checking CMA Status

You can check the run status of the CMA in the **Status** column of the MDG **General View**:

- ✓ This CMA is started.
- ! This CMA is stopped.
- ? Unknown Status information has been received regarding the Run Status of this CMA.
- ⬤ Waiting... This CMA is waiting for a status update. Displayed from the time the MDG starts running until the time the first status is received.

### Deleting a CMA

Before deleting a CMA, make sure to stop it. Select it in the MDG **Customer Contents** view and then choose the delete tool in the menu bar, or **Manage > Delete**, or right-click the CMA and select **Delete** **Customer Management Add-on/Delete Customer Log Module** (respectively) from the right-click menu.
Chapter 5

Global Policy Management

In This Chapter

Security Policies in Provider-1 72
Global SmartDashboard 75
Creating a Global Policy through Global SmartDashboard 78
Global IPS 79
Assigning Global Policy 83
Configuration 87

Security Policies in Provider-1

Introduction to Security Policies in Provider-1

A Security Gateway at a network boundary acts as a gateway that inspects and provides access control for all traffic passing through the gateway. Traffic that does not pass through the Security Gateway is not controlled.

Figure 5-36 Check Point Security Gateway inspects all traffic

The administrator is responsible for implementing the company security policy. Check Point Security Gateway allows the company Security Policy to be consistently enforced across multiple Security Gateways. To achieve this, an enterprise-wide Rule Base is defined for a Customer through the CMA. SmartDashboard is used to install the policy, and distribute it to the Customer's gateways. Granular control of the policy is possible by having specific rules apply only on specific gateways.

Security policies are created to enforce security rules. Provider-1 administrators can create security policies and rules tailored to a specific Customer, or for many Customers of a certain type. In the Provider-1 environment, administrators create a Customer's security policies for a specific set of gateways, using the CMA.
The CMA, which is the equivalent of the Security Management server in the Security Gateway model, allows administrators to create rules that apply to specific Customer networks and their Security Gateways. For information about using SmartDashboard to construct security policies, see the Security Management Administration Guide.

Figure 5-37 How security policies are created

The administrator directly defines a Customer's network and the security policy and QoS policy via the CMA, using SmartDashboard. SmartDashboard is launched for a particular CMA, and the administrator defines all the network objects, gateways, hosts and nodes in the Customer's network. The administrator also uses SmartDashboard to create a set of rules (a rule base) which compose a security policy. The CMA then downloads (or installs) the Security Policy to the Customer's Security Gateways.

The fundamental concept of the security policies' rule base is "That which is not explicitly permitted is prohibited." The rule base specifies what communication will be allowed to pass and what will be blocked, and specifies the source and destination of the communication, what services can be used, at what times, and whether to log the connection.

When creating rules for the system, an administrator must consider the needs of the organization:

- What are the physical and logical components that make up the organization? Each component of the organization needs to be accounted for. Every server, every printer, every resource, etc.
- Who are the users and administrators and how should they be divided into different groups?
- What are the access needs of these users?
- Are there public access needs?
- What types of access must be prevented?

A substantial amount of planning should go into deciding how to define the Customer network (by creating representative objects), and how they should be implemented.

The Need for Global Policies

Besides security policies for a specific set of gateways, administrators need to create policies which apply to the entire Provider-1 environment or to a group of Customers. The separation between different levels of policies, and different types of policies, means that Customer-level security rules do not need to be reproduced throughout the entire Provider-1 environment.
Security policies can be created and privately maintained for each Customer, ensuring a Customer's security integrity. Global policies enforce security for the entire Provider-1 system or for a group of Customers.

**Figure 5-38** Policy creation workflow

The Global Policy as a Template

Security policies can be created and privately maintained per Customer, ensuring a Customer's security integrity, but some security rules are enforced by all Customers. Global policies can serve as security templates with rules that are applied to many Customers, and their individualized security policies.

Types of Global Policies can be designed for groups of Customers with similar security needs. This eliminates the need to recreate identical policies for each Customer. This feature greatly improves management efficiency. A service provider may use Global Policy rules to provide Customers with access to common MSP services but does not allow Customers to access private information about each other.

An MSP may provide several basic types of security policies. Rather than recreate the rule base for each new Customer, they can create a Global Policy for banks, a different Global Policy for independent dentists and therapists, and a Global Policy for small businesses, such as grocery stores, florists, gas stations or tax accountants.

An enterprise may use a Global Policy to set corporate wide policies. For example, an airline company with many branches and sales-offices, sales points and Customer check-in facilities may want to set rules for many different types of standard access needs. Rather than painstakingly recreating the same rule or set of rules for each branch, a global security policy can secure access across the board.

Global Policies and the Global Rule Base

Global policies are created using the global rule base, which contains a hierarchy of rules. In a Global Policy, you define common (global) rules, which are given priority in the rule base. These rules can be distributed (or assigned) to whichever Customers you choose. The Global Policy rule base is similar to the management rule base, except that it includes a demarcation or a "place holder" for Customer-specific rules.

The placeholder signifies that all the rules before and after it are global rules. The rule base layout is hierarchical: the most important global rules are highest up in the rule base. They take precedence over the Customer rules. Global rules that are designated as being of lower priority than Customer rules appear below the place holder.
The rules of the Global Policy are not specific to a single policy of single Customer, but apply to all Customers assigned the Global Policy.

Global rules can serve many uses. They can be used to rapidly implement defense against new cyber attacks or viruses. They can be used to prevent logging for specific types of traffic in order to reduce the amount of information in log files. They can be used to set up rules for CMA communication management, such as allowing additional GUI Clients to be implemented at Customer sites.

Only one set of objects is used for all the Global Policies. The Global Policies database contains this set of objects, which can be used in any global rule in any Global Policy. The administrator creates these objects using Global SmartDashboard. Global Object icons are displayed with a purple G. For example, a Global Check Point Node has the G icon.

Global policies can be assigned to one or more Customers. Once Global Policies are assigned to a Customer's CMA, they become part of the CMA's rule base. The entire CMA's rule base, including assigned global rules, can then be installed onto selected Security Gateways.

Global SmartDashboard

Introduction to Global SmartDashboard

In order to create Global Policies, the Global SmartDashboard is used to create the Global Policy Rule Base. The Global SmartDashboard, launched off the MDS Manager, represents the network and is used to create rules and network objects at the Provider-1 system level.

SmartDashboard differs from Global SmartDashboard in that it applies only to the Customer level and below. After a Global Policy is assigned to a Customer, SmartDashboard for the Customer's CMA will show global rules automatically inserted either above or below editable Customer rules. The Customer administrator can create or edit Customer rules using SmartDashboard, and then install the policy onto the Customer's Security Gateway.

Once a Global Policy is assigned to a Customer, the global rules are displayed as read-only in the Customer's SmartDashboard. A Customer administrator cannot edit global rules or Global Objects from SmartDashboard.

Global Services

Default services defined by Security Gateway are available for global use. Other services need to be defined. To avoid collision, ensure that you name services with unique names, which should not be the same as in the CMAs' databases.
Dynamic Objects and Dynamic Global Objects

*Dynamic objects* are generic network items such as a host or server object that has no IP specified. The administrator creates them in SmartDashboard, and uses them to create generic rules for Customer's gateways. At each gateway, the dynamic object can be translated into a specific local computer, host or other network object, with an IP address.

Global rules may similarly use dynamic *Global Objects*, which are generic items (such as a web server) that can be applied to any network. Global objects are defined through the Global SmartDashboard and SmartDashboard are downloaded to the CMAs.

At the global level, an administrator defines *dynamic Global Objects* in addition to standard Global Objects which are available in the Global SmartDashboard. Once a Global Policy is assigned to a Customer, the dynamic global object is replaced by a corresponding Customer object. This makes it possible to create global rules without requiring that the rule use specific network objects. This allows the administrator to create rules that are "templates."

A dynamic global object serves as virtual place holder for a network element. The network element type can be anything that the administrator designates, including gateways, hosts, or services, or even groups. A dynamic global object is created in the Global SmartDashboard with the suffix _global_ (for example, FTPserver_global). This object is applied to a global rule.

To "translate" the dynamic global object, the administrator creates an object in SmartDashboard with the same name, but with an IP address and other details. The Customer's database substitutes the dynamic global object in the global rule with the local object from the CMA database. Alternatively, the dynamic global object is replaced with a CMA dynamic object, and the object is assigned an IP at the gateway level.

To understand how the dynamic global object is used, let us consider an example. An administrator creates a global rule applying to a dynamic global object representing a generic ftp server. But instead of specifying exactly which ftp servers and their IP addresses will be affected by the rule, the servers are represented by a dynamic global object (FTPserver_global).

In each CMA, the Customer administrator will define a host object with the same name. During the assignment of the Global Policy, the references to the global dynamic object in different rules will be replaced by the reference to the local host object with the same name. The _global_ syntax triggers the reference replacement mechanism.

**Applying Global Rules to Gateways by Function**

It is possible to create Security Rules in Global SmartDashboard that are installed on certain gateways or groups of gateways and not others. Thus gateways with different functions on a single CMA can receive different security rules designed for a specific function or environment. When installing global policy to a number of similarly configured CMAs, the relevant global rules are installed to all of the relevant gateways on each CMA.

This feature is particularly useful for enterprise deployments of Provider-1, where Customer CMAs typically represent geographic subdivisions of an enterprise. For example, an enterprise deployment may have Customer CMAs for business units in New York, Boston, and London, and each CMA will be similarly configured, with a gateway (or gateways) to protect a DMZ, and others to protect the perimeter. This
capability allows an administrator to configure the global policy so that certain global security rules are installed to DMZ gateways, wherever they exist, and different rules are installed to the perimeter gateways.

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

**To install a specific security rule on a certain gateway or types of gateways:**
1. Launch Global SmartDashboard for the relevant Global Policy.
2. In the Objects Tree, right-click **Dynamic Objects** and select **New Dynamic Object**.
3. Name the dynamic object, and add the suffix **_global** to the end of the name.
4. On the **Firewall tab**, create rules to be installed on gateways with this function, and drag the dynamic object you created into the **Install On** column for each rule.
5. Launch the SmartDashboard for each relevant CMA.
6. Create a group object with the name of the dynamic object you created, including the suffix **_global**.

**Note** - While you can name a gateway with the name of the global Dynamic Object, it is recommended to create a group to preserve future scalability (for instance, to include another gateway with this function). It is not recommended to change the name of an existing gateway to the dynamic object name.

7. Add all gateways on the CMA that you want to receive global security rules with this target to the group.
8. Select **File > Save**.
9. From the MDG, re-assign the global policy to the relevant Provider-1 Customer(s).

**Synchronizing the Global Policy Database**

The Global Policy database is synchronized on all MDS Managers automatically, or manually, depending on the settings. Global policies must be synchronized for the entire system, since they are system-wide security templates, and the entire system uses the same Global Objects. Synchronization is performed when the Global Policy is saved, or at a configurable interval.
Creating a Global Policy through Global SmartDashboard

Global policies are created using the Global SmartDashboard. Customer policies are made using SmartDashboard launched via the CMA. Let us consider an MSP that wants to implement a rule which blocks unwanted services at Customer sites. The Provider-1 Superuser, Carol, wants to set up a rule which will allow Customer administrators discretion to decide which computers are allowed to access the Internet.

Figure 5-39 Carol creates a rule for the web server

Carol launches Global SmartDashboard. She creates a global dynamic object to represent a group of computers that are allowed to access the Internet, and names it `gInternetAccessAllowed_Global`. She creates a rule using the global dynamic object.

<table>
<thead>
<tr>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>VPN</th>
<th>SERVICE</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>gInternetAccessAllowed_Global</code></td>
<td>Any</td>
<td>Any Traffic</td>
<td>Any</td>
<td>Allow</td>
</tr>
</tbody>
</table>

Once she has created a Global Policy including this rule, she assigns/install it for specific Customers and their network gateways. Each Customer administrator must create a group object with the same name as in the CMA database. This is done through SmartDashboard. In this way, local administrators translate the dynamic global object into sets of network object from the local database.

For details about using SmartDashboard, consult the Security Management Administration Guide. The differences between the Customer's SmartDashboard and the Global SmartDashboard are as follows:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Customer SmartDashboard</th>
<th>Global SmartDashboard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Base</td>
<td>Local, applying to the Customer network only.</td>
<td>Global, applying to multiple networks of all Customers assigned this Global Policy.</td>
</tr>
<tr>
<td></td>
<td>Is not associated with the Customer's other security policies.</td>
<td>Automatically added to all of the assigned Customers’ security policies.</td>
</tr>
<tr>
<td></td>
<td>Each Customer policy is independent, with its own rules</td>
<td>All the assigned Customers’ policies share the global rules</td>
</tr>
<tr>
<td>Network Objects</td>
<td>Local, applying to this network only.</td>
<td>Global, applying to multiple networks of all Customers assigned this Global Policy.</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Global Properties</td>
<td>Enabled.</td>
<td>Disabled (manipulations is through the Customer SmartDashboard).</td>
</tr>
<tr>
<td>Saving a Security Policy</td>
<td>Adds the security policy to the list of Customer security policies</td>
<td>Adds the Global Policy to the Global Policies database (and displays it in the <strong>Global Policies</strong> Tree of the MDG).</td>
</tr>
</tbody>
</table>

**Note** - Global SmartDashboard cannot be used to create Connectra or Security Gateway objects. Instead, use a SmartDashboard connected to a specific CMA to create these objects.

## Global IPS

### Introduction to Global IPS

IPS protections are centrally managed using the Global SmartDashboard, and then distributed to Customers via the **Assign Global Policy** operation in the MDG. Multiple IPS Profiles can be configured in the Global SmartDashboard. When Global Policy is assigned to a CMA, the CMA receives all of the IPS Profiles. Customer Administrators can then assign different profiles to various gateways. Customer can make limited changes to further customize the protections of a Profile through the SmartDashboard of the CMA.

It is important to note that the *global* nature of Global IPS refers to the ability to set IPS Profiles for all subscribed Customers from the Global SmartDashboard. However, the CMA administrator for each Customer can assign different profiles to each gateway and modify the IPS protections in certain ways once they have been installed. So in this case, the term *global* does not confer a meaning of *read only*, as it does in the case of the Global Security Policy.
IPS in Global SmartDashboard

The Global IPS Policy is configured on the IPS tab in the Global SmartDashboard.

IPS protections available in the Global SmartDashboard are identical to the default settings and protections for a CMA. Any changes made to the Global Profiles apply to all CMAs subscribed to the IPS service.

**Note** - You must have an Enterprise Software Subscription to update IPS protections. Enterprise Software Subscriptions are available for purchase at the User Center (http://usercenter.checkpoint.com).

IPS Profiles

An IPS Profile is a complete set of configured IPS protections that can be applied to multiple gateways. On the CMA, multiple IPS Profiles can be assigned to suit gateways that are exposed to different types of threats.

Global SmartDashboard supports multiple IPS Profiles. Changes made to IPS protections for a Global Profile are replicated when the Global Policy is assigned to CMAs that are subscribed to the IPS Service.

For further details regarding IPS Profiles, See the IPS Administration Guide at http://supportcontent.checkpoint.com/documentation_download?ID=8746.

Managing IPS Profiles

You IPS Profiles are managed from the IPS tab in the Global SmartDashboard. Select Profiles from the Navigation Tree to view all Profiles and make changes.

Creating a New IPS Profile

**To create a new IPS Profile:**
1. In SmartDashboard (Global or CMA), select the **IPS** tab.
2. Select **Profiles**.
3. Select New and either Create New Profile or Clone Selected Profile (to clone a profile, one must be selected).
4. Enter a Profile Name and Comment. Select the IPS mode (Prevent or Detect) and a Protection Activation method.

Editing an IPS Profile

To edit an IPS Profile:
1. In SmartDashboard (Global or CMA), select the IPS tab.
2. Select Profiles.
3. Double-click a profile.
4. Edit parameters as required on any of the pages.
5. On the Networks Exceptions page, add and edit exception rules by clicking New or Edit.

Subscribing Customers to IPS Service

Any Customer that you want to include in the global IPS policy must be subscribed to the IPS service.

To subscribe an existing customer to the IPS Service:
1. In the MDG, enable the Customer Contents Mode.
2. On the Selection Bar, select General.
3. Double-click a customer name in the list.
4. In the Customer Configuration window, select the Assign Global Policy tab.
5. Enable the Subscribe Customer to IPS Service option.

Customers who subscribe to the IPS Service are automatically assigned to an Exclusive subscription. Once Customers are subscribed to the IPS service via the global policy, any changes made to the Global IPS Profiles are forwarded to the CMAs whenever Global Policy is assigned. See Assigning Global Policy (on page 83) for details.

Note - Merge and Override IPS subscriptions are no longer supported in Provider-1.
Managing IPS from a CMA

After Customers are assigned Global Policy, the IPS Profiles configured on the Global Dashboard are augmented to the local profiles list on the CMA. Customer Administrators can assign the Profiles to specific gateways. They can also modify the profiles in limited ways.

Protection settings for Global Profiles cannot be edited from the CMA. However, exceptions can be defined for specific traffic in the IPS tab of SmartDashboard.

Once a Profile has been downloaded to a CMA, there will be a 'G' prefix at the beginning of the Profile name and 'Global' appears in the activation column in the local SmartDashboard.

Any exceptions set globally for a specific Global Profile are indicated with a 'G' icon and cannot be changed from the CMA.

Assigning IPS Profiles to Gateways

IPS policy will not be activated on any gateways until the gateway is assigned a Profile.

To assign an IPS Profile to a gateway:
1. Navigate to the Profile Assignment page in one of two ways:
   a) From the gateway object:
      ▪ In the SmartDashboard of the CMA on which the gateway is managed, right-click the gateway and select Edit.
      ▪ Select IPS from the navigation tree in the Check Point Gateway dialog box.
   b) From the IPS tab:
      ▪ In the SmartDashboard of the CMA on which the gateway is managed, select the IPS tab and Enforcing Gateways from the navigation tree.
      ▪ Select a gateway from the list and click Edit.
2. Select Assign Profile and select a profile from the list, then click OK.
3. If you do not want to apply IPS on the gateway, select Do not apply IPS on this gateway.
4. Select Policy > Install, and make sure the gateway is selected in the Advanced Security column.
5. Click OK to install policy and activate the assigned IPS Profile.

Removing Global IPS from a CMA

To remove Global IPS from a CMA:
1. In the IPS tab of the CMA SmartDashboard, make sure that gateways on the CMA are not using Global Profiles.
2. In the Global Policy page of the MDG, select a customer, right-click, and select Configure Customer.
3. In the Assign Global Policy tab, clear Subscribe to Customer IPS Service and click OK.
4. In the Global Policy page, select the customer again, right-click, and select Reassign Global Policy.
   Click OK to confirm.

   Note - If you select Remove Global Policy, Global IPS will be removed from the CMA regardless of the check box setting.

Making Changes to an IPS Profile

Customer administrators can make exceptions to protections in a Profile and can override actions of a protection. These changes are made from the IPS tab of the CMA's SmartDashboard by clicking Edit. See the IPS Administration Guide for more information on creating exceptions and changing actions within protections.

If a customer administrator makes changes to a profile, changes are saved in the CMA's local policy. If the Profile is later altered in the Global SmartDashboard, the customer administrator's changes will not be affected when Global Policy is reinstalled on the CMA.
Assigning Global Policy

Global Policy, which includes the Global Security Policy and Global IPS, should be assigned to Customers when it is first configured, and whenever you want to implement a change. All Global Policy assign operations are performed from the Global Policies - Security Policies and IPS view.

Assigning Global Policy for the First Time

To assign Global Policy for the first time:

1. From the Global Policies view of the MDG, select the target Customer.
2. From the Manage menu, select Assign/Install Global Policy.
3. In the Assign/Install Global Policy window, select a global policy from the list.

Note - To configure a Customer for IPS, see Subscribing Customers to IPS Service (on page 81).

Assigning Global Policies to VPN Communities

When assigning and/or reassigning global policies to VPN Communities, you should perform the following procedure to ensure that all participating gateway domains update each other correctly.

To assign global policies to VPN Communities:

1. Assign global policies to customers.
2. Using the CMA SmartDashboard for active customers, install policies and/or databases as required.
3. Reassign the global policy and install the most recent policy on all gateways.

Re-assigning Global Policies

Whenever you make changes to a global policy, you must re-assign it to the appropriate customer CMAs. This ensures that global policy changes are reflected in individual Customer networks.

Automatic Gateway Policy Installation

When re-assigning a global policy to CMAs, you have the option to automatically re-install the last policy installed on individual CMA gateways. This option ensures that changes made to the global policy are correctly updated at the gateway level.

The term ‘last policy installed’ on a gateway refers to the most recent version of the last policy installed on that gateway using SmartDashboard.
Important - Any gateway on which a policy has never been installed (such as a new gateway) will not be affected when re-assigning global policies. No policy will be installed automatically unless a policy has been previously installed on that gateway.

In order to ensure that policy installation on a given gateway occurs when re-assigning a global policy, you must first select and install a policy on that gateway using the CMA SmartDashboard.

Re-assigning Global Policy to an Individual Customer
To re-assign a Global Policy to an individual CMA:
1. From the Global Policy page in the MDG, right-click a Customer and select Reassign/Install Global Policy.
2. In the Reassign/Install Global Policy window, enable the Reassign Global Policy option.
3. If you wish to automatically install policies on CMA gateways, select one or more gateways from the list.
4. Click OK to finish.

Re-assigning Global Policies to Multiple Customers
You can also reassign Global Policies to multiple Customers at the same time.

To reassign a policy to multiple Customers,
1. From the Manage menu, select Reassign Global Policy and IPS to Customers. Alternatively, you can click the Reassign Global Policy toolbar icon.
2. Select the Customers to re-assign this global policy.
3. Enable the Install last Policy on all gateways of assigned Customers option, if you wish to automatically re-install the last policy installed on all gateways belonging to the selected customers.
4. Enable the **Install last IPS Sensor Policy on all IPS-1 Sensors of assigned Customers** option, if you wish to automatically re-install the last policy on all IPS-1 sensors belonging to the selected customer.

### Considerations For Global Policy Assignment

#### Introduction to Considerations for Global Policy Assignment

When assigning a Global Policy to one or more Customers, Global Objects are copied to the database of the Customer's CMA. Whether all the Global Objects in the database are copied, or only those related to the Global Policy, can be configured per Provider-1 Customer in the **Customer Configuration** window, (which can be accessed by selecting Manage > Configure when selecting a Customer in the **General-Customer Contents** view).

Rules belonging to the Global Policy package being assigned are added above and below the rules inside ALL local policies defined in that CMA database.

After the Global Policy is assigned, when issuing the "install policy" command for a CMA's gateways, the gateways will receive the most updated CMA policy containing the latest updates from the Global Policy. Changes may be made to a Global Policy, after which the Global Policy is reassigned to one or more Customers. When a Customer's CMA then installs the updated policy to the Customer gateways, any modifications to global and local objects/rules are updated on the selected gateways.

The assign and install procedure are two separate processes. The administrator can re-assign a Global Policy without installing a local policy to Customer gateways.

#### Assigning Policy for the First Time

Once you create a Customer's internal network, you will want to create a policy for the Customer. The first step may be creating a Global Policy template for general use by different types of Customer. This allows you a certain amount of flexibility in how you manage security policy assignment.

Global policies are designed in Global SmartDashboard, but the assign/install procedure is handled through the MDG. The MDG provides a **Global Policy** Mode which gives you a few options to handle the procedure of assigning Global Policies. The Global Policy is assigned to the Customer's CMA.

#### When You Change a Global Policy

If you change the Global Policy, you must reassign it to all Customers using this policy, and reinstall it onto the Customer's gateways.

Re-install the Customer's network policy to a Customer's gateways when:

- You have made changes to a Global Policy and reassigned it to the CMA, without installing the updated policy to the Customer's gateways **or**,
- When you have made changes to the Customer's network policy.
If you have network load considerations, rather than install the gateways all at once, you may prefer to perform the procedure in stages. You can re-install a current policy to Customers' gateways using the **Install Last Policy** command or to IPS-1 Sensors by selecting the **Install last IPS Sensor Policy on all IPS-1 Sensors of assigned Customers** option. You can also install on selected gateways by right clicking a Customer and selecting **Reassign/Install Global Policy**.

### Assigning a Different Global Policy

To assign a *different* Global Policy to a Customer, use the same procedure as for initially assigning a Global Policy to a Customer. The Global Policy is overwritten when a new one is assigned.

### Global Object Transfer Method

During Customer configuration, you define for each Customer how the Global Policy database will transfer objects during global security policy assignment (this is located in the **Add Customer Wizard — Assign Global Policy** tab). When Global Policies are assigned to CMAs, two methods can be used to transfer all the information to the CMA's database from the Global Policy database.

It is possible to assign *all* Global Objects when assigning the Global Policy to a CMA. Or it is possible to assign only objects *required* by the rule base of the Global Policy assigned to the CMA. This includes objects directly or indirectly referenced by rules, such as network objects contained in groups. Indirectly references objects will also be copied to the CMA's database, and the administrator will see them in both group and individually.

You can decide to change settings later, but be careful when changing settings. Consider the following scenario: a Customer assigns a Global Policy and transfers all the Global Objects. All objects are copied to the global database. When a Global Policy is re-assigned with just those objects relevant to the Global Policy assigned, extraneous objects not used by the Global Policy will be removed from the Customer's configuration database. However, if these objects are used by a Customer's network security rules or objects, the assignment operation will terminate (an error message lists the objects that prevented the operation from proceeding).

### Viewing the Status of Global Policy Assignments

You can view global policy assignments from the MDG while in the **Security Policies and IPS** mode in the **Global Policies** view.

In this window, each Customer is displayed under the Global Security Policy to which it is assigned, or under the category **No Global Policy**. The time and date at which the Global Policy was assigned to each Customer is reported, and a status indicator shows whether that assignment is the most up-to-date version of the Global Policy.

When a change is made in Global SmartDashboard, either to a Global Security Policy or to the Global IPS, the change will be reflected in the Global Policy state of each Customer assigned the relevant Policy. (A green check mark indicates that the Policy is up-to-date, while a red exclamation mark indicates that since the Policy was assigned, it has changed, and should be reassigned.)

### Global Policy History File

Each Customer's **log** directory includes a history file (named `gpolicy.log`) which maintains a summary of all actions taken by the Global SmartDashboard that affect the Customer. It records all actions taken, including assigning Global Policies to a CMA and installation on a remote gateway. The file includes time, operations performed, Global Objects added, and problems. To access this file, see Viewing the Customer's Global Policy History File (on page 89).
Configuration

Assigning or Installing a Global Policy

To assign, reassign, install or remove policies for Customers, you must be a Superuser (either a Customer Superuser or a Provider-1 Superuser). All these actions are performed in the MDG, using the Global Policies view.

You cannot assign a Global Policy to a Customer if a Read/Write SmartDashboard is logged in to the Customer's CMA. First, close SmartDashboard and then assign the Global Policy. You can, however, assign a Global Policy to a Customer if there is a Read Only SmartDashboard logged in to the CMA. The changes won’t be displayed in SmartDashboard until it is disconnected from and then reconnected to the CMA.

Assign to Many Customers: How To Assign/Install from a Global Policy Object

To Assign/Install from a Global Policy Object

Use the following method to create a Global Policy, then assign it to several Customers at once. You can also install a policy to all the Customers' gateways at the same time. If a Customer already has a different Global Policy, it is overwritten.

1. Select the desired Global Policy. Right-click the Global Policy and choose Assign/Install Global Policy from the options menu. Select the Global Policy Name of the Global Policy you want to install (for example, Standard_Global_Policy).
2. Select the Customers to which you want to assign this Global Policy from the Unassigned to selected Policy list. To install the policy on all the gateways of the Customers to which the policy is assigned, check Install Policy on assigned Customers.
   - To install a policy on specific gateways, perform the assign/install operation using the Customer object and select the specific gateways on which to install the policy.
3. Click OK. A Global Policy Assignment progress window lets you follow each step of the procedure, as the Global Policy is enforced on the selected Customer's CMAs. You can track installation attempts using the History file.

Assign to One Customer: Assign/Install from a Customer Object

To Assign/Install from a Customer Object:

Select a Customer that does not have a Global Policy, and assign one of the Global Policies you have created. This method gives you more control over the installation procedure for particular Customer gateways.

For Customers that already have a Global Policy, the option will be to Reassign/Install Global Policy.

1. Select a Customer, then choose Manage > Assign/Install Global Policy..., or right-click the Customer and select Assign/Install Global Policy...
2. The Assign/Install Global Policy window allows you to select the policy to be installed. Select one or more gateways. A policy must already have been installed on the gateways, or the operation will not work. Click OK.
3. The Global Policy is assigned to the Customer's CMA and the Customer policy is re-installed on the selected gateways.

Reassigning/Installing a Global Policy on Customers

Once a Customer has been assigned a Global Policy, it is possible to update the policy by re-assigning it.

To Reassign/Install a Global Policy for a Specific Customer who already has been Assigned a Global Policy

When performing a Reassign/Install the user does not choose the policy. The policy is already selected. You can also re-install the Customer policy to the Customers' gateways at the same time, but note that this
is for all the gateways at once and will only work if there is already a Customer policy resident on the gateway.

1. Select a Customer, then choose Manage > Reassign/Install Global Policy..., or right-click the Customer and select Reassign/Install Global Policy...
2. The Reassign/Install Global Policy window will display the policy currently installed.
3. Select the specific gateways for which to re-install the policy. Click OK. The Global Policy is assigned to the Customer's CMA and the resident Customer policy is re-installed on the selected gateways.

**To Reassign/Install a Global Policy for Multiple Customers**

1. Right-click a Global Policy and select Reassign/Install Global Policy from the options menu.
2. In the Reassign/Install Global Policy window, select on or more customers.
3. Enable the Install last Policy on all gateways of assigned Customers option, if you wish to automatically re-install the last policy installed on all gateways belonging to the selected customers.
4. Enable the Install last IPS Sensor Policy on all IPS-1 Sensors of assigned Customers option, if you wish to automatically re-install the last policy on all IPS-1 sensors belonging to the selected customer.

Reinstalling a Customer Policy on Customer Gateways

The Install Last Policy window allows you to select a group of Customers and re-install policies onto their gateways. You can use this method only if the selected gateways already have a policy installed.

**To Reinstall a Customer Policy on Customer gateways:**

1. From the Manage menu, select Reassign Global Policy and IPS to Customers. Alternatively, you can click the Reassign Global Policy toolbar icon.
2. In the Install Last Policy window, select the Customers to re-assign this global policy.
3. Enable the Install last Policy on all gateways of assigned Customers option, if you wish to automatically re-install the last policy installed on all gateways belonging to the selected customers.
4. Enable the **Install last IPS Sensor Policy on all IPS-1 Sensors of assigned Customers** option, if you wish to automatically re-install the last policy on all IPS-1 sensors belonging to the selected customer.

![Configuration Page](image)

The policy will be installed on *all* gateways for selected Customers.

### Remove a Global Policy from Multiple Customers

1. Select the Global Policy and choose **Manage > Remove Global Policy from Customers...**, or right-click the policy and select **Remove Global Policy from Customers...** from the right-click menu.
2. Check Customers in the **Assigned to selected Policy** list. To remove the policy from all Customers, click **Select All**. Customers from which the Global Policy has been removed are automatically assigned to the **No Global Policy** group.

### Remove a Global Policy from a Single Customer

To remove a Global Policy from only single Customer:

1. Select the Customer and right-click and choose **Manage > Remove Global Policy**, or choose **Remove Global Policy** from the **Manage**.
2. You are asked whether you are sure you want to remove this Customer from the Global Policy. Click **Yes** to confirm. The Customer is automatically assigned to **No_Global_Policy**.

### Viewing the Customer's Global Policy History File

To view the Customer's history file, select a Customer, right-click and choose **View History File...**, or from the **Manage**, select **View History File**.

### Global Policies Tab

The **Manage > Provider-1 Properties menu > Global Policies** tab allows you to specify how Global Policies are to be assigned to Customers and installed on their gateways.

### Policy Operation Options

- **Perform Policy operations on... Customers at a time** — each Policy operation is performed for a group (segment) of Customers at a time. This field allows you to specify the maximum number of Customers per segment. For example, if there are 5 Customers in the system and the segment number is 2, a Global Policy assign operation will be divided as follows:
a) The operation is performed on the CMAs of the first two Customers.
b) The operation is performed on the CMAs of the next two Customers.
c) The operation is performed on the CMA of the fifth Customer.

- **Install Security Policy only if it can be installed on all gateways** — specify that an installation succeeds only if the Policy is installed on each and every one of a Customer's gateways. If the installation on any of the gateways fails, then the whole installation fails and the previous Policy remains installed.

- **Install Security Policy on cluster, only if it can be installed on all cluster members** — for each cluster, the installation succeeds only if the Policy is installed on each and every cluster member. If the installation on any of the clusters members fails, then the whole installation for this cluster fails and the previous Policy remains installed. It is recommended that you enable this option.

**Global Names Format**

The Manage > Provider-1 Properties menu > Global Names Format window allows the user to define a template for Gateway Global Names, that consists of the original name of the gateway, the name of the Customer and other details. When enabling the gateways for Global Use, an automatic suggestion for an appropriate name will be offered, based on this template.

The configurable fields are:

- **Global Name** - A name is automatically suggested. You can use the default name suggested, which is in the format g<GATEWAY>_of_<CUSTOMER> where the name of the gateway and the Customer are the variables. For example, a template defined as g<GATEWAY>_of_<CUSTOMER> for gateway MyGateway of Customer MyCustomer, will result in the suggested name gMyGateway_of_MyCustomer.

  The global name should be self explanatory and easy to understand and therefore the template must consist of the Customer's name and the gateway's original name. The Administrator can later choose to override the template and create a Global Name which can be any unique legitimate string.

- **VPN Domains** - The additional configurable part of the template is the suffix for the VPN domain object. The template for the domain object contains the Global Name and the suffix. For example, if the defined suffix template is _Domain, the name of the VPN Domain will be gMyGateway_of_MyCustomer_Domain.
Chapter 6

Working in the Customer's Network

In This Chapter

- Overview .................................................................................................................. 91
- Installing and Configuring Security Gateways ....................................................... 92
- Managing Customer Policies .................................................................................... 93
- Working with CMAs and CLMs in the MDG .............................................................. 94

Overview

Management within the customer network is much the same for a Provider-1 customer as it is in the Security Gateway management model, but with a few key differences. In the Security Gateway management model, policy management is handled through the Security Management server. In the Provider-1 model, policy management is handled by the Customer Management Add-on (CMA).

Customer Management Add-on (CMA)

CMAs are the Provider-1 equivalent of Security Management servers, and support all Security Gateway features. Using the CMA, an administrator defines, edits and installs the customer's security and QoS policies to customer gateways. Each customer can have either one or more CMAs, where the second and subsequent CMAs are defined for High Availability purposes. In this case, one of the CMAs is defined as Active and the others as Standby.

In addition, a Security Management server can also be added as a backup of the Customer's CMAs.

Let's look at a deployment. The CMA (the Security Management equivalent) is located on the MDS within the Provider-1 network.

Figure 6-40 Customer network and service provider environment

Once you have created a Customer's CMA, you can start defining its policies, as described in the Security Management Administration Guide. Gateways are "defined" in the Provider-1 environment and managed via the Customer's CMA. VSX is described in the VSX Administration Guide.
Remember that routing must be set up to enable communication between Customer's gateways and the Customer's CMA(s). Traffic must be allowed between the Provider-1 management network gateway and Customer's gateways. It should also be enabled for SmartConsole Client applications and CMA connections. Access rules must be set up as appropriate in Customer gateways’ rule bases.

If Logging is set up for the Customer network, or High Availability is enabled, routing must support these functions. For further details, see Logging in Provider-1 (on page 119), and High Availability (on page 104).

Administrators

Administrators are assigned in a way that is slightly different to the way it is done in the Security Gateway management model, as it is centralized through the Provider-1 environment. Two types of administrators are assigned to manage specific Customers’ networks: Customer Managers and None administrators.

For details about the different types of administrators and their levels of system permissions, see Introduction (on page 8).

SmartConsole Client Applications

Administrators use the following SmartConsole Client applications to design, manage, monitor and log the Security Gateway enforcement policies:

- **SmartDashboard** is used by the system administrator to define and manage the Security Policy. From this SmartConsole you can create and define networks, gateways, hosts, user groups, services, and policy rules. You can also access many Check Point features and add-ons.

- **SmartView Tracker** is used for managing and tracking logs throughout the system.

- **SmartUpdate** is used to manage and maintain a license repository, as well as to facilitate upgrading Check Point software.

- **SecureClient Packaging Tool** is used to define user profiles for SecuRemote/SecureClient clients.

- **SmartView Monitor** is used to monitor and generate reports on traffic on interfaces, Provider-1 and QoS gateways, as well as on other Check Point System counters. It is also used for managing, viewing alerts and testing the status of various Check Point components throughout the system.

- **SmartReporter** is used to generate reports for different aspects of network activity. SmartReporter integration is described in Provisioning Provider-1 (on page 46) and in Logging in Provider-1 (on page 119).

- **SmartProvisioning** is used for managing large numbers of SmartLSM Security Gateways using Security Management server/CMAs.

For further information about the SmartConsole Clients, see the Security Management Administration Guide. To see how tools are used to monitor the Provider-1 environment, see Monitoring in Provider-1 (on page 127).

Installing and Configuring Security Gateways

The procedure for installing and licensing Security Gateways in customer networks is as described in the Security Management Administration Guide. Please refer to this guide for details. Check Point Security Gateway should be installed on customer gateways, without a Security Management server.
Managing Customer Policies

A customer CMA is similar to a `<tp_sgates>` in a Security Management Server deployment. You use SmartDashboard to create and configure network objects representing customer gateways, hosts, nodes, and groups. Furthermore, you create, maintain and install customer security policies using SmartDashboard.

You launch SmartDashboard for a specific customer directly from that customer's CMA. The procedures required to create, configure and manage network objects and security policies are described in the Security Management Administration Guide.

UTM-1 Edge Appliances

UTM-1 Edge management is integrated into CMA functionality.

Creating Customer Policies

Policies are used to enforce and protect communication. Administrators create customer policies for the gateways they manage, using SmartDashboard (as in the Security Gateway management model). There are a few important differences to be aware of. In the Provider-1 environment, global policies containing global rules are created for the entire Provider-1 system. These rules appear as part of the Customer's rule base, but cannot be edited.

When launching SmartDashboard from the CMA, the rule base that is displayed for the customer will include global rules that were assigned to the Customer. Global rules can appear either before or after the Customer rule base. These global rules cannot be edited except by Provider-1 superuser administrators.
Global Policies and the global rule base are described in greater detail in Global Policy Management (on page 72).

For general information regarding creating policies using SmartDashboard, see the Security Management Administration Guide.

Revision Control

You can configure a Customer to save a snapshot of its settings whenever policy is assigned or installed to it. This allows a Customer administrator to roll Security Management back to an earlier state, if necessary.

The property Create Database Version is located on the Assign Global Policy tab of the Customer Configuration wizard. While the default setting is not enabled, it is recommended to enable it if disk space is not an issue.

Working with CMAs and CLMs in the MDG

All activities such as creating, editing, deleting, starting and stopping CMAs and CLMs, can be performed by administrators using the Provider-1 MDG. These activities are described in Customer Management (on page 56), and in Logging in Provider-1 (on page 119).
Chapter 7

VPN in Provider-1

In This Chapter

Overview 95
VPN Connectivity in Provider-1 97
Global VPN Communities 100
Configuring Global VPN Communities 102

Overview

Branch offices need to connect with other branch offices. Partner sites also need to establish local and remote communication. Once connectivity has been established, the connections must remain secure, offering high levels of privacy, authentication, and integrity.

Only legitimate traffic must be allowed to enter a customer's internal network, and possibly harmful traffic must be inspected for content. Within the customer's internal network, different levels of access must also exist so that sensitive data is only available to the right people.

A Security Gateway at a network boundary acts as a gateway that inspects and provides access control for all traffic passing through the gateway. Traffic that does not pass through the gateway is not controlled.

Figure 7-41  A Security Gateway inspects all traffic that crosses it

The Security Gateway enforces a company's security policy. To achieve this, an enterprise-wide Security Policy Rule Base is defined at the CMA. SmartDashboard is used to install the policy, and distribute it to a Customer's gateways. VPN traffic management is controlled and enforced as part of the Security Policy Rule Base.

Access Control at the Network Boundary

Check Point Security Gateway provides secure access control through granular understanding of underlying services and applications traveling on the network. Stateful Inspection technology provides access control for more than 150 pre-defined applications, services and protocols as well as the ability to specify and define custom services. For more information about services and access control, see the IPS Administration Guide.
Authentication Between Gateways

Before gateways can exchange encryption keys and build VPN tunnels, they first need to authenticate to each other. Gateways authenticate to each other by presenting one of two types of "credentials":

- **Certificates.** Each gateway presents a certificate which contains identifying information of the gateway itself, and the gateway's public key, both of which are signed by the CMA's trusted CA.
- **Pre-shared secret.** A pre-shared can be defined for a pair of gateways. Each gateway must "prove" that it knows the agreed upon pre-shared secret. The pre-shared secret can be a mixture of letters and numbers.

Certificates are the preferred means and considered more secure. The Customer CMA's Internal CA automatically provides a certificate to each gateway it manages, so it is also more convenient to use this type of authentication.

More information about PKI and authentication procedures and methods are available in the VPN Administration Guide.

How VPN Works

A Virtual Private Network (VPN) is a network that employs encrypted tunnels to exchange securely protected data. VPN creates encrypted tunnels by using the Internet Key Exchange (IKE) and IP Security (IPSec) protocols. IKE creates the VPN tunnel, and this tunnel is used to transfer IPSec encoded data.

**Note - IKE & IPSec.** Refers to the secure VPN protocols used to manage encryption keys, and exchange encrypted packets.

**Encryption algorithm.** A set of mathematical processes for rendering information into a format which is incomprehensible. The mathematical transformations and conversions are controlled by a special key. In VPN, various encryption algorithms such as 3DES and AES ensure that only communicating peers are able to understand an encrypted message, using keys to decode the incomprehensible format into the original message.

IKE can be thought of as the process that builds a tunnel, and IPSec packets as "trucks" that carry the encrypted data along the tunnel, from the source gateway to the destination gateway.

For example, a Customer has two hosts (host1 and host6), who are behind different gateways, but need to communicate. Packets pass in the clear between host1 to the local gateway. Using the packet's source and destination addresses, the gateway determines that a connection should be established with a remote gateway. According to the rule base, the connection is permitted and should be encrypted.

If this is the first connection between the hosts, the gateway initiates an IKE negotiation with the peer gateway protecting host6. During the negotiation, both gateways authenticate each other, and agree on encryption methods and keys.

**Note - Key Exchange** is the process by which communicating parties negotiate the keys and methods for exchanging data. In a VPN, this negotiation takes place using the IKE protocol. Keys are used to transform a message into an incomprehensible format (encryption), and to decode the encrypted message back into the original message.

After a successful IKE negotiation, a VPN tunnel is created. From now on, every packet that passes between the gateways is encrypted according to the IPSec protocol. IKE supplies authenticity (so that gateways are sure they are communicating with each other) and creates the foundation for IPSec. Once the tunnel is created, IPSec provides privacy (through encryption) and integrity (via one-way hash functions).
**Note -**

**Endpoint Security.** Endpoint Security checks (via hash functions) ensure that the message has not been intercepted and altered during transmission.

**Trust.** Public key infrastructure (PKI), certificates and certificate authorities are employed to establish trust between gateways. Gateways "trust" that they are indeed communicating with each other, and not with an intruder, based on these methods that establish identity.

**Pre-shared Secret.** Secret data which gateways agree to employ to ensure that they are communicating with each other. In the absence of PKI, gateways employ a pre-shared secret to establish each other's identity, which is less secure than PKI.

Now host1 wants to speak to host8. After another IKE negotiation, host1 establishes a second VPN tunnel with the gateway protecting host8.

**Figure 7-42**  VPN tunnels established for host1

For each VPN tunnel, after it has been established, packets are dealt with in the following way:

- A packet leaves the source host and reaches the gateway.
- The gateway encrypts the packet.
- The packet goes down the VPN tunnel to the second gateway. The packets are actually standard IP packets passing through the Internet. However, because the packets are encrypted, they can be considered as passing through a private "virtual" tunnel.
- The second gateway decrypts the packet.
- The packet is delivered in the clear to the destination host. From the host's perspective, they are connecting directly.

**VPN Connectivity in Provider-1**

A VPN can be established between any type of VPN endpoint, such as a customer's Security Gateways, or clusters of Security Gateways. VPN trust is established via trusted entities, namely the certificates issued by a CMA's Internal Certificate Authority (ICA), external third party Certificate Authority servers (via OPSEC connectivity), or by pre-shared secrets.

Similar to the Security Management server, the CMA's ICA issues certificates that are used by the customer's network gateways to establish trusted SIC connections. The primary MDS Manager issues certificates to authenticate administrators.
VPN connectivity is the same whether run by Provider-1 or by Security Management. A new method is introduced to provide cross-Customer connectivity, namely the Global VPN Community. The procedure for establishing Global VPN Communities automates part of the step-by-step process of establishing Externally Managed gateways for each Security Management server and exchanging certificates manually.

Connections to a Customer Network

**Traditional VPN**

In Traditional VPN Mode, a single rule, with the Encrypt rule action, deals with both access control and encryption. VPN properties are defined for gateways in the regular rule base, and rules are per pair of gateways: source and destination.

An Encryption domain refers to the hosts behind the gateway. The Encryption domain can be the whole network that lies behind the gateway, or just a section of that network.

For example, one Customer's gateway might protect both the corporate LAN (Net_A and Net_B) and the DMZ (Net_C). However, only the corporate LAN is defined as the Encryption domain. The DMZ is not secured. Another gateway may protect a set of hosts, all of which are included in the Encryption domain (Net_D).

**Figure 7-43** A VPN between gateways, and the Encryption (VPN) Domain of each gateway

![Diagram of a VPN between gateways and Encryption Domains](image)

The following shows how VPN might be implemented in a Traditional Encrypt rule:

**Table 7-2** Sample Encrypt rule in a Traditional Rule Base

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>host1</td>
<td>host2</td>
<td>My_Services</td>
<td>Encrypt</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

VPN is established between two gateways managed by the same CMA, in the same way that is done between Security Gateways managed by a standalone Security Management server. Using SmartDashboard launched from the CMA, customer gateways are configured to route VPN traffic. More information about Traditional VPN is available in the **VPN Administration Guide**.

**Simplified VPN**

In Simplified VPN Mode, the security rule base deals only with access control. VPN properties, on the other hand, are dealt with per **VPN community**. A VPN community is defined in SmartDashboard, and is a group of gateways. (In Traditional VPN, communication is defined for a pair of gateways.) The community definition also specifies encryption methods for VPN.
Once a community is established, all communication between community members is encrypted. Communication with outside gateways is not encrypted. To better understand VPN Communities, a number of terms are defined here:

- **VPN Community member** refers to the gateway at each end of a VPN tunnel.
- **VPN domain** refers to the hosts behind the gateway. (In Traditional VPN, this domain is called the Encryption domain.)
- **VPN Site** is a community member plus VPN domain. A typical VPN site would be the branch office of a bank.
- **VPN Community** is the collection of VPN tunnels/links and their attributes.

Figure 7-44 VPN entities

Simplified VPN Mode and communities are described in the **VPN Administration Guide**. As with a standalone Security Management server, an administrator establishes VPN between a single Customer's gateways by defining it via the CMA's SmartDashboard.

A simplified VPN policy makes it easier for the administrator to configure VPN. However, Traditional policies allow VPNs to be created with greater granularity than Simplified policies, because it defines whether or not to encrypt can be defined per rule (source, destination and service). Simplified policies require all the connections between two gateways to be encrypted using the same methods, via a unitary Community definition.

A Traditional VPN implementation can be converted to Simplified mode via a wizard. Because of the granularity of Traditional VPN, after running the wizard, some manual optimization of the rule base may be required.

**Conversion Considerations**

When a Traditional policy is converted to a Simplified policy, an Encrypt rule is converted to community rule. In order to understand the conversion, it is important to understand how an Encrypt rule works. These issues are described in the **VPN Administration Guide**.
Global VPN Communities

Sometimes customers need to establish VPN between gateways that are managed by different CMAs. This might happen, for example, in large enterprises that have created different CMAs to manage corporate networks in different cities or countries. Or, an MSP deployment may require communication between partners, managed as different customers.

Cross-customer VPN is handled by establishing Global VPN Communities. This community is similar to the regular VPN community with the exception that it can deal with gateways managed by different CMAs. An administrator establishes VPN between a single Customer's gateways by defining it via the CMA's SmartDashboard. A Global VPN Community however is defined at the Provider-1 level, using MDG and Global SmartDashboard.

Provider-1 utilizes its knowledge about different customer network environments to ease the definition of VPN for environments run by different CMAs. In the standalone model, cross-customer VPN is established by creating gateways that are defined as externally managed gateway objects. Then certificates and network information are imported into each gateway's Security Management server databases.

In Provider-1, during the Global VPN Community setup, the MDS Manager automatically exports relevant ICA information (such as the CA certificate) for each customer's CMA, so that both sides can trust the other's ICA.

Gateway Global Names

One Customer's gateways are not "known" to CMAs of other customers. (This ensures privacy, and the integrity of each customer's security.) In order for CMAs to "recognize" another Customer's gateway, the gateway must first be enabled for global use, which "promotes" the gateway object from the customer level to the Provider-1 level.

In order to establish cross-customer VPN, "global gateway objects" are created in the global policy database. A global gateway object is also known as a Neighbor VPN Object. A Customer's gateway is "promoted" to be a Neighbor VPN Object. It can then participate in a Global VPN Community.

Different customers may coincidentally name their gateways with the same name (i.e. ftp_gateway). Since each global gateway object must have its own unique Global Name, the Provider-1 uses a Global Names Template, which automatically suggests a unique name. The default format includes the customer name using the format: g<GATEWAY>_of_<CUSTOMER>.

For example, the BigBank enterprise has a London branch, whose Security Gateway is named "London_gw." Its Customer is named BigBankUK. Martin, the Provider-1 Superuser administrator, wants to change the default template to add UK (country) at the end.

In MDG, via Manage > Provider-1 Properties, in the Global Names Format tab, Martin specifies that the template should use the gateway and customer name and country name, as follows: g<GATEWAY>_of_<CUSTOMER>_of_<COUNTRY>. When Martin goes through the process of enabling the gateway for global use, the template automatically names the gateway gLondon_gw_of_BigBankUK.

Once a gateway is enabled for global VPN and given a unique name, it appears in the Global Policy.

The templates for global names of gateways and global names of VPN Domain objects can be defined in MDG, via Manage > Provider-1 Properties.

Global or Neighbor VPN Gateway

For Global VPN Communities, VPN tunnels are created between Neighbor VPN gateways. (In a Security Management deployment, this is known as an externally managed gateway, or a gateway managed by a different Security Management server.

The neighboring gateway supports certificates issued by the other Customer's CA. Both gateways need to trust the other's CA.
VPN Domains in Global VPN

The administrator defines each Customer gateway via SmartDashboard. When defining if the gateway is a VPN gateway, the administrator specifies whether the VPN Domain is to be based on the network's topology or a specific address range.

This type of network information is managed at the individual Customer's network level. The information resides in the CMA's customer network information and is centralized in the CMA database. For VPN between a single customer's Security Gateways, the VPN domain is flexible and can be defined by the Customer's administrator.

CMA databases would have to maintain complete data on all other customer networks, which could also be a security breach. Instead, Provider-1 computes address ranges from those specified in VPN gateway properties. It uses this list as the base for the VPN domain of a particular gateway from another customer's 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 gateways for a customer's Global VPN Community does not create a de facto access control policy between the gateways. The fact that two gateways belong to the same VPN community does not mean the gateways have access to each other.

The configuration of the gateways into a Global VPN Community means that if these gateways are allowed to communicate via 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. **VPN is another level of security separate from the access control level.**

Access Control in Global VPN

Access control for global communities VPN is the same as for a single customer's VPN community. Namely:

- If 'Accept all encrypted connections' is enabled, the appropriate implied VPN rules appear in the policies of relevant CMAs.
- Add the community in the 'VPN' tab of a rule.

Information about access control for VPN communities is available in the **VPN Administration Guide**.

Joining a Gateway to a Global VPN Community

There are several steps necessary to join a customer's gateway to a Global VPN Community. First, each customer's gateway must be enabled for global use. Then a VPN Community must be defined in Global SmartDashboard, including the global gateway objects representing participating customers' gateways.

Lastly, a Global Policy must be assigned to participating customers' CMAs, and installed on the customer's gateway, for each customer and gateway participating in the VPN Community. **All** 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 Customers, global objects are copied to the database of the Customer’s CMA. Whether all the global objects in the database are copied, or only those related to the global policy, is configurable per Customer using the Customer 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 CMA database.

For more information about global policies, see Global Policy Management (on page 72).

**Considerations**

After the global policy is assigned, when issuing the "install policy" command for a CMA's gateways, the gateways will receive the most updated CMA policy containing the latest updates from the Global Policy. Changes may be made to a global policy, after which the global policy is reassigned to one of more Customers. When a Customer's CMA then installs the updated policy to the Customer gateways, any modifications to global and local objects/ rules are updated on the selected gateways.

The assign and install procedure are two separate processes. The administrator can re-assign a global policy without installing a local policy to Customer gateways.

During the re-assign operation, gateways that participate in Global VPN Communities are provided the CA certificate for other Customers participating in the community. Certificates are automatically installed in the certificate database of the CMA assigned a global policy.

For each participating Customer, other than the CMA's Customer, a global "CA Server" object is created in the CMA's database, representing the certificate authority of the peer Customer. The existence of this object allows for authentication by 'Matching Criteria' to work. If by chance the certificate of the peer Customer has already been imported manually into the database, the 'Matching Criteria' references the existing certificate.

### Configuring Global VPN Communities

#### Enabling a Customer 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.

The procedure to join a Global VPN Community is described below.

**Step 1 - In the MDG**

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

1. In the **General View - Customer Contents** Mode (or **Network Objects** Mode) right click a customer's gateway and select **Enable for Global Use** (or **Manage > Enable for Global Use**). You will be required to provide a **Global Name** for the gateway.

   A global gateway object and a VPN Domain object are created for the customer gateway in the Global Database.

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

**Step 2 - In Global SmartDashboard**

1. Define a Global Site-to-Site VPN Community.

2. Add the global gateway objects, defined in step 1, as participating gateways in this community.

3. Define global rules as needed for the new Global VPN Community, the global gateway objects, and the External Domains.
Step 3 - In the MDG

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

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

To assign to one customer 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 customer and select Reassign/Install Global Policy.... Select the customer gateways to which the policy should be installed. The policy is assigned to the CMA database, then to the selected customer gateways.

or

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

or

To assign to many customers 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 customers selected, then installs the policy to the customers' gateways, in one go. It does not allow you to select specific gateways to which to install the policy. If chosen, the policy will be installed to all of the gateways for the selected Customers. Assigning the policy to many Customers and all their gateways may take some time. Use this option with caution.

You can now create security rules regarding VPN via SmartDashboard for a customer's CMA. Gateways which are external to a customer but are part of the Global VPN Community, will appear as global externally managed gateway objects in the CMA's SmartDashboard.

The customer's own participating gateways will appear as they usually do. It is not necessary to define authentication for the external global gateway objects. Matching criteria are automatically defined for the global gateway objects referring to the other CMA's Certificate Authority.

A Customer can be assigned a Global Policy which references a Global VPN Community, in which, however, none of the Customer's gateways participate. If this happens, the CMA database will have an empty community (without community members).
Chapter 8

High Availability

In This Chapter

Overview 104
CMA High Availability 104
MDS High Availability 108
Configuration 114
Failure Recovery in High Availability Deployments 117

Overview

Provider-1 supports High Availability — a Check Point feature that ensures uninterrupted service availability in case of a computer crash. Provider-1 implements High Availability at three levels:

- The gateway level, such as through ClusterXL.
- The CMA level: multiple CMAs (one Active, and at least one Standby) are supported, as is one Security Management backup server, per Customer.
- The MDS level, through MDS synchronization.

By using ClusterXL, Customer networks are protected in the event of a gateway computer failure. Customers may choose to implement gateway clustering within their network environments, using SmartDashboard to configure the system. CMAs support cluster gateway management.

An administrator can implement failover gateway management for a Customer network by creating multiple CMAs, configured to High Availability. These CMAs regularly synchronize their databases, at a configurable interval or specified event (such as saving or installing a policy). One CMA is Active, while the others are Standby. Further High Availability can be achieved by installing a Security Management backup server, which can take over if all CMAs fail.

Note - The current Provider-1 version supports more than two CMAs per Customer. In versions NGX R65 and earlier, only two CMAs are supported per Customer; one Active and one Standby.

The MDS Manager is the point of entry to the Provider-1 system. Any Manager can serve as a point of entry: if one fails for any reason, another can be used as an access point for system management. Managers are configurable to regularly synchronize their databases, so that if one fails, others contain updated data regarding the system. It is possible to set up MDS Container mirror sites, so that Containers are mirrored.

CMA High Availability

Implementing CMA High Availability guarantees management failover capability for a Customer network. At any given time, one gateway management (CMA) is Active while at least one is in Standby mode. Data synchronization between the CMAs greatly improves fault tolerance and enables the administrator to seamlessly activate a Standby CMA when required.

With High Availability, should a CMA fail for any reason, a Standby CMA can seamlessly continue operation. The High Availability scheme requires one Primary CMA and one Secondary CMA, which are housed separately, on different MDS Containers.
Note - MDSs may use different operating systems. All MDSs in the Provider-1 environment must be running the same version of Provider-1.

Two or more CMAs can be created at the same time, or a secondary CMA may be added at a later point. After a secondary CMA has been properly initialized and synchronized, no functional differences exist between the CMAs. Each CMA must be on a different Container. The same Container cannot contain two CMA's belonging to the same Customer.

It is possible to set up one Container with primary CMAs, and other Containers to contain all of the secondary CMAs. This is called a "mirror system" and is explained later in this chapter. This can be a useful solution for a service provider, which concentrates all resources in a network operations center.

It is also possible to use a Security Management backup server that will allow a Security Management server to have Management HA relations with a Provider-1 Customer.

It is not necessary to dedicate a Container to hold only secondary CMAs, a Container can hold a mix of primary and secondary CMAs, as long as they are for different Customers. Provider-1 provides this functional flexibility to support different setup needs. An international corporate network may need to have a mixture of management and backup capabilities that are quite different from those of a large-scale local service provider.

For example, a corporate bank with numerous branches finds it useful to have Active CMAs for local branches maintained on a Container in the area's central branch. The Standby (High Availability) CMAs are maintained on the MDS in another area's central branch.

By contrast, an MSP does not mix Active and Standby CMAs to support widespread distribution needs. The MSP implements a single, remote, mirror site for disaster recovery (see MDS Mirror Site (on page 108)).

To see how this works with two Containers, look at the example below. The Active CMA for a bank's Chicago network is housed on the Chicago MDS. The Active CMA for the Atlanta network is housed on the Atlanta MDS. Each of the Standby CMAs, however, are housed at the other location's MDS.

Figure 8-45  CMA High Availability in an Enterprise network
To look at a more distributed example, let's examine a medical supplies firm that has many offices, which want partial failover capabilities. They have MDSs in three branches: Kansas, Osaka, and Montenegro. Each MDS has a mix of Active and Standby CMAs. Mission critical networks have CMAs with High Availability (CMA 1,3,6), while others do not (CMA 2,4,5,7,8).

**Figure 8-46** CMA High Availability in an Enterprise network

Administrators make security policy changes through the Active CMA, not the Standby. CMA updates are made through the CMA SmartDashboard. If policy changes are made with the Active CMA, the Standby CMA is synchronized automatically to reflect these changes (unless configured otherwise, i.e. manually synchronized).

**Active Versus Standby**

All management operations such as editing and installing the Security Policy and modifying users and objects, are done by the Active Management server. If the Active Management server is unavailable, and any of the aforementioned operations need to be performed, one of the Standby Management servers should be made Active. This transition from Standby to Active should be **initiated manually**.

The Standby Management servers are synchronized to the Active Management server, and therefore, are kept up to date with all changes in the databases and Security Policy. Thus gateways can fetch the Security Policy and retrieve a CRL from both the Active Management server and the Standby Management servers.

The frequency of the synchronization between the Standby Management servers and the Active Management server is set by the System Administrator. This process can be configured to take place automatically, or it can be set to occur manually.

It is possible to configure the High Availability feature to synchronize automatically for each policy installation operation, on each policy save operation and on any other scheduled event. If the Standby Management server's data has not been synchronized with the Active Management server, you can still use the Standby Management server, which is updated until the moment of the last synchronization.

The terms "Active" and "Standby" are not the same as the terms "Primary CMA" and "Secondary CMA," which have to do with the chronological order of creation. Either CMA can be set up to be Active or Standby. Initially, the Primary CMA (the first one created) is the Active one, but later on the administrator can manually change this as needed.

**Setting up a Mirror CMA**

When you add a Mirror CMA through the MDG, Provider-1 performs a series of automatic operations (no user intervention is required), as below:

1. Creates the CMA on the MDS selected. Copies the Certificate Authority (CA) files of the primary CMA to the mirror CMA.
2. Starts the mirror CMA and exchanges the activation key between the two CMAs. Then initializes SIC communication between the two CMAs.
3. Synchronizes the mirror CMA with the primary CMA. At this stage, both CMAs are running (if the primary CMA is down, the system will automatically attempt to start it).

If the operation fails at stage 2 or 3, the administrator can complete these stages manually.
See Mirroring CMAs with mdscmd (on page 116) for instructions on mirroring CMAs using the CLI.

CMA Backup using Security Management Server

Security Management backup server is able to backup a specific Provider-1 Customer CMA or a High Availability CMA as described above, and can function as an Active/Standby management. For example:

- The Security Management backup server is the Standby management and the CMA server is the Active management. When the CMA server is unavailable, the Security Management backup server can become the Active management.

- The CMA server is the Standby management and the Security Management backup server is the Active management. When the Security Management backup server is unavailable, the CMA server can become the Active management.

  **Note** - A Security Management backup server cannot be installed on Windows or Nokia IPSO platforms.

GUI Clients and Administrators definitions are separate for the CMAs and for the Security Management backup server.

GUI Clients and Administrators that were defined on the Provider-1 server are not automatically used on the Security Management backup server and vice versa.

**Figure 8-47**  Security Management backup server

---

**Security Management backup server Setup Procedure**

To perform a Security Management backup server fresh installation:

2. Use `cpconfig` to configure the following:
   a) Select an activation key that will be used to establish secure internal communication (SIC) between the Security Management server and CMA.
   b) Define GUI Clients and Administrators.
3. In SmartDashboard connected to the Provider-1 CMA, create a network object that will represent the secondary Security Management backup server.
   a) Select Manage > Network Objects > Check Point > New > Host
   b) In the Check Point Host window, check Secondary Management Station under Check Point Products. This automatically selects Log Server as well.
4. From the object created in step 3 establish secure communication with the secondary Security Management backup server.

5. From SmartDashboard access the **Policy** menu, select **Management High Availability** and press the **Synchronize** button.

**To setup a Security Management backup server from an existing Security Management server:**

1. Migrate the existing Security Management server to the Provider-1 CMA using the tools in "Upgrading Provider-1" of the R70 Upgrade Guide.

2. Perform a fresh Security Management server installation as a secondary Security Management server on an existing or new machine.

3. Using `cpconfig` to select an activation key that will be used to establish secure internal communication (SIC) between the CMA and Security Management.

4. Create a network object in the Provider-1 CMA that will represent the secondary Security Management backup server.
   a) Select Manage > Network Objects > Check Point > New > Host
   b) In the Check Point Host window, check Secondary Management Station under Check Point Products. This automatically selects Log Server as well.

5. From the object created in step 4 establish secure communication with the secondary Security Management backup server.

6. From SmartDashboard access the **Policy** menu, select **Management High Availability** and press the **Synchronize** button.

**MDS High Availability**

**MDS Mirror Site**

It is possible to mirror an entire MDS, using a second MDS. For all CMAs on the first MDS Manager/Container, High Availability CMAs can be created on a second MDS Manager/Container. By default, when changes are made to the CMAs in the first Container, the system synchronizes the Active CMAs with the Standby CMAs. The two MDS Managers are automatically synchronized also. However, CMA synchronization can be set up to occur at specified events, such as every time a Customer's policy is saved, or when it is installed onto one or more Customer gateways.

**Figure 8-48** Mirror MDS/CMA system
MDS Managers

MDS Managers are "mirrors" of each other. If there is more than one MDS Manager in the system, each Manager will contain all the information regarding the Provider-1 management system such as the network setup, administrator hierarchy, selected customer and network information.

MDS Manager synchronization does not mirror CMA-specific data. For example, internal domains and customer level policy rules are known only at the CMA level, so they are not synced by MDS Managers.

Interconnected, mutually redundant MDS Managers form a robust management system providing non-stop access, without the need to deploy dedicated hardware or software redundancy. For MDSs, the Active/Standby status affects only the login to the Global SmartDashboard (as opposed to the login to the MDG). MDG management activities can be performed using any of the MDS Managers.

Figure 8-49 MDS Synchronization in an Enterprise network

In terms of using MDGs, all MDS Managers are simultaneously accessible and can perform Read/Write operations at all times, except for creating/revoking MDS certificates in the MDS Configuration window, which can only be done from the Active MDS. MDS information is synchronized at configurable intervals.

Setting up a New MDS and Initiating Synchronization

MDS Clock Synchronization

For proper MDS synchronization, all MDSs' system clocks must be synchronized, as the synchronization method relates to time of modification.

The time of modification is written using UTC (Universal Time Coordinated), used by MDSs' system clocks. The administrator can synchronize MDS clocks using available synchronization utilities. Resetting regularly to compensate for clock drift is strongly recommended. Correct database synchronization requires that the MDS clocks are synchronized to the second. It is therefore recommended that MDS clocks be synchronized automatically at least once a day.

Whenever a new MDS is defined in the MDG, it must receive a certificate and communication must be established with the new MDS. The MDS also needs to be synchronized in time with the other MDSs. The MDG guides the user through the stages of performing this initial synchronization.

MDS: Active or Standby

Provider-1 MDS High Availability means that all MDS Managers are accessible at all times, in the sense that they are all equally available to an MDG as entry points to the Provider-1 system. However, only one MDS Manager at a time can be Active in the following respects:

- The administrator can log into the Global SmartDashboard with Read/Write permissions from the MDS.
• The MDS acts as the MDS Certificate Authority.

When the first MDS Manager is created, its status is automatically **Active**. Any further MDS Managers that are created will be Standby. Each MDS’s **Active/Standby** status is displayed in the **High Availability View - MDS Contents** Mode.

The MDS Active/Standby status can be changed, so that a different Manager can be chosen to be Active. Should the Active Manager fail for any reason, another Manager can thus be selected as the Active Manager. All other Managers will then become Standby.

### The MDS Manager's Databases

The MDS Manager's stored data is divided into three databases: MDS, Global Policies and ICA. The content and synchronization method of each database is described below.

**MDS Database**

This database holds data objects describing MDSs, Customers, CMAs, gateways, licenses, administrators, GUI-clients, and information about assignment of Global Policies to customers. This database is synchronized automatically between MDS Managers. MDS Containers also contain parts of this database, which is synchronized for proper operation.

The synchronization method of this database enables simultaneously opening MDGs to different MDS Managers, and performing Read and Write operations at any time from any MDG. Changes committed to the database of one MDS Manager are distributed immediately to all other MDS Managers, and to the MDGs connected to them as well.

If MDSs were disconnected from each other, it is recommended to make changes only on one of them, to avoid data collision. Once the MDSs are reconnected, they will synchronize with each other according to modification time.

**Global Policies Database**

This database holds the global objects (network objects, services, servers, etc.) and global rules. In terms of the Global Policies database, one of the MDS Managers is Active (the first logged into), while the rest are Standby.

Some operations can only be performed on the Active MDS, such as opening a Read/Write Global SmartDashboard. It is possible to open Global SmartDashboard in read-only mode on a Standby MDS.

**ICA (Internal Certificate Authority) Database for MDSs**

This database holds certificates for MDSs, administrators and CRLs (certificate revocation lists). Each MDS has a certificate issued by the MDS ICA that is used for secure communication with other MDSs. This database is synchronized whenever the Global Policy database is synchronized. Only the Active MDS can issue and revoke certificates for MDSs. When a Standby MDS Manager is made Active, its ICA also becomes "Active."

### The MDS Container's Databases

The MDS Container also stores data, including MDS and Global Policies database information, at the MDS level. Databases at the CMA level are stored separately **per Customer**. Customer policies, the Customer's ICA, and CMA-specific information are stored at the CMA level.

The MDS Container does not hold the MDS ICA database. It does hold CMA ICA databases, one per Customer. If a Customer has High Availability, both CMAs share the **same** CMA ICA, so that they can communicate securely with the Customer's network gateways using the **same** certificates.

**ICA (Internal Certificate Authority) Database for CMAs**

This database holds certificates for the Customer's CMA(s) and gateways. Each Customer’s gateway has a certificate issued by the CMA ICA that is used for secure communication between the CMA and gateway,
and between gateways. Only the Active CMA can issue and revoke certificates for the Customer’s gateways. When a Standby CMA (the High Availability CMA) is made Active, its ICA also becomes “Active.”

**How Synchronization Works**

**MDS Database Synchronization**

MDS database synchronization occurs automatically whenever an object is changed. The MDS databases are synchronized for the specific object change.

For example, if a new administrator is added to the system, all MDSs will be updated with this information. In this system, with an MDS Manager/Container and an MDS Container, the MDS database must be synchronized between the Manager/Container and Container so that they are both contain information about the Administrator’s existence.

**MDS ICA Database Synchronization**

If a new MDS is added to the system, the MDS ICA must issue a certificate to the new MDS. If a new administrator is added to the system, the MDS ICA may issue a certificate to the new administrator, depending on the administrator’s authentication method. The MDS ICA database is updated. If there is more than one MDS Manager in the system, the MDS Manager’s ICA databases must be synchronized to reflect these additions.

Let us say that when a new administrator is added to the system, she is issued a certificate from the MDS ICA, which she will use at MDG login to authenticate her identity.

If there is more than one MDS Manager in the system, the MDS Manager’s ICA databases are synchronized to reflect this update. But in this system, as there is only one MDS Manager (the MDS Manager/Container), there is no need for MDS ICA synchronization. The MDS Container does not hold the MDS ICA database.

**Global Policies Database Synchronization**

Global Policies data synchronization occurs either when the global policy is saved, or at another defined event (for details about synchronization settings, see Automatic Synchronization for Global Policies Databases (on page 115)). Unlike the MDS database synchronization, which is per object, the entire contents of the Global Policies database are synchronized.
For example, if a new Global Policy is defined, all MDSs will be updated with this information. In this system, containing an MDS Manager/Container and an MDS Container, the Global Policies databases are synchronized so that they both contain information about the new Global Policy.

**Figure 8-51** Global Policies database synchronization

CMA Database Synchronization

For Customers with High Availability, data synchronization occurs per Customer. The CMAs for each Customer are synchronized when a Customer policy is saved, or at another defined event (for details about synchronization settings, see Automatic CMA Synchronization (on page 116)). The entire contents of the CMA database are synchronized.

Different Customers may have different synchronization settings. This means that different Customer's CMAs synchronize according to the specific settings for that Customer only. When information is changed or updated for a Customer, if the Customer has High Availability, all CMAs must receive the new information. For example, if a gateway is added to a Customer's network, and the gateway receives a certificate from the Customer's ICA, this information must be synchronized between all of the Customer's CMAs.

**Figure 8-52** CMA database synchronization
Cross-MDS Synchronization

All of these synchronizations take place according to individual synchronization settings or conditions, even though they may take place on the same machines.

Figure 8-53  MDS and CMA level synchronizations between two MDSs

Setting up Synchronization

Using the MDG to Synchronize the MDSs

Provider-1 High Availability is managed through the MDG's High Availability View. The administrator can perform all management High Availability activities through this view, and view the status of these actions after a configurable delay.

The Sync Status displays synchronization statuses for MDSs and CMAs. Every synchronization takes a certain amount of time to update the status. The default is 5 minutes. Statuses are as follows:

- **Unknown** — No information has been received about this CMA/MDS (see footnote ("Footnotes:" on page 114)) synchronization status.
- **Never synced** — This CMA/MDS has never been synchronized with the other CMA/MDS to which the MDG is connected.
• **Synchronized** — This CMA/MDS (see footnote "Footnotes:" on page 114) is synchronized with the other CMA/MDS to which the MDG is connected.

• **Lagging** — The data of this CMA/MDS (see footnote "Footnotes:" on page 114) is less updated than the data of the other CMA/MDS to which the MDG is connected.

• **Advanced** — The data of this CMA/MDS (see footnote "Footnotes:" on page 114) is more updated than the data of the other CMA/MDS to which the MDG is connected.

• **Collision** — The data of this CMA/MDS (see footnote "Footnotes:" on page 114) conflicts with the data of the other CMA/MDS to which the MDG is connected.

**Footnotes:**
1. When dealing with MDS synchronization status, the status is relevant for the Global Policies database. The ICA database is synchronized automatically between MDSs when new certificates are created for administrators/MDSs/MLMs, but when the database is modified as a result from operations in Global SmartDashboard, it will be synchronized with the next Global Policies database synchronization.

**Configuration**

**Adding another MDS**

The following steps are described in greater detail in the section Creating a Primary MDS Manager (on page 47).

1. Synchronize the system clock of the new MDS computer with all other MDSs computers’ system clocks.
2. Run the MDS installation script to install the MDS. When you are asked if this is an MDS Manager or Container MDS, select the type of MDS you want to add.
3. If you set up an MDS Manager, when you are asked if this is the Primary MDS, answer No.
4. During the configuration phase add an MDS license, and the **Activation Key** (password). This **Activation Key** is for passing the SIC certificate to the new MDS from the primary MDS.
5. In the MDG connected to the first MDS, define a new MDS. Assign it the IP address of the Leading Interface you selected for it in the configuration phase. Send the new MDS a certificate by the Initialize Communication option. Use the same **Activation Key** you entered in the configuration of the new MDS.
6. You will be prompted to perform an "Initial synchronization" for this MDS. Select to do so. Your new MDS Manager is now ready. You can connect directly to it with the MDG client.

**Creating a Mirror of an Existing MDS**

Mirroring an existing MDS means creating a duplicate MDS, with all information synchronized from the original MDS. The duplicate can be a Container or Manager/Container. Whether or not to create another Manager depends on how many access points are required for the Provider-1 system setup. The mirroring applies to both the MDS data and the data of the CMAs that it maintains.

**To mirror an existing MDS:**

1. Set up route tables.
2. Synchronize the system clock of the computer on which you will install the MDS with all other MDSs.
3. Install and create a new MDS Container or Manager/Container. Define the new MDS through the MDG connected to the Active MDS Manager, and perform initial synchronization. (See Initializing Synchronization between MDSs (on page 115).) The MDG must be connected to an Active MDS Manager so that the Manager can pass a SIC certificate. The MDS database will be synchronized.
4. To complete the synchronization, run this utility:
   ```
   mdscmd mirrorcma <-s source MDS> <-t target MDS> [-m MDS server -u user -p password]
   -s source_mds stands for the source MDS's name
   -t target_mds stands for the mirror MDS's name
   -m mds server stands for another MDS logged into to perform this action, and -u user -p password are the login user name and password. Note that -m, -u and -p are optional, but if used, must be used together.
   ```
This command will synchronize the data of all the CMAs maintained by the source MDS. In fact, a duplicate (Mirror) CMA will be created for each CMA in the original MDS. For further details, review this command in Commands and Utilities (on page 148).

**Initializing Synchronization between MDSs**

This step can be performed in the MDS Configuration window while creating the MDS. Or it can be done later after the MDS is created, through the MDG's High Availability View, as follows:

1. Verify that the Sync Status status of the MDS whose synchronization you want to initialize is Never synced.
2. Ensure that SIC has been established between the two MDSs.
3. Right-click the MDS, then select Initialize Synchronization, or select Initialize Synchronization from the Manage menu. The Status Report window is displayed, showing whether synchronization initialization succeeded or failed.

**Subsequent Synchronization for MDSs**

If you have already initialized the synchronization of an MDS, but at some point the synchronization encountered problems, you can synchronize the MDS once again through the High Availability View - MDS Contents mode.

You can either select a single MDS and synchronize it with the MDS Manager you logged into; or select a group of MDSs and synchronize all of them with each other.

**To Synchronize a Single MDS with an MDS Manager**

1. Select the MDS you want to synchronize with the MDS Manager you logged into. Check that its Sync.Status is other than Never synced or Unknown.
2. Right-click the MDS and select Synchronize, or select Synchronize from the Manage menu.

**To Synchronize a Group of MDSs**

Choose Select and Synchronize from the Manage menu. The Multi Domain Server Synchronization window is displayed, in which you to select which MDSs are to be synchronized.

**Selecting a Different MDS to be the Active MDS**

If the Active/Standby status of the MDS Manager is Standby, you can use the Change Over command to change its status to Active. Once you change the status there is a delay (by default 5 minutes) until the status is updated.

**To Change the Active MDS**

1. Ensure that you are not logged into Global SmartDashboard (except in Read-only mode).
2. Select the MDS Manager you want to make Active.
3. Select Change Over from the Manage menu.
4. The status will be changed to Active. The statuses of all other MDS Managers in the system will be Standby.

**Automatic Synchronization for Global Policies Databases**

The Global Policies database synchronization method is selected in the Global SmartDashboard (Policy > Global properties > Management High Availability menu).

The following options are available:

**On Save** - after the Save operation in the Global SmartDashboard, the database is synchronized to other MDS Managers and container MDSs as well.
Scheduled - you can select a scheduled synchronization (for example, once a day at a certain time). Use local time for the scheduled event.

On Save and Scheduled can be selected simultaneously, or none of the options can be selected.

### Add a Secondary CMA

Add a CMA through the MDG. A customer must have at least one CMA before a secondary CMA can be added to it. The secondary CMA must be created on a different MDS. Ensure that the primary CMA’s SmartDashboard is closed. This procedure is described in more detail in Customer Management (on page 56), in the section Configuration (on page 66).

**To add a secondary CMA:**

1. In the MDG Customer View, select a customer, then select Add Customer Management Add-on/Add Customer Log Module from the Manage menu, or right-click the customer and select Add Customer Management Add-on/Add Customer Log Module.
2. You are required to complete the fields shown. Enter a name for the CMA which does not contain any spaces. Select the Container MDS on which this CMA will be maintained.
3. Next, fill in the license information.

### Mirroring CMAs with mdscmd

Use the `mdscmd mirorcma` command to mirror all CMAs on one MDS to another MDS. In the current version, the new mirror CMAs will be created even for Customers that already have two or more CMAs.

If you want to limit mirror CMA creation to Customers that have only one CMA (or any other number of CMAs), use the new `-c` flag. The full command syntax is:

```
mdscmd mirorcma -s <source_MDS> -t <target_MDS> [-c <max_total_number>] [-m MDS server -u user -p password]
```

where `<max_total_number>` is the maximum resulting total number of CMAs per Customer.

For example, to mirror CMAs only for Customers that have only one CMA, run:

```
mdscmd mirorcma -s FirstMDS -t SecondMDS -c 2
```

### Automatic CMA Synchronization

When a mirror CMA is created, it is automatically synchronized with the primary CMA’s database. To keep these two CMAs regularly synchronized, it is recommended that you set up automatic synchronization through SmartDashboard. The synchronization method is user selectable, through SmartDashboard’s Policy > Management High Availability menu. For detailed instructions on synchronizing management stations, see the “High Availability” chapter of the Security Management Administration Guide.

### Synchronize ClusterXL Gateways

The gateway synchronization feature provides the mechanism for synchronizing the states of two Security Gateways. High Availability for Security Gateways is described in the ClusterXL Administration Guide. High Availability for encrypted connections is described in the VPN Administration Guide.
Failure Recovery in High Availability Deployments

Provider-1 version R70 and higher includes capabilities that enable recovery in many cases of a failed MDS in a High Availability deployment. Specifically, in the case of a failed MDS, you can promote a secondary CMA to become a primary CMA.

Note - CMA promotion in other cases is not supported.

The correct procedure for failure recovery depends on whether one of the remaining, functioning MDSs is a manager or not. You may have a remaining, functioning MDS manager in cases where there was more than one manager MDS or the failed MDS was not the manager. If the failed MDS was the only manager, the entire deployment needs to be migrated to a different MDS.

Recovery with a Functioning Manager MDS

If one of the remaining, functioning MDSs is a manager (there was more than one MDS or the failed MDS was not the manager), perform the following procedure.

Connecting to a Remaining MDS

To connect to a remaining MDS:

1. Make sure that all remaining MDSs and MLMs are running.
2. Connect to a remaining manager MDS with the MDG.
3. If there is no remaining manager MDS that is active, make one active. In the High Availability - MDS Contents view of the MDG for a manager MDS, Change Over that MDS from Standby to Active.
4. On each remaining MDS and on each remaining MLM, run the following two lines:
   ```
   mdsenv
   cp $MDSDIR/conf/mdsdb/customers.C $MDSDIR/conf/mdsdb/customers.C.prepromote
   ```
5. In the General - MDS Contents view of the MDG, delete the failed MDS.
   If the failed MDS was the primary MDS, the MDG will by default not allow you to delete the MDS. In this case, first run the following command on a remaining manager MDS:
   ```
   enable_mds_deletion <name>
   ```
   where `<name>` is the name of the failed primary MDS. Then delete the failed MDS in the MDG.
   Note - Deleting the MDS causes all of its CMAs, many network objects, and Global Policy assignments to disappear from the MDG as well. Objects that are still relevant will be automatically restored after the next step.
6. On each remaining MDS and on each remaining MLM, run the following lines:
   ```
   mdsstop
   mv $MDSDIR/conf/mdsdb/cp-deleted.C $MDSDIR/conf/mdsdb/cp-deleted.C.prepromote
   cp $MDSDIR/conf/mdsdb/customers.C $MDSDIR/conf/mdsdb/customers.C.afterpromote
   cp $MDSDIR/conf/mdsdb/customers.C.prepromote $MDSDIR/conf/mdsdb/customers.C
   mdsstart
   ```
   Relevant network objects and Global Policy assignments are automatically restored in the MDG.

Resetting Customer CMAs

To reset customer CMAs:

For each Customer whose primary CMA was on the failed MDS, perform the following:
1. Choose a CMA to be made primary. If the CMA is standby, first make it active by opening SmartDashboard for it. SmartDashboard prompts you to change the CMA's status to Active. Close SmartDashboard.

2. Promote the Customer's active CMA from secondary to primary by setting its host MDS's environment to that CMA (with `mdsenv <cma_name>`), and then running the following:
   
   ```
   promote_util
   ```

3. In SmartDashboard for the promoted CMA, locate (with `Where Used`) and remove all uses of the failed CMA, and the failed CMA itself. Save the policy.

4. Synchronize the Customer's CMAs manually, if necessary, and re-assign Global Policies and install policies on all gateways.

5. If the promoted CMA is using an HA CMA license, replace it with a regular CMA license.

### Restoring the High Availability Deployment

**To restore your High Availability deployment:**

1. Install a new secondary MDS.
   
   **Important** - The newly promoted secondary MDS must **NOT** use the same name as the failed MDS.

2. Mirror CMAs onto the new MDS as required.

### Recovery from Failure of the Only Manager MDS

If your deployment had only one manager MDS, and it has failed, your deployment is no longer manageable from the MDG. Therefore, you need to completely recreate the Provider-1 deployment.

### Recreating the Provider-1 Deployment

**To recreate the Provider-1 Deployment:**

For each Customer whose primary CMA was on the failed MDS, perform the following:

1. Choose a CMA to be made primary. If the CMA is standby, first make it active by opening SmartDashboard for it. SmartDashboard prompts you to change the CMA's status to Active. Close SmartDashboard.

2. Promote the Customer's active CMA from secondary to primary by setting its host MDS's environment to that CMA (with `mdsenv <cma_name>`), and then running the following:
   
   ```
   promote_util
   ```

3. Install a new Primary manager MDS, and additional MDSs according to your deployment's needs.

4. Migrate the Provider-1 environment from the old deployment to the new one according to the instructions for a Gradual Upgrade in the Provider-1 Upgrade Practices section of the Upgrading Provider-1 chapter in the Upgrade Guide. For the migration process, as the source CMA for each Customer, use the primary CMA (the original primary CMA, if remaining, or the one promoted in step).
   As part of the migration process, in SmartDashboard for the new CMA, make sure to locate (with `Where Used`) and to remove all uses of the old deployment's CMAs (except the primary CMA used for migration), and these CMA objects themselves. Save the policy.
   The Gradual Upgrade process includes migrating Global Policies. Afterwards, remember to re-assign Global Policies and install policies on all gateways.

5. Mirror new secondary CMAs according to your needs.
Chapter 9

Logging in Provider-1

In This Chapter

- Logging Customer Activity .................................................. 119
- Exporting Logs .................................................................. 121
- Logging Configuration ......................................................... 122

Logging Customer Activity

Logs are records of information that are generated when different events occur and then stored for future reference. In Provider-1, logs are generated by a Customer's network gateways, CMAs and the MDS. The Security Policy that is installed on the gateway governs the events which trigger logs originating from the Security gateways. For more information about configuring logs see the Security Management Administration Guide.

Logs can be stored locally on gateways, but a more common configuration is to deploy a remote machine to handle log repository storage. The gateway sends logs to a Log server (sometimes referred to as Logger), which collects and stores them. In Provider-1 the Log server is by default the CMA.

It is recommended that you deploy dedicated Log servers under either of the following circumstances:

- If heavy logging is expected.
- When the Container on which the CMA resides is expected to be heavily loaded.

Figure 9-54 Log server collects gateway activity logs & stores them in the Customer's network
A Customer Log Module (CLM) can be deployed to function as a Log server for a specific Customer. The CLM is housed on an MDS Container. It is possible to set up a CLM on any MDS Container in the system, as long as the MDS does not have another CMA or CLM of the same Customer on it. Once a CLM is created for a Customer, the Customer's gateways send records to the CLM, which stores logs on the MDS on which the CLM is housed.

By default, a Log server and/or a CLM receive logs from gateways of a specific Customer. However, you can configure a Log server/CLM to receive logs from multiple customers. For more information, refer to Check Point's SecureKnowledge database.

A special MDS Container that hosts only CLMs, and is actually dedicated to housing logs for multiple Customers, is called a Multi-Customer Log Module (MLM). If you expect heavy logging, it is advisable and more cost effective in terms of licensing to dedicate a separate server to deal solely with logs.

**Figure 9-55**  
CLM stores gateway activity records on the MLM

Logging can be deployed for a single Customer by:

- Enabling local logging on the Customer's network gateway. Refer to the Security Management Administration Guide to find out when to use local logging.
- Logging data to the Customer's CMA (the default setting).
- Logging to a Log server set up on a dedicated machine for the Customer.
- Logging to a Customer's CLM, which is installed on a Container or MLM.

It is possible to have a combined logging setup, with the following two components:

- CLMs extracting information from the Provider-1 environment,
- a Log server in the Customer's network receiving records.

In this case, logs are then maintained both in the Provider-1 environment and in the Customer's network environment.

The table below highlights the similarities and differences between CMA, CLMs and Log servers:

**Table 9-3  CMA vs. CLMs vs. Log servers**

<table>
<thead>
<tr>
<th></th>
<th>CMA</th>
<th>CLM</th>
<th>Log server</th>
</tr>
</thead>
</table>

Logging in Provider-1  Page 120
### Exporting Logs

There are several ways and formats in which a log file can be exported:

**Table 9-4  Exporting Logs**

<table>
<thead>
<tr>
<th>Format</th>
<th>Environment</th>
<th>Export to...</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>simple text file</td>
<td>Customer or</td>
<td>file</td>
<td>any time</td>
</tr>
<tr>
<td></td>
<td>Provider-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>database</td>
<td>Customer or</td>
<td>external Oracle database</td>
<td>manual one time event</td>
</tr>
<tr>
<td></td>
<td>Provider-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>database</td>
<td>Provider-1</td>
<td>external Oracle database</td>
<td>daily event</td>
</tr>
</tbody>
</table>

**Log Export to Text**

Export logs to a text file at any given time using SmartView Tracker. For more information, see the SmartView Tracker documentation in the *Security Management Administration Guide*.

**Manual Log Export to Oracle Database**

Export logs manually to an external Oracle Database at any given time.

---

**Note** - Provider-1 supports SmartReporter Reports. An SmartReporter server is installed on a separate machine and then configured in the Provider-1 environment.
Automatic Log Export to Oracle Database

You can export Check Point and OPSEC logs to Oracle commercial relational databases. To do this, you must configure the MDS to support log exports (see Configuring an MDS to Enable Log Export (on page 124)). Logs can automatically be exported once a day at a scheduled time.

Logs exports can only be done on log files that are not currently open and Active. The automatic log export will not take place in the following cases:
- The MDS, CMA or CLM is down at the scheduled log export time.
- The latest log file has not been closed and all previous logs were already exported.

Log Files

For each CLM, an Active log file, the fw.log file, is created. Logged data is stored to this file for a scheduled period or until it reaches a certain size limit, after which the fw.log file is saved with a new extension, say fw.log.109, and a new file is opened (this process is also known as log "switching"). Once a log file is closed, it is possible to export the file, automatically or manually.

Export Profiles

Automatic log exports are performed according to a Log Export Profile. This profile defines log export parameters, such as the schedule and the log fields to be exported. Each CMA and CLM can be assigned a Log Export Profile. The same log profile can be applied to a number of CMAs and CLMs that share the same logging needs.

Logs exports are performed on log files that are not currently open. The file must be inActive and not yet exported.

Choosing Fields to Export

As part of the Log Export Profile, a Provider-1 Superuser designates a list of log fields to export. You can set Default fields to automatically be included in each new Log Export Profile, or modify the fields selection as needed. If you need to define a new profile that is similar to an existing Profile, you can duplicate an existing profile and modify its properties as needed.

Log Forwarding

It is possible to use SmartView Tracker to forward a log file from one MLM to another computer. For more information, see the SmartView Tracker documentation in the Security Management Administration Guide.

Cross Domain Logging

By default, each security gateway managed by a Provider-1 CMA can send its logs either to the CMA (primary or secondary) or to a Log server (a physical machine or a CLM hosted on an MLM). When using Log servers or CLMs, the security gateways can send logs only to Log servers defined in the same management domain (i.e., belonging to the same Provider-1 Customer).

If required, a manual workaround can allow cross-domain (cross-Customer) logging. The workaround is recommended in very limited cases, as it has scalability restrictions, and its setup requires manual intervention in the SIC (Secure Internal Communications) authentication process.

The procedure for setting this up is detailed in SecureKnowledge; see SK12882.

Logging Configuration

The following section outlines the configuration issues that are involved with logging in Provider-1.
Setting Up Logging

1. To create an MLM, follow the same procedure that is done for creating a Container. See Provisioning Provider-1 (on page 46).
2. Using the MDG, create one or more CLMs per customer. Each must be on a different MDS. Remember to enable communication between the Provider-1 network and the customer's gateways. Add appropriate rules permitting the CLMs to communicate from the Provider-1 network with the customer's gateways, and install the policy on the relevant gateways.
3. Setup each relevant gateway to send its logs to the new CLM.
4. Synchronize the new CLM database with the CMA's database using the "install-database" operation. This must be done so that logs are properly processed. See Synchronizing the CLM Database with the CMA Database (on page 124).
5. Configure the MDS for the log exporting procedure. See Configuring an MDS to Enable Log Export (on page 124).
6. If you want to enable automatic log exporting, create a Log Export Profile and assign it to the customer's CLMs and CMAs. See Configuring Log Export Profiles (on page 124), and Choosing Log Export Fields (on page 125).

If you experience any difficulty, consult the Troubleshooting section. See Log Export Troubleshooting (on page 125).

Working with CLMs

Add a CLM

CLMs can be added through the MDG. Note the following:
- A Customer must have at least one CMA before a CLM can be added to it.
- Each CLM created for the same customer must be deployed on a different MDS.
- A Customer's CLM and CMA cannot be installed on the same MDS.

To add the new CLM:
1. In the MDG Customer View, select a customer, then select Add Customer Log Module from the Manage menu, or right-click the Customer and select Add Customer Log Module.
2. You are required to enter values for the displayed fields.
   - Enter a name for the CLM.
   - Select the Container MDS on which this CLM will be maintained.
3. Assign a virtual IP address to the CLM. Configuration details for creating Virtual IPs and installing licensing are similar to those of the CMA. See Planning the Provider-1 Environment (on page 32).
4. Next, fill in the license information, if required.

Starting or stopping a CLM

To start or stop a CLM from the MDG General View:
1. Select the CLM.
2. Do one of the following:
   - Choose Manage > Start Customer Management/Start Customer Log Module or Stop Customer Management/Stop Customer Log Module as appropriate, or
   - Select Start or Stop from the toolbar.
   The run status of the CLM will change accordingly, and the change will be reflected in the Status column.

An alternative way to start or stop a CLM is from the MDS command line, by using the mdsstart_customer and mdsstop_customer commands.
**Deleting a CLM**

Before deleting a CLM, make sure to stop it. Select it in the MDG **Customer Contents** view and then choose the delete tool in the menu bar, or **Manage > Delete**, or right-click the CLM and select **Delete Customer Management Add-on/Delete Customer Log Module** (respectively) from the right-click menu.

**Setting up Customer Gateway to Send Logs to the CLM**

Logs are not automatically forwarded to new CLMs. You must manually setup each relevant gateway to send its logs to the new CLM.

**To set up customer gateways to send logs to the CLM:**
1. Launch SmartDashboard for the Customer's CMA and double-click the gateway object to display its **Check Point Gateway** window.
2. Display the **Additional Logging** page (under **Logs and Masters**) and check **Forward log files to Security Management Server**. The Security Management Servers drop-down list is enabled.
3. Select the new CLM from the Security Management Servers drop-down list and click **OK**.

**Synchronizing the CLM Database with the CMA Database**

To process logs properly, the CLM database should be synchronized with the CMA database.

**To process logs to synchronize the CLM Database with the CMA Database:**
1. In SmartDashboard, select **Policy > Install Database**. The **Install Database** window is displayed.
2. Under **Install Database on**, check the CLM you have created and click **OK**. The **Install Users Database** status window is displayed. From this window you can follow the progress of the installation.

**Configuring an MDS to Enable Log Export**

**To configure an MDS to Enable Log Export:**
1. Stop the MDS processes.
2. Install and configure the Oracle Client.
3. Define the environment variable **ORACLE_HOME** according to the installation.
4. Add $ORACLE_HOME/lib to the $LD_LIBRARY_PATH.
5. Add $ORACLE_HOME/bin to the $PATH.
6. Restart the MDS processes.

**Configuring Log Export Profiles**

The first time you perform a Log Export, a log field table is created in the external database. The table is structured according to the log fields settings defined in the **Log Export Profile**. The table’s naming convention is `<CMA Name>_<Customer Name>_CPLogs`. For example, for CMA1 of Customer1, the table will be named `CMA1_Customer1_CPLogs`.

**To configure Log Export profiles:**
1. Select **Manage > Log Export > Profiles...** from the menu.
2. To view the CMAs and CLMs assigned a selected profile, click **Show Assigned**. To remove a specific CMA or CLM, click **Remove**.
3. In the **General** tab, specify basic export parameters, such as the Oracle server receiving the logs, the name and password of the administrator managing that Oracle server, the schedule etc.
4. In the **Log Fields** tab, select the fields to be exported. Some fields are checked by default. Change these settings as needed.
   - If you modify this list (for example, changing a field's length), once the data is exported, the list details will become incompatible with the target table and future Log Exports will fail. To avoid this, **rename** the current table.
   - Next time you perform a Log Export, the process will create a new table using the original table’s name.
5. In the **Assign** tab, specify which CMAs and CLMs are assigned this profile.
6. To find the profile assigned to a specific CMA or CLM, click **Find** in the **Log Export Profiles** window. The window will either display the Log Export Profile’s name, or indicate that no profile has been assigned.

### Choosing Log Export Fields

Use the **Log Export Fields** window to determine which log fields are exported. You can add, edit and delete fields as needed. **Default** fields can be selected in this window, to be automatically included in each new Log Export Profile.

Be aware that changing or removing log export fields affects all profiles using these fields.

**To choose Log Export fields:**

1. Select **Manage > Log Export > Fields...** from the menu.
2. Use the **Add**, **Edit** and **Delete** buttons to create a list of fields according to the logging data you want to export.
   - The **Name** of the field is as it appears in the Log File. The **Exported Name** is the name you give to the field you want to appear in the exported Oracle table. The **Exported Name** should follow Oracle naming restrictions.
   - Enter a **Type**, and **Length**. Check **Export by default** to have a field selected by default for all new Log Export Profiles.
3. These select fields to automatically include in each new Log Export Profile, check **Export by default** in the **Add Log Export Field** window (or double-click an existing field). You can later modify this selection as needed.

### Log Export Troubleshooting

Log Export troubleshooting suggestions are presented below:

**Table 9-5  Log Export Troubleshooting**

<table>
<thead>
<tr>
<th>Error Message</th>
<th>What to do</th>
</tr>
</thead>
<tbody>
<tr>
<td>No connection with CMA.</td>
<td>Verify the following:</td>
</tr>
<tr>
<td></td>
<td>• The CMA is running properly.</td>
</tr>
<tr>
<td></td>
<td>• The CMA has a valid license.</td>
</tr>
<tr>
<td>Configuration file not found.</td>
<td>Update the Log Export Profile using the MDG.</td>
</tr>
<tr>
<td>No data to export.</td>
<td>Run two commands:</td>
</tr>
<tr>
<td></td>
<td>• mdsenv &lt;cmaname&gt;</td>
</tr>
<tr>
<td></td>
<td>• fw lslogs -e.</td>
</tr>
<tr>
<td>Failed to load dll.</td>
<td>The external database’s client is not configured properly.</td>
</tr>
<tr>
<td></td>
<td>Proceed as follows:</td>
</tr>
<tr>
<td></td>
<td>1. Stop the MDS.</td>
</tr>
<tr>
<td></td>
<td>2. Prepare your system for the Log Export process (see Configuring an MDS to Enable Log Export (on page 124)).</td>
</tr>
<tr>
<td></td>
<td>3. Start the MDS.</td>
</tr>
</tbody>
</table>
## Error Message | What to do
--- | ---
Failed to connect to the external database. | Verify the following:
- The external database is accessible and running properly.
- The external database's client is configured correctly.
- The administrator name and password specified in the Log Export Profile can indeed be used to login to the database.
- The Oracle Client and the MDG use the same Oracle server name.

Failed to create table in database. | Verify the following:
- The administrator has been assigned the appropriate permissions.
- The exported log field names conform to the external database's naming conventions.

Failed to read Check Point logs. | Verify the following:
- The CMA is running properly.
- The CMA has a valid license.

Failed to write to external database. | Verify that the external database's table structure (e.g. the log field names and the columns' width) conforms to its definition in the Log Fields tab of the Log Export Profile window.
If the two are incompatible, rename the table.

---

### Using SmartReporter

SmartReporter can now produce both Log Based reports and Express reports for gateways managed by Provider-1 CMAs. Use SmartReporter to create selected reports for specified customers and gateways. Reports can be scheduled at any time, and can be sent by email or uploaded to an FTP site. SmartReporter needs to be properly configured to work with Provider-1, see the "Getting Started" chapter of the SmartReporter Administration Guide for further details.
Chapter 10

Monitoring in Provider-1

In This Chapter

Overview 127
Monitoring Components in the Provider-1 System 128
Checking the Status of Components in the System 129
Monitoring Issues for Different Components and Features 131
Using SmartConsole to Monitor Provider-1 Components 137

Overview

Provider-1’s MDG is designed to support daily monitoring and maintenance activities. It has a variety of MDG views that can be used by administrators to confirm that the system is running smoothly and that management activities are being successfully performed.

By default, management activities receive system confirmation within five minutes. Once confirmation has been received, Administrators can use status indicators to determine if management activities were performed successfully. The following status checks can be executed:

Table 10-6 What can be checked?

<table>
<thead>
<tr>
<th>Components</th>
<th>Status Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateways</td>
<td>Are they responding?</td>
</tr>
<tr>
<td>CMAs/CLMs</td>
<td>Are they started or stopped?</td>
</tr>
<tr>
<td>High Availability</td>
<td>Which MDS or CMA is Active?</td>
</tr>
<tr>
<td></td>
<td>Which MDS or CMA is Standby?</td>
</tr>
<tr>
<td>Global Policies</td>
<td>Which Global Policies are available</td>
</tr>
<tr>
<td></td>
<td>When were the Global Policies assigned?</td>
</tr>
<tr>
<td></td>
<td>Was the Global Policy Assign operation a success?</td>
</tr>
<tr>
<td>Local Policies</td>
<td>Which Policy is installed on the gateway?</td>
</tr>
<tr>
<td>Global VPN Communities</td>
<td>What Global VPN Communities are available?</td>
</tr>
<tr>
<td></td>
<td>Are the peer Policies updated?</td>
</tr>
<tr>
<td>Administrators</td>
<td>Which Administrators are currently logged on?</td>
</tr>
<tr>
<td>GUI Clients</td>
<td>Which GUI Clients are in use?</td>
</tr>
</tbody>
</table>

If a status check reveals that management activities were not successful, you can use the MDG views such as the Critical Notification window to yield further information for troubleshooting purposes.

It is also possible to use the SmartView Console clients (such as SmartView Monitor and SmartView Tracker) for monitoring, tracking and troubleshooting purposes.
Monitoring Components in the Provider-1 System

The MDG's General View provides a Customer Contents mode which lets you see at a glance all the components of the system, including Customers, CMAs and their network gateways.

The Customer Contents mode is divided into 2 sections or panes. The far right pane gives a statistical breakdown, or summary of the components in the system depending on what you have selected in the left pane.

For example, if you select the Provider-1 root, a summary of Provider-1 root Customer-related statistics is displayed: the number of Customers, CMAs, gateways, Administrators and GUI Clients in the system.

Another example, if you select a Customer in the left pane, Customer Properties are displayed, including: user-defined free field information (e.g. Contact Person), entered in the Properties tab of the Customer Configuration window.

The left pane provides a view of all the Customers in the system, their CMAs and gateways. Information displayed in this pane includes:

- The MDS which contains the CMA and CLM.
- The IP addresses of all the components in the system
- Whether the component is Active or Standby (for High Availability).
- Whether the component has been enabled for global use, in this case the global name is displayed.

Exporting the List Pane's Information to an External File

You can save List Pane information to an external file (such as an Excel sheet) for future examination by selecting Manage > Export to File.

Working with the List Pane

You can change the way that the Network Objects mode List Pane looks in order to focus on specific components or networks in the system.
Filtering

To focus on a specific group of objects that share a certain common denominator (such as their IP address range, Customer name or the MDS they are installed on), filter any of the List pane’s columns by right-clicking the column heading and selecting Column Filter... from the displayed menu. Additionally:

- To view existing filters, select View > Filter Details.
- To clear all filters, select View > Clear All.

Showing and Hiding Selected List Pane Columns

You can set the List pane to display only the columns you are interested in and hide all others. To hide a specific column, right-click its header and choose Hide Column from the menu. To hide or show more than one column at a time, select View > Show/Hide Columns.

Checking the Status of Components in the System

The most basic monitoring activity is to check that all components in the system (Security Gateways, UTM-1 Edge appliances, CLMs, CMAs, MDSs) are up and running. This can be done via the MDG’s General View in the Network Objects mode. In this mode, administrators can examine how system components are functioning.

The Network Objects mode shows general and status information for all components in the system. This information is displayed in the upper part of the window, or the List pane.

In the Network Objects mode List Pane you can right-click or double-click on a component and execute a command. For example, you can start, stop, configure or update a selected component. Additionally you can launch any of the SmartView Console clients and take advantage of their facilities. For example, if a Customer’s gateway is behaving sluggishly, launch SmartView Monitor and/or SmartView Tracker from the said gateway to check what activities are taking place at the gateway so as to determine the root of the sluggishness.

Status symbols in the List pane include:
Checking the Status of Components in the System

<table>
<thead>
<tr>
<th>Status</th>
<th>Applies to...</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Writing...</td>
<td>All objects</td>
<td>Displayed from the time the MDG starts running until the time the first status is received. This takes no more than 30 seconds.</td>
</tr>
<tr>
<td>✔ Started</td>
<td>MDS/CMA/CLM</td>
<td>The object has been started.</td>
</tr>
<tr>
<td>! Stopped</td>
<td>MDS/CMA/CLM</td>
<td>The object has been stopped.</td>
</tr>
<tr>
<td>🚧 Disconnected</td>
<td>MDS</td>
<td>The object has been disconnected.</td>
</tr>
<tr>
<td>✔ OK</td>
<td>Gateway</td>
<td>An application is installed on this gateway and is responding to status update requests from the Security Management Server.</td>
</tr>
<tr>
<td>✔ Needs Attention</td>
<td>Gateway</td>
<td>At least one of the applications installed on this gateway is not running properly.</td>
</tr>
<tr>
<td>✗ Not Responding</td>
<td>Gateway</td>
<td>There is either no application installed on this gateway, or the application is installed, but cannot be reached.</td>
</tr>
<tr>
<td>? Unknown</td>
<td>Gateway</td>
<td>A status has been received from the server, but the system does not recognize it.</td>
</tr>
<tr>
<td>N/A</td>
<td>Clusters</td>
<td>Cluster objects report the status <em>N/A</em> (Not Available). However the status of each member of the cluster is displayed.</td>
</tr>
</tbody>
</table>

Viewing Status Details

To get more details about a network component, select it in and choose Get Status Details... from the Manage menu. The Status Details window provides hardware, policy and/or run status details according to the selected object. Status details include:

<table>
<thead>
<tr>
<th>Object</th>
<th>Status Details Available</th>
</tr>
</thead>
</table>
| MDS        | • Version  
             • Operating System  
             • CPU  
             • Memory  
             • Disk |
| Gateway    | • Policy name and installation time  
             • Interface table  
             • Encryption and description  
             • Virtual and real memory  
             • CPU  
             • Disk |
Locating Components with Problems

The Critical Notifications Pane; which is the lower pane in the Network Objects mode, focuses on components which need critical attention. If a component stops or disconnects, this is displayed in the Critical Notifications pane.

The following types of statuses appear in the Critical Notifications Pane:

<table>
<thead>
<tr>
<th>Status</th>
<th>Applies to...</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>! Not Stopped</td>
<td>MDS/CMA/CLM</td>
<td>The object has been stopped.</td>
</tr>
<tr>
<td>☢ Disconnected</td>
<td>MDS</td>
<td>The object has been disconnected.</td>
</tr>
<tr>
<td>✅ Needs Attention</td>
<td>Gateway</td>
<td>At least one of the applications installed on this gateway is not running properly.</td>
</tr>
<tr>
<td>✗ Not Responding</td>
<td>Gateway</td>
<td>There is either no application installed on this gateway, or the application is installed, but cannot be reached.</td>
</tr>
</tbody>
</table>

For each object, the name, status and time of status update is displayed.

Monitoring Issues for Different Components and Features

In this section you will find specific information about different Provider-1 elements and the status issues that are raised for each one individually.
MDS

MDSs are managed via their own special view, MDG's General View - MDS Contents mode, for administrator convenience. Since MDSs are so vital to smooth Provider-1 operations, only the Provider-1 Superuser administrator has the ability to view and manage the MDS Contents mode. This mode allows the Provider-1 Superuser administrator to perform MDS management activities and check all MDS statuses at a glance.

However, non Provider-1 Superuser administrators can view the status of MDSs in the MDG's General View - Network Objects mode. This view displays all system components and how they are functioning.

For a granular view of MDS activity, the Provider-1 Superuser administrator can launch SmartView Tracker in Audit mode. In SmartView Tracker you can see:

- the management activity logs generated by the administrator
- the time the log was generated
- the GUI Client source
- the administrator performing the actions, and changes to network objects.

The Provider-1 Superuser administrator can also start, stop, add or delete an MDS.

Global Policies

Customer network systems operate according to the behavior specified in their Security and Global Policy rules. To see how Global Policies have been applied to Customers in the Provider-1 system, use the Global Policies View - Security Policies mode. This mode displays:

- the Global Policies in the system,
- the Customers and CMAs that are assigned to these policies,
- the time when the assignment took place,
- the last time that the global policy was modified,
- the status of the assignment operation (whether or not it was successful).

Customer Policies

**Checking a CMA's Policy**

A CMA's policy may or may not contain global rules, depending on whether a global policy was assigned to the Customer. Use the **Global Policies View - Security Policies** mode to check:

- if a Customer's CMA has been assigned a global policy,
- which Global Policy was assigned,
- the time of the assignment,
- the time that the Global Policy was last changed,
- whether the assignment operation was successful.

You can also use the MDG's **General View - Network Objects** mode to see which Customer policy is assigned to a CMA.

Gateway Policies

**Checking a Gateway's Current Policy**

To see which policy is installed on a specific gateway, you can use the **General View - Network Objects** mode. For each gateway the following information is displayed:

- the **Policy Name**,
- the **Gateway Local Installation Time**,
- the local date and time when the policy was installed.

If there are problems with the gateway, they will be displayed in the **Critical Notifications** Pane, which focuses on components that need attention.

High Availability

Provider-1 implements High Availability on the following levels:

- The gateway level.
• The CMA level - multiple CMAs are supported, as well as an optional Security Management Backup server.

• The MDS level.

CMA and MDS High Availability are managed through the MDG's High Availability View. The administrator can do all management activities relating to MDS High Availability through this view, and examine the status of these actions.

In the **High Availability - MDS Contents** mode, the following information is displayed:

- **MDSs** Active/Standby (login) status,
- **The Sync Status.** This status displays synchronization statuses for MDSs and CMAs. Every synchronization takes a certain amount of time to update the status. The default is 5 minutes. Statuses are as follows:
  - **Unknown**, no information has been received about this CMA synchronization status.
  - **Never synced**, this CMA has never been synchronized with the other CMA.
  - **Synchronized**, this CMA is synchronized with the other CMA.
  - **Lagging**, the data of this CMA is less updated than the data of the other CMA.
  - **Advanced**, the data of this CMA is more updated than the data of the other CMA.
  - **Collision**, the data of this CMA conflicts with the data of the other CMA.

**Global VPN Communities**

The **Global Policies - VPN Communities** mode is dedicated to Global VPN Communities. This view shows which Global VPN Communities exist in the system.

![Global Policies - VPN Communities](image)

After the Global VPN Communities are defined in the Global SmartDashboard, the **Global Policies View - VPN Communities** mode displays the configuration update status for each community, and the Customers and gateways that participate in the community.
Administrators

To view all the administrators that have been created in the system, and the Customers for which they are responsible for, use the Administrators View - Customers per Administrator mode.

The Administrators View allows you to:

- Add, edit and delete an Administrator.
- Specify and edit the Administrator's password.
- Specify and edit the Administrator's Provider-1 permissions.
- Specify and edit the Administrator's Customer permissions (for various Check Point applications).
- Assign or remove an Administrator from managing a Customer's network.

Alternatively, you can view the system by looking at a list of Customers, and which Administrators are assigned to each of them, through the Administrators View - Administrators per Customers mode.
**Connected Administrators**

To see which administrators are Active in the system at any time, use the Connected Administrators View. This view allows you determine if any questionable activity has taken place. This view also allows the Provider-1 Superuser to use mouse's right-click and regular menus to delete an administrator's connection.

**GUI Clients**

To see which GUI Clients have been assigned for use, and to which MDSs or Customer environments they are connected, use the GUI Clients View. In this view information is displayed by default in a Customer per GUI Client hierarchy, in other words where you can see the GUI Clients and the Customers assigned to each. You can manage these entities by right-clicking on the GUI Client and selecting to assign Customers to it. This view can be toggled so that the hierarchy is reversed, in other words where you can see GUI Clients per Customer. Similarly, by right-clicking on a Customer you can select to assign GUI Clients to it.
Using SmartConsole to Monitor Provider-1 Components

Log Tracking

The Provider-1 system uses either CMAs or CLMs to gather information about Customer gateways’ activities. CMAs and CLMs can gather detailed log information from Security Gateways, UTM-1 Edge appliances, and many OPSEC-certified security applications. This information can then be accessed using the SmartConsole Clients.

Tracking Logs using SmartView Tracker

All administrator activity using SmartConsole Client applications, such as SmartDashboard, is logged in audit logs. These logs can be monitored using SmartView Tracker, which can dramatically reduce the time needed to troubleshoot configuration errors.

The graphical SmartView Tracker uses the logging data on the server to provide real-time visual tracking, monitoring, and accounting information for all connections including VPN remote user sessions. Administrators can perform searches or filter log records to quickly locate and track events of interest. To use SmartView Tracker, in the MDG, select a CMA, then right click and choose Launch Application > SmartView Tracker.

If there is an attack or other suspicious network activity, administrators can use SmartView Tracker to temporarily or permanently terminate connections from specific IP addresses. For more information about using SmartView Tracker, see the Security Management Administration Guide.

Real-Time Network Monitoring with SmartView Monitor

SmartView Monitor is an easy-to-use monitoring tool that allows you to inspect network traffic and connectivity. In addition, it provides real-time information about the performance and security state of both gateway and VPN operations.
**Monitoring the Status of a CMA**

To use SmartView Monitor, select a CMA from any view, then right click and choose **Launch Application > SmartView Monitor**.

If your network experiences problems such as sluggishness, loss of data or security related problems, it is important to immediately identify these phenomena. SmartView Monitor provides a real-time monitoring tool designed to help administrators find the cause of these problems, when and why they occur, and how to fix them. Use SmartView Monitor to examine traffic, requested services, and network load in the customer network. For more information, see the **SmartView Monitor Administration Guide**.

**Check Point System Counters**

SmartView Monitor uses Check Point System Counters to collect information about the status, activities, hardware and software usage of different Check Point products in real time. System Counters are used to plot graphs and to view reports of current or archived data collected by Counter Logs.

**Traffic Flow and Virtual Link Monitoring**

Traffic flow can be monitored per service or network object. SmartView Monitor also enables monitoring based on a variety of parameters, for example the QoS Policy rules installed on an interface, etc. Compliance to a Service Level Agreement (SLA) can be monitored, and alerts can be generated. Traffic can be monitored between two Check Point Security Gateways or two QoS gateways for real time analysis of bandwidth and latency.

**Blocking Suspicious Connections**

Suspicious Activity rules are security rules that enable the administrator to instantly block suspicious connections not restricted by the currently enforced Security Policy.

**Using Thresholds**

SmartView Monitor can be used to configure predefined actions that are triggered when certain changes in status occur. For instance, a rule can be defined to send an email to a certain address if the load on a gateway’s CPU surpasses a threshold that you set.

By default the engine responsible for triggering the events is disabled for Provider-1 CMAs, but it can be enabled per CMA by running the following commands from the root shell of the MDS machine:

1. Change to the CMA’s environment with the command `mdsenv <CMA Name>`
2. `cpstat_monitor &`

After running this command, thresholds are monitored until the CMA is stopped.
To permanently enable this functionality for a specific CMA, you must modify the value of the registry key that sets whether the `cpstat_monitor` process auto-starts whenever the CMA is started. You can do so by running the following command from the CMA's environment:

```
cpprod_util CPPROD_SetValue PROVIDER-1 RunCpstatMonitor 1 1 1
```

**Note** - To revert to the registry's original setting, enter the following on the MDS in the CMA's environment:

```
cpprod_util CPPROD_SetValue PROVIDER-1 RunCpstatMonitor 1 0 1
```

### SmartReporter Reports

The SmartReporter delivers a user-friendly solution for auditing traffic and generating detailed or summarized reports in the format of your choice (list, vertical bar, pie chart etc.) for events logged by CMA-managed gateways that are running SmartView Monitor. SmartReporter produces reports for these gateways.

See the *SmartReporter Administration Guide* to understand how to generate SmartReporter Reports.
Chapter 11

Architecture and Processes

In This Chapter

- Packages in MDS Installation 140
- MDS File System 140
- Processes 142
- MDS Configuration Databases 144
- Connectivity Between Different Processes 145
- Issues Relating to Different Platforms 146

Packages in MDS Installation

Provider-1 Multi-Domain Server installation consists of the following packages:

<table>
<thead>
<tr>
<th>Package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPCON62CMP-R70</td>
<td>Check Point Connectra CM Compatibility Package</td>
</tr>
<tr>
<td>CPEdgecmp-R70</td>
<td>Check Point UTM-1 Edge Compatibility Package</td>
</tr>
<tr>
<td>CPPIconnectra-R70</td>
<td>Check Point Connectra Plug-in</td>
</tr>
<tr>
<td>CPmds-R70</td>
<td>Check Point Multi-Domain Server</td>
</tr>
<tr>
<td>CPSuite-R70</td>
<td>Check Point Security Gateway</td>
</tr>
<tr>
<td>CPvsxngxcmp-R70</td>
<td>Check Point Power VSX</td>
</tr>
</tbody>
</table>

On Linux and SecurePlatform, package names contain the suffix "-00". For example, the full name of CPSuite-R70 package for these platforms is CPSuite-R70-00.

All of these packages have pre-defined dependencies between them. Under no circumstances should these packages be manually removed.

⚠️ Important - Manually removing a package has negative implications on the Multi-Domain Server.

MDS File System

MDS Directories on /opt and /var File Systems

DS Installation creates subdirectories under /opt and /var/opt directories. Following is the list of subdirectories created under /opt:
Table 11-8 **Subdirectories under /opt**

<table>
<thead>
<tr>
<th>Subdirectory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPInstLog</td>
<td>Contains installation and upgrade log files.</td>
</tr>
<tr>
<td>CPsuite-R70</td>
<td>Contains the installation of the CPsuite-R70 package.</td>
</tr>
<tr>
<td>CPshrd-R70</td>
<td>Contains information from the CPsuite-R70 package.</td>
</tr>
<tr>
<td>CPhared</td>
<td>Exists for compatibility with previous versions.</td>
</tr>
<tr>
<td>CPEdgecmp</td>
<td>Contains the installation of the CPEdgecmp package.</td>
</tr>
<tr>
<td>CPngcmp-R70</td>
<td>Contains the installation of the CPngcmp-R70 package.</td>
</tr>
<tr>
<td>CPmds-R70</td>
<td>Contains the installation of the CPmds-R70 package.</td>
</tr>
</tbody>
</table>

Table 11-9 **Subdirectories under /var/opt**

<table>
<thead>
<tr>
<th>Subdirectory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPsuite-R70</td>
<td>Contains configuration, state and log files for Check Point Security Gateway management.</td>
</tr>
<tr>
<td>CPshrd-R70</td>
<td>Contains the configuration of Check Point SVN Foundation, as well as the registry files.</td>
</tr>
<tr>
<td>CPEdgecmp-R70</td>
<td>Contains configuration files for the CPEdgecmp package.</td>
</tr>
<tr>
<td>CPngcmp-R70</td>
<td>Contains configuration files for the CPngcmp-R70 package.</td>
</tr>
<tr>
<td>CPmds-R70</td>
<td>Contains configuration of the Multi-Domain server, MDS-level logs and configuration/state/log files of Customer databases.</td>
</tr>
</tbody>
</table>

Structure of CMA Directory Trees

On Multi-Domain Container server, the CMA directories can be found under /var/opt/CPmds-R70/customers directory. For each CMA residing on the server, there is a separate directory under this path. Each CMA directory contains the following subdirectories:

Table 11-10 **CMA Subdirectories**

<table>
<thead>
<tr>
<th>Subdirectory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPsuite-R70</td>
<td>Contains the configuration, state and log files of this Customer, as well as links to the shared binaries and library files.</td>
</tr>
<tr>
<td>CPshrd-R70</td>
<td>Contains the configuration for the SVN Foundation for the Customer owning this CMA, as well as links to shared binaries and library files.</td>
</tr>
<tr>
<td>CPEdgecmp</td>
<td>Contains configuration files of the CPEdgecmp package for the Customer owning this CMA, as well as links to shared binaries and library files.</td>
</tr>
<tr>
<td>CPngcmp-R70</td>
<td>Contains configuration files of the CPngcmp-R70 package for the Customer owning this CMA, as well as links to shared binaries and library files.</td>
</tr>
</tbody>
</table>
Check Point Registry

Information related to the installation and versioning issues of different components that is requested by different Check Point processes, is centrally stored in a registry file.

The registry is stored in $CPDIR/registry/HKLM_registry.data (where the value of CPDIR environment variable is different whether you are in the MDS environment or whether you are in different CMA environments. This means that there are separate registry files for the MDS and for the CMAs.

Automatic Start of MDS Processes, Files in /etc/rc3.d, /etc/init.d

The script for the automatic start of MDS processes upon boot can be found in /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.

Processes

Environment Variables

Different Multi-Domain server processes require standard environment variables to be defined. The variables have the following functionality, they:

- 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.

MDS installation contains shell scripts for C-Shell and for Bourne Shell, which define the necessary environment variables:

- The C-Shell version is /opt/CPshrd-R70/tmp/.CPprofile.csh
- The Bourne Shell version is /opt/CPshrd-R70/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 MDS processes to run.

Standard Check Point Environment Variables

Table 11-11 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>
<tr>
<td></td>
<td>- In the MDS environment, this environment variable is equal to MDSDIR</td>
</tr>
<tr>
<td></td>
<td>- In CMA environment, it contains /opt/CPmds-R70/customers/&lt;CMA Name&gt;/CPsuite-R70/fw1</td>
</tr>
<tr>
<td>CPDIR</td>
<td>Location of Check Point SVN Foundation binary/configuration/library files. It points to different directories in MDS and CMA environments.</td>
</tr>
<tr>
<td>MDSDIR</td>
<td>Location of the MDS installation. In Provider-1 the path is /opt/CPmds-R70</td>
</tr>
</tbody>
</table>
### Parameters/Thresholds for Different MDS functions

#### Logging Cache Size

By default, the CMA reserves 1MB memory for log caching on the Management. In very intensive logging systems it is possible to raise the cache size. This requires more memory, but boosts the performance. To change the cache size, set:

```
LOGDB_CACHE_SIZE variable to the desired size in Kilobytes. For example, to set the cache to 4MB enter:

setenv LOGDB_CACHE_SIZE 4096 (in C-Shell syntax)
```

Additional environment variables controlling such mechanism as statuses collection mechanism (like `MSP_SPACING_REG_CMAS_FOR_STATUSES`) or connection retries (like `MSP_RETRY_INTERVAL`) are described later in this chapter.

### MDS Level Processes

Each MDS Level process has one instance on every MDS/MLM machine, when the MDS/MLM server is running. The following processes run on the MDS level:

**Table 11-12 MDS Level Processes**

<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. This process doesn't run on Log Managers or Container MDSs.</td>
</tr>
<tr>
<td>fwd</td>
<td>Audit Log server process.</td>
</tr>
<tr>
<td>fwm mds</td>
<td>MDS main process.</td>
</tr>
</tbody>
</table>

For proper operation of the Multi-Domain server all four processes must be running, unless dealing with configurations where `cpca` shouldn't be running.

### CMA Level Processes

Each one of these processes has a separate instance for every running CMA. The following processes run on the CMA level:

**Table 11-13 MDS Level Processes**

<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. This process doesn't run on Log Managers and Container MDSs.</td>
</tr>
<tr>
<td>fwd</td>
<td>Log server process.</td>
</tr>
<tr>
<td>fwm</td>
<td>Security Management server main process.</td>
</tr>
<tr>
<td>status_proxy</td>
<td>Status collection of SmartLSM Security Gateways. This process runs only on CMAs that were enabled for Large Scale Management.</td>
</tr>
<tr>
<td>Process</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>sms</td>
<td>Manages communication (status collection, logs collection, policy update, configuration update) with UTM-1 Edge gateways. This process runs only on CMAs that manage UTM-1 Edge devices.</td>
</tr>
</tbody>
</table>

For proper operation of the CMA, at least `cpd`, `cpca`, `fwd` and `fwm` must be running, unless dealing with configurations where `cpca` shouldn't be running. Other processes are required only for CMAs using specific functionality for which these processes are responsible.

### MDS Configuration Databases

The Multi-Domain Server environment contains a number of configuration databases, as opposed to a single Security Management server, that contains only one.

Each Multi-Domain Server contains:

- one Global Database (located in `/var/opt/CPmds-R70/conf` directory)
- one MDS Database (located in `/var/opt/CPmds-R70/conf/mdsdb` directory)
- a number of CMA databases (on Multi-Domain Server Containers only).

Each CMA database is located in `/var/opt/CPmds-R70/customers/`<CMA Name>/CPsuite-R70/fw1/conf directory.

### Global Policy Database

This database contains the definitions of global objects and global Security Policies. It can be viewed and edited using Global SmartDashboard client.

When the **Assign Global Policy** operation is invoked, the objects and policies defined in Global Policy database are copied to CMA databases, where they can be seen and used by SmartDashboard. These objects are editable only from Global SmartDashboard, CMA databases will contain read-only copies.

### MDS Database

This database contains two kinds of objects:

- MDS-level management objects – such as like administrators, customers, MDSs and CMAs. These objects are defined either using the Multi-Domain GUI or the MDS Command Line utilities.
- CMA-level Check Point objects – in order to display all customers' network objects in Multi-Domain GUI, these are centrally collected in MDS Database. Each time the object is updated in SmartDashboard, the changes are automatically updated in MDS Database as well.

### CMA Database

This database contains:

- Definitions of objects and policies created and edited by SmartDashboard, when connecting to the CMA.
- Global Objects (in read-only mode) copied by the **Assign Global Policy** operation.
- SmartLSM Security Gateways definitions made by SmartProvisioning.

Different CMAs residing on the same MDS have different separate databases.
Connectivity Between Different Processes

MDS Connection to CMAs

The main MDS process (fwm mds) looks for CMAs which are up and can be reached, but with which it has no CPMI connections. This connection is used for collecting statuses on the CMA and its gateways, and for receiving changes in objects that are relevant to the MDS/MDG system.

Normally, a special task wakes up every 120 seconds and searches for "CMA connection candidates". If the task has found connection candidates previously, then by default it wakes up after only 90 seconds. This shorter interval boosts CMAs connections upon MDS startup.

You can change the values of the default intervals:

- To change the CMA connection candidates search interval, set the `MSP_RETRY_INTERVAL` variable to the desired number of seconds.
- To change the status collection interval, set the `MSP_RETRY_INIT_INTERVAL` variable to the desired number of seconds.

  **Note** - Changing these values (especially `MSP_RETRY_INIT_INTERVAL`) makes the MDS-CMA connections faster during MDS startup, but may overload the connection if the value is set too low.

By default this task attempts to reconnect the MDS to no more than five CMAs per iteration. So, a system with 50 CMAs requires 10 iteration (of 90 seconds each, by default), so connecting to all the CMAs could take up to 15 minutes.

To change the maximum number of CMAs to which the MDS can connect per cycle, set the `MSP_RETRY_INIT_INTERVAL` variable to the desired value.

  **Note** - Raising this value makes the MDS connect to all CMAs faster during startup, but may overload if it is set too low.

Status Collection

Status collection begins when an MDG connects to a Manager. The MDS sends all CMAs a request to start collecting statuses. The MDS contacts the CMAs one by one, spacing these requests by one second, thus preventing the MDS load from peaking when multiple statuses arrive. You can change this default spacing and set the required spacing in milliseconds, with the environment variable `MSP_SPACING_REG_CMAS_FOR_STATUSES`.

Changing the Status Collection Cycle

The default status collection cycle takes 300 seconds, i.e. each system entity is monitored once every 5 minutes. This value can be changed per MDS in the MDG as follows:

1. In the **General View**, display the **MDS Contents** Mode. Choose and double click an MDS. The **Configure Multi Domain Server - General** window opens.
2. Under **Status Checking Interval**, specify the desired number of seconds in the **Set to** field (this value is saved in the `$MDSDIR/tmp/status_interval.dat` file).

Once the Status Checking Interval is set in the MDG, it is effective immediately, with no need to restart the MDS. The higher you raise this value, the longer it takes to detect a change in a gateway's status.

Collection of Changes in Objects

Check Point objects defined in CMA databases are copied to the MDS database and presented in the **Network Objects** view of the MDG. Every time one of these objects is updated by SmartDashboard that is connected to the customer's Active CMA, this change is immediately propagated to the MDS database of
the MDS hosting the Active CMA. From there it is distributed to the other MDSs participating in the High Availability environment.

Connection Between MDSs
Whenever the MDS/MLM servers are connected in High Availability environment they keep a constant network connection open between them. This connection is used to distribute:

- The statuses of CMAs and gateways between the MDS Containers.
- The status of administrators connected to MDS Managers.
- Latest updates of the objects propagated from CMAs.

Large Scale Management Processes
The Status Proxy process runs for each CMA that is enabled for Large Scale Management, and is constantly connected to the CMA to which it belongs. This process, amongst other functions, updates the CMA configuration database with such details as the last known IP address of the Dynamic IP address SmartLSM Security Gateway, as well as, the gateway status.

UTM-1 Edge Processes
The SMS process runs for each CMA that manages UTM-1 Edge devices, and is constantly connected to the CMA to which it belongs. UTM-1 Edge devices can be created either using SmartDashboard or using SmartProvisioning (where they are defined as UTM-1 Edge SmartLSM Security Gateways).

Reporting Server Processes
When the SmartReporter Add-on for Provider-1 is used, the SmartReporter server maintains a connection to the MDS. Whenever reports are generated, another component called SmartReporter Generator opens a connection to the MDS as well.

Issues Relating to Different Platforms
The Multi-Domain Server supports the following platforms:

- Check Point SecurePlatform
- RedHat Enterprise Linux
- Solaris

High Availability Scenarios
When creating High Availability environments with:

- a number of Multi-Domain Managers/Containers
- a number of MLMs

Provider-1 Multi-Domain Servers (MDSs) connected to a single environment can run on different platforms (for example, one MDS can be installed on Solaris and another on RedHat Enterprise Linux or SecurePlatform.

Migration Between Platforms
Use the existing Provider-1 migration tools to move configuration databases (such as the Global Policies databases or the CMA databases) between different Provider-1 platforms:
<table>
<thead>
<tr>
<th>Action</th>
<th>Use Script/Command</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migrate the Global Policies Database</td>
<td>migrate_global_policies script</td>
<td>Run this script without any parameters in order to see its usage. The files required before executing this script are specified in the script's usage. The specified files should be copied manually to the destination MDS.</td>
</tr>
<tr>
<td>Export a CMA, Security Management, or Global Policy database from one machine to another.</td>
<td>export_database script</td>
<td>This script exports the comprehensive database files into one .tgz file on the source machine that can be imported to a different MDS machine.</td>
</tr>
<tr>
<td>Migrate complete CMA databases from one MDS machine to another.</td>
<td>migrate_assist script</td>
<td>This script retrieves all of the required files for the migration of the CMA, including its configuration database and log files. The script works remotely, file by file.</td>
</tr>
</tbody>
</table>
| Migrate the CMA into the destination environment. | Use any one of:  
- **Import Customer Management Add-on** command from the MDG  
- cma_migrate script  
- mdscmd migratema utility | |
Chapter 12

Commands and Utilities

In This Chapter

Cross-CMA Search 148
P1Shell 150
Command Line Reference 154

Cross-CMA Search

Overview

The Cross-CMA Search feature enables searching across multiple CMA databases for defined network objects (including groups, dynamic objects and Global objects) and for rules (including Global and implied rules) that contain or affect a specified object.

Cross-CMA Search is a powerful tool for analyzing the functioning of network components in the context of a Provider-1 environment. The search function is similar to SmartDashboard's Where Used.

Performing a Search

You can access Cross-CMA search from the General - Customer Contents or from the General - Network Objects view of the MDG.

To open the Cross-CMA search window, select Cross-CMA Search from the Manage menu, or click the Cross-CMA Search icon.

Select a query, what you want to search for, and the Customer or Customers to search in. The following queries are available:

- **Specified Object query:**
  - **Find network objects by exact name** - finds objects defined in the CMA database, where the object's name exactly matches the query entry.
  - **Find network objects by partial name** - finds objects defined in the CMA database, where the object's name contains the query entry.
  - **Find network objects by IP address** - finds objects defined in the CMA database, where the object's IP address matches the query entry.

  Results for object queries include object and Customer information.

- **Find Policy rules that use a global object** - the query entry is a global object name. The query finds rules in the CMA policies, where the global object is part of the rule definition. This includes cases where the global object is not explicit in the rule definition, but is included in some object (such as a group or cluster) that appears in the rule.

  Results include Customer, policy and rule information, and the specific rule column where the global object appears. The first Results column, **Object Name**, indicates the relevant object as defined in the rule. This object may be one that includes, but is not identical to, the query entry.

- **Find Policy rules that use a global object explicitly** - this query is the same as the previous query, except that the results are limited to rules where the global object is explicit. Rules where the global object is merely included in some object (such as a group or cluster) that appears in the rule are excluded.
Results include Customer, policy and rule information, and the specific rule column where the global object appears. Two additional Results columns are:
- **Last in Cell?** - indicates whether the object is the sole object in its rule column, so that removing it would cause the cell content to become **Any**.
- **Is Removable?** - indicates whether an object is not a non-deletable object.

- **Find network objects that use a global object explicitly** - the query entry is the name of a global object. The query finds network objects (such as groups or clusters), defined in the CMA database, that contain the global object explicitly.

Results include object and Customer information.

The **Object Name** Results column indicates the relevant object as defined in the rule. This object may be one that includes, but is not identical to, the query entry.

- **Is Removable?** - indicates whether an object is not a non-deletable object.

### Copying Search Results

You can copy search results to use them in other applications.

To copy search results to the clipboard, right-click in the Results pane and select **Copy**. The copied results are in Comma Separated Values (CSV) text format.

### Performing a Search in CLI

You can perform a cross-CMA search in the CLI. The search results will be sent to standard output in Comma Separated Values (CSV) format.

The command syntax is:

```bash
mdscmd runcrosscmaquery <find_in> <query_type> <entry_type> <entry>
```

where `<find_in>` is one of the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-f &lt;filename&gt;</code></td>
<td>Searches in Customers listed in file <code>&lt;filename&gt;</code>.</td>
</tr>
<tr>
<td><code>-list &lt;list&gt;</code></td>
<td>Searches in Customers in <code>&lt;list&gt;</code>. <code>&lt;list&gt;</code> should be Customer names separated by commas (e.g. cust1,cust2).</td>
</tr>
<tr>
<td><code>-all</code></td>
<td>Searches in all Customers.</td>
</tr>
</tbody>
</table>

 `<query_type>` refers to one of the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>MDG version of the query</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>query_network_obj</code></td>
<td>One of the Specified Object queries (according to <code>&lt;entry_type&gt;</code>)</td>
</tr>
<tr>
<td><code>query_rulebase</code></td>
<td>Find Policy rules that use a global object</td>
</tr>
<tr>
<td><code>whereused_rules</code></td>
<td>Find Policy rules that use a global object explicitly</td>
</tr>
<tr>
<td><code>whereused_objs</code></td>
<td>Find network objects that use a global object explicitly</td>
</tr>
</tbody>
</table>

 `<entry_type>` refers to one of the following parameters:
Table 12-16  **Options for `<entry_type>` in Cross-CMA Command Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-n</code></td>
<td>Specifies that <code>&lt;entry&gt;</code> is the full object name. Available for all values of <code>&lt;query type&gt;</code>.</td>
</tr>
<tr>
<td><code>-c</code></td>
<td>Specifies that <code>&lt;entry&gt;</code> is a partial object name. Available only for <code>query_network_obj</code>.</td>
</tr>
<tr>
<td><code>-i</code></td>
<td>Specifies that <code>&lt;entry&gt;</code> is an IP address. Available only for <code>query_network_obj</code>.</td>
</tr>
</tbody>
</table>

*<entry>* refers to the query entry.

**Example**

To search CMAs for all Customers for objects containing 'my_gw' in their names:

```
mdscmd runcrosscmaquery -all query_network_obj -n my_gw
```

## P1Shell

### Overview

P1Shell is a command line shell that allows administrators to run Provider-1 CLI commands on the MDS, in both MDS and CMA environments, without root permissions. P1Shell authorizes users who are recognized by the MDS as Provider-1 Superusers or Customer Superusers. Lower level Provider-1 administrators must use the MDG (unless they have root permissions).

P1Shell can be defined as the default login shell for Provider-1 users, or it can be manually started in the CLI.

Because Provider-1 authentication is provided by the MDS, MDS processes must be running for an administrator to be authorized for P1Shell. However, starting MDS processes should not be available to non-Provider-1 administrators, so a password is required for mdsstart. The Start-MDS password can be set in `mdsconfig`, and should be given to Provider-1 administrators.

P1Shell maintains a connection with the MDS. P1Shell may be disconnected from the MDS by an MDG user (from the Connected Administrators view of the MDG), but as soon as P1Shell processes a command, P1Shell will reconnect to the MDS. The P1Shell user will be notified neither of the disconnecting nor of reconnecting. The MDG Connected Administrators view will display the reconnected P1Shell user only when the view is refreshed.

**Note** - P1Shell settings and commands are defined in configuration files that should not be changed. Any change to P1Shell configuration files will block P1Shell. If that happens, restore the files to their original versions to enable access to P1Shell.

### Starting P1Shell

To work in P1Shell, it must first be enabled. To enable P1Shell, run:

```
mdsconfig
```

and select P1Shell.
To start P1Shell, if it is not your default login shell, run:

```
p1shell
```

If the MDS is not running, you will be prompted for the Start-MDS password to authorize starting the MDS. Then, you will be prompted to enter your Provider-1 user name and password to authorize you for P1Shell.

**File Constraints for P1Shell Commands**

For security reasons, commands that run in P1Shell can read files only from within a defined input directory. Commands can write only to a defined output directory.

Note - The `mds_backup` command is an exception to this rule. The output of the backup is created at the path: `/var/opt/mds_backups/<timestamp>`, where `<timestamp>` is the time that the backup started.

Upon starting, P1Shell defines both input and output directories as the user's home directory. They can be changed for the work session, only within the home directory. Change the directories with the following commands:

```
set_inputdir <path>
set_outputdir <path>
```

where `<path>` is an existing directory, defined relative to the user's home directory.

To view existing input and output directories, enter:

```
display_io_dirs
```

Filenames appearing in commands cannot be paths (/ will be considered an illegal character) and must be located in the defined input or output directory.

Note - For security reasons, the output directory cannot be soft linked.

**P1Shell Commands**

P1Shell includes both general Provider-1 commands and its own Native P1Shell commands. For more information, see Native P1Shell Commands (on page 153).

To view a list of available Provider-1 commands, enter `help` or `?`. When the logged-in user is a Customer Superuser, commands that are available only to Provider-1 Superusers, not to Customer Superusers, will not appear in the list.

**General Provider-1 Commands**

Available commands are listed below. For further command details see the Provider-1 Administration Guide and the Command Line Interface Reference Guide.

Commands indicated as **Limited** are available only to Provider-1 superusers, not to Customer superusers. All other listed commands are available to both Provider-1 superusers and to Customer superusers.

Any commands listed in the **Not Supported** column are not currently supported in P1Shell. If the **Available Command Options** column says **All**, it should be understood as: All commands are available, except for those in the **Not Supported** column.

<table>
<thead>
<tr>
<th>Command</th>
<th>Limited</th>
<th>Not Supported</th>
<th>Available Command Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>c pca_dbutil</td>
<td>?</td>
<td>Supported</td>
<td>print; convert; d2u;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>get_crl_mode</td>
</tr>
<tr>
<td>Command</td>
<td>Limited?</td>
<td>Not Supported</td>
<td>Available Command Options</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------</td>
<td>---------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>cpd_admin</td>
<td></td>
<td></td>
<td>For Provider-1 superuser: All; for Customer superuser: debug on; list; ver</td>
</tr>
<tr>
<td>cpinfo</td>
<td></td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>cplic</td>
<td></td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>CPperfmon</td>
<td></td>
<td>hw; mdsconfig; procmem; monitor; off; summary</td>
<td></td>
</tr>
<tr>
<td>cppkg</td>
<td></td>
<td>add; setroot; del; print; getroot; get</td>
<td></td>
</tr>
<tr>
<td>cpprod_util</td>
<td>Limited</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>cprinstall</td>
<td></td>
<td>get; verify; install; transfer; uninstall; boot; cprestart; cpstart; cpstop; show; snapshot; revert; delete</td>
<td></td>
</tr>
<tr>
<td>cprlic</td>
<td></td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>cpstat</td>
<td></td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>cpstat_monitor</td>
<td></td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>cpvinfo</td>
<td></td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>cpwd_admin</td>
<td></td>
<td>list</td>
<td></td>
</tr>
<tr>
<td>dbedit</td>
<td></td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>dbver</td>
<td></td>
<td>-help; -s; -c; -u; -w; -m; -p</td>
<td></td>
</tr>
<tr>
<td>enable_mds_deletion</td>
<td>Limited</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fw</td>
<td>fetch; log; fetchlogs; monitor; stat; tab; mergefiles</td>
<td>For Provider-1 superuser: All for Customer superuser: logswitch; debug fwd; debug fwm</td>
<td></td>
</tr>
<tr>
<td>fwm</td>
<td>dbimport; logexport</td>
<td>For Provider-1 superuser: All for Customer superuser: load; dbload; ver; unload; logexport; mds recalc_lics; mds fwmconnect; mds rebuild_global_communities_status</td>
<td></td>
</tr>
<tr>
<td>LSMcli</td>
<td>cpinstall; snapshot; delete; revert</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>mds_backup</td>
<td>Limited</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>mds_user_expdate</td>
<td></td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Limited?</td>
<td>Not Supported</td>
<td>Available Command Options</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------</td>
<td>---------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>mdscmd</td>
<td>Limited</td>
<td>migratecma</td>
<td>All</td>
</tr>
<tr>
<td>mdsconfig</td>
<td>Limited</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>mdsenv</td>
<td></td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>mdsquerydb</td>
<td></td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>mdsstart</td>
<td>Limited</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>mdsstart_customer</td>
<td></td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>mdsstat</td>
<td></td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>mdsstop</td>
<td>Limited</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>mdsstop_customer</td>
<td></td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>promote_util</td>
<td></td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>sam_alert</td>
<td></td>
<td></td>
<td>All</td>
</tr>
</tbody>
</table>

**Native P1Shell Commands**

Besides enabling Provider-1 commands, P1Shell implements the following shell commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>help [command]</td>
<td>Displays the command's help text, or (without arguments) lists available commands.</td>
</tr>
<tr>
<td>Idle [minutes]</td>
<td>Sets idle time before automatic logout to &lt;minutes&gt;, or (without arguments) displays current idle time (default is 10 minutes).</td>
</tr>
<tr>
<td>exit</td>
<td>Exits P1Shell.</td>
</tr>
<tr>
<td>? [command]</td>
<td>Same as help.</td>
</tr>
<tr>
<td>set_outputdir &lt;path&gt;</td>
<td>Sets the output directory to be &lt;path&gt;, where &lt;path&gt; is relative to the user's home directory.</td>
</tr>
<tr>
<td>set_inputdir &lt;path&gt;</td>
<td>Sets the input directory to be &lt;path&gt;, where &lt;path&gt; is relative to the user's home directory.</td>
</tr>
<tr>
<td>display_io_dirs</td>
<td>Displays the input and output directories.</td>
</tr>
<tr>
<td>copy_logfiles -&lt;process_name&gt; [-l]</td>
<td>Copies the process's debug log files according to the environment context (CMA/MDS) to the output directory. &lt;process_name&gt; is one of: fwm, fwd, cpd, c pca. If -l is used, only the most recent log file is copied.</td>
</tr>
<tr>
<td>run &lt;batch_file&gt;</td>
<td>Runs a batch of MDS commands in sequence. The batch file must be in the defined input directory.</td>
</tr>
<tr>
<td>scroll [on</td>
<td>off]</td>
</tr>
</tbody>
</table>
Audit Logging

P1Shell logs audits in two different ways.

P1Shell saves all audits to a text file:

$MDS_SYSTEM/p1shell/log/p1shell_cmd_audit.log

In addition, P1Shell sends audits to the MDS to be logged. These audits can be viewed in SmartView Tracker. If the MDS is not running at the time as the audited event, and the MDS later starts during the same P1Shell session, the audit is then sent to the MDS. If the MDS is down from the time of the event until the end of the P1Shell session, the MDS does not receive the audit.

Command Line Reference

cma_migrate

**Description**  This command imports an existing Security Management server or CMA into a MDS so that it will become one of its CMAs. If the imported Security Management or CMA is of a version earlier than the MDS to which it is being imported, then the Upgrade process is performed as part of the import.

It is recommended to run `cma_migrate` to import CMA or Security Management database files created using the `export_database` tool.

Bear in mind that the source and target platforms may be different. The platform of the source management to be imported can be Solaris, Linux, Windows, SecurePlatform or IPSO.

**Usage**  
```
cma_migrate <source management directory path> <target CMA FWDIR directory>
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source database directory path</td>
<td>The root of the original source database directory; the FWDIR directory, or a copy of it.</td>
</tr>
<tr>
<td>target CMA FWDIR directory</td>
<td>The directory of the CMA that you are migrating to.</td>
</tr>
<tr>
<td></td>
<td>The target CMA cannot ever have been started before running <code>cma_migrate</code>.</td>
</tr>
<tr>
<td></td>
<td>There is no need to stop the MDS before running <code>cma_migrate</code>.</td>
</tr>
</tbody>
</table>

**Further Info.**  For further information and procedures for using the `cma_migrate` command, refer to the High End Installation and Upgrade Guide at http://supportcontent.checkpoint.com/documentation_download?ID=8752.

CPperfmon - Solaris only

**CPperfmon** is a performance monitoring utility. Call it with specific arguments to initiate or interrupt various performance monitoring processes.

**CPperfmon hw - Solaris only**

In this mode the performance monitoring tool collects hardware configuration information and either displays it to the user or stores it to the repository. There are three possible parameter configurations for the execution of the "hw" mode. Without any arguments, the command displays hardware information to the user (to screen).

**Usage**
```
CPperfmon hw
CPperfmon hw store
CPperfmon hw store=/new_path/new_sub_path
```
## Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>store</td>
<td>Stores the collected hardware information in the default repository ($MDSDIR/log/pmrepository). The generated file name contains a timestamp, and its extension is .hardware. For instance, the file 0207111112.hardware was generated at 07/11/2002 (DD/MM/YYYY) at 11:11 (local time). Using this convention the user can &quot;record&quot; the changes in the hardware configuration by executing &quot;CPperfmon hw store&quot; command after every change.</td>
</tr>
<tr>
<td>store=/new_path/new_sub_path</td>
<td>If the intended repository directory is different from the default one, the argument &quot;store=/new_path/new_sub_path&quot; should be added. The default repository base path is $MDSDIR/log, under which the performance monitor creates &quot;pmrepository&quot; subdirectory where it stores all of the data files.</td>
</tr>
</tbody>
</table>

### Further Info.

To list system swap configuration, run:
```
/usr/sbin/swap -l
```

To view swap status, run:
```
/usr/sbin/swap -s
```

### Output

Following is a sample output:
System Configuration:  Sun Microsystems  sun4u Sun Ultra 5/10
UPA/PCI (UltraSPARC-Ill 360MHz)
System clock frequency: 90 MHz
Memory size: 256 Megabytes

================================= CPUs ==========================
<table>
<thead>
<tr>
<th>Brd</th>
<th>CPU</th>
<th>Gateway</th>
<th>MHz</th>
<th>MB</th>
<th>Impl.</th>
<th>Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>360</td>
<td>0.2</td>
<td>12</td>
<td>9.1</td>
</tr>
</tbody>
</table>

================================= IO Cards ==========================
<table>
<thead>
<tr>
<th>Bus#</th>
<th>Freq</th>
<th>Brd</th>
<th>Type</th>
<th>MHz</th>
<th>Slot</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>33</td>
<td>PCI-1</td>
<td>network-SUNW,hme</td>
<td>1</td>
<td>ebus</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>33</td>
<td>PCI-1</td>
<td>SUNW,m64B</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>33</td>
<td>PCI-1</td>
<td>ide-pci1095,646</td>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No failures found in System

==================================
<table>
<thead>
<tr>
<th>swapfile</th>
<th>dev</th>
<th>swaplo</th>
<th>blocks</th>
<th>free</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/dsk/c0t0d0s1</td>
<td>136,9</td>
<td>16</td>
<td>1049312</td>
<td>740912</td>
</tr>
</tbody>
</table>

CPperfmon procmem - Solaris only

Description  Use the performance monitoring tool in this mode to schedule MDS processes memory monitoring. This mode consists of periodic sampling of address space maps of all running MDS and CMA processes. The user must provide sampling frequency (number of samples per single day). When scheduling sampling process, CPperfmon creates crontab entries with equal gap between them, i.e. if the requested frequency is twice a day, then two executions will be scheduled, one at 24:00 and one at 12:00. Address space maps sampling process (when initiated by cron) iterates through all of the defined CMAs and collects information.

Usage  CPperfmon procmem <frequency>
CPperfmon procmem <frequency> store= /new_path/new_sub_path
CPperfmon procmem off

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency</td>
<td>For continuous monitoring, specify how often to store data.</td>
</tr>
<tr>
<td>Argument</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>store</td>
<td>Store to the repository. If the intended repository directory is different from the default one, the argument &quot;store=/new_path/new_sub_path&quot; should be added. The default repository base path is $MDSDIR/log, under which the performance monitor creates &quot;pmrepository&quot; subdirectory where it stores all of the data files.</td>
</tr>
<tr>
<td>off</td>
<td>De-schedules all of the scheduled periodic tasks.</td>
</tr>
</tbody>
</table>

**Example**  
CPperfmon procmem 4 store=/tmp/mdsmon

Schedule MDS processes memory monitoring to run 4 times a day and store the results in /tmp/mdsmon/pmrepository.

---

**CPperfmon monitor - Solaris only**

**Description**  
Use the performance monitoring tool in this mode to schedule MDS processes memory monitoring. This mode consists of periodic sampling of system virtual memory statistics, system paging activity, Active processes statistics and connected clients statistics. Parameters which change frequently are sampled every 30 seconds, while other parameters are sampled every 30 minutes.

**Usage**  
CPperfmon monitor <duration>
CPperfmon monitor <duration> store=/new_path/new_sub_path
CPperfmon monitor off

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>duration</td>
<td>Duration of monitoring.</td>
</tr>
<tr>
<td>monitor off</td>
<td>De-schedules all of the scheduled monitoring processes. Removes crontab entries for low frequency processes, terminates high frequency monitoring processes.</td>
</tr>
<tr>
<td>store</td>
<td>Store to the repository. If the intended repository directory is different from the default one, the argument &quot;store=/new_path/new_sub_path&quot; should be added. The default repository base path is $MDSDIR/log, under which the performance monitor creates &quot;pmrepository&quot; subdirectory where it stores all of the data files.</td>
</tr>
</tbody>
</table>

**Example**  
CPperfmon monitor 3

Schedule system performance monitoring to run for 3 hours and use the default repository directory.

---

**CPperfmon mdsconfig - Solaris only**

**Description**  
Collects statistics and information about the user’s MDS and CMA databases. The information is either displayed to screen or stored in the repository. The user can record the changes in various configuration databases by occasionally executing the "CPperfmon mdsconfig store" command.
**Usage**
CPperfmon mdsconfig
CPperfmon mdsconfig store
CPperfmon mdsconfig store=/new_path/new_sub_path

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>store</td>
<td>Path of the CPPerfmon repository. The default repository base path is $MDSDIR/log, under which the performance monitor creates &quot;pmrepository&quot; subdirectory where it stores all of the data files.</td>
</tr>
<tr>
<td>store=/new_path/new_sub_path</td>
<td>Stores the collected databases information in the specified repository (creates a pmrepository subdirectory if necessary). The generated file name contains a timestamp, and has extension .mdsconf. For example, the file 0207111112.mdsconf was generated at 07/11/2002 (DD/MM/YYYY) at 11:11 (local time).</td>
</tr>
</tbody>
</table>

**Additional Information:**
Collected parameters are:
- Size of CMA's objects_5_0.c file.
- Size of CMA's rulebases_5_0.fws file.
- Number of network objects in CMA's objects_5_0.C file.
- Number of gateways with firewall installed among the defined network objects.
- Number of rule bases and number of rules in every rule base.

**Output:**

```
**********************************************
Customer: b52-1

Network Objects: 8
Gateways With Firewall Installed: 2
Objects Database Size: 337296
Rules Database Size: 11369

No. of Rules   Rulebase Name
-----------------------------------------
3              Exceptional
2              Standard
-----------------------------------------
5              2

**********************************************
```
**CPperfilmon summary - Solaris only**

**Description**  This mode collects data from the "mdsconfig" mode. It displays it to screen if no argument is provided. Otherwise it stores data to the repository, with a short summary of hardware configuration, and a time stamp both in local time and in UTC. Record the changes in various configuration databases by executing `CPperfilmon mdsconfig store` command every once in a while.

**Usage**
- `CPperfilmon summary`
- `CPperfilmon summary store`
- `CPperfilmon summary store=/new_path/new_sub_path`

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>store</td>
<td>Path to the repository file. The default repository base path is <code>$MDSDIR/log</code>, under which the performance monitor creates &quot;pmrepository&quot; subdirectory where it stores all of the data files.</td>
</tr>
<tr>
<td>store=/new_path/new_sub_path</td>
<td>Stores the collected databases information in the specified repository (creates the pmrepository subdirectory when necessary). The generated file name contains a timestamp and extension .mdsconf.</td>
</tr>
</tbody>
</table>

**Output**
Following is a sample output:

```
Date: Thu Jul 11 15:12:31 IDT 2002
GMT Date: Thu Jul 11 12:12:31 GMT 2002
Sun Microsystems sun4u Sun Ultra 5/10 UPA/PCI (UltraSPARC-IIIi 360MHz 256 Megabytes
/dev/dsk/c0t0d0s1 136,9 16 1049312 741040

CMA Name  Rulebase  Objects  Size  Network  Objects  Gateways  Rules  Rulebases
         Size      Size                  
  b52-1   11369    337296  8       2       5       2
  b52-2   20       317520  5       0       0       0
```

**CPperfilmon off - Solaris only**

**Description**  Use this utility to de-schedule all of the currently scheduled monitoring processes. It is equivalent to calling `CPperfilmon monitor off` and `CPperfilmon procmem off` together.

**CPperfilPack**

**Description**  This utility is used to package the performance monitor repository into single compressed file in order to send it to Check Point technical personnel.

**Usage**
- `CPperfilPack [store=<your store>] [target=<your target>]`

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>store</td>
<td>Path to the repository file. The default repository base path is <code>$MDSDIR/log</code>.</td>
</tr>
</tbody>
</table>
Argument | Description
---|---
target | CPperfPack compresses the performance monitor repository and saves it in .tar.gz file in the target directory ($MDSDIR/tmp unless specified otherwise). The extension is ".tar.gz". Example: the file CPperfMon0207111718.tar.gz was generated at 07/11/2002 (DD/MM/YYYY) at 17:18 (local time).

Example

Example CPperfPack store store =$MDSDIR/log and saves the compressed file in $MDSDIR/tmp.

cpmiquerybin

Description cpmiquerybin utility is the binary core of the Database Query Tool. (For the Database Query Tool, see mdsquerydb (on page 172).)
This command-line CPMI client connects to the specified database, executes a query and displays results as either a collection of FW-1 Sets or tab-delimited list of requested fields from each retrieved object. The target database of the query tool depends on the environment settings of the shell being used by the user. Whenever the user desires to access one of MDS databases, he/she should execute the mdsenv command, in order to define the environment variables necessary for database connection. In order to connect to a database of a certain CMA, the user should execute mdsenv command providing CMA name or IP address as a first parameter. (See also mdsenv (on page 171).)

Note - A MISSING_ATTR string is displayed when the user specifies an attribute name that does not exist in one of the objects in query result. The MISSING_ATTR string indicates that that attribute is missing.

Exit Code

0 when query succeeds, 1 if query fails, or query syntax is bad.

Usage cpmiquerybin <query_result_type> <database> <table> <query> [-a <attributes_list>]

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
</table>
| query_result_type    | Requested format of the query result. Possible values:
| database             | Name of the database to connect to, in quotes. For instance, "mdsdb" or ".". |
| table                | Table to retrieve the data from, for instance, network_objects |
| query                | Empty query ("") or a query specifying objects range for retrieval, for instance name='a*'. |
### Argument Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a attributes_list</td>
<td>If query_result_type was specified &quot;attr&quot;, this field should contain a comma delimited list of objects fields to display. Object name can be accessed using a special &quot;virtual&quot; field called &quot;<strong>name</strong>&quot;. Example: <strong>name</strong>,ipaddr</td>
</tr>
</tbody>
</table>

**Example**

- Print all network objects in the default database
  
  cpmiquerybin object "" network_objects ""

- Print hosted_by_mds and ipaddr attributes of all network objects in database "mdsdb"
  
  mdsenv
cpmiquerybin attr "mdsdb" network_objects "" -a hosted_by_mds,ipaddr

---

### dbedit

**Description**

This utility can be used in Provider-1 configuration and is further described in the *Security Management Administration Guide*. It is used in conjunction with the mdsenv command. Particular commands for accessing the MDS and CMA environment are included here.

**Usage**

- **mds**
dbedit -mds
dbedit -s <MDS_IP> -d mdsdb -u <P1_Admin> -p <password>
dbedit -s <CMA_IP> -u <CMA_Admin> -p <password>

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-mds</td>
<td>Access without user name and password. Use this command only for CMA- or MDS-configuration on the same machine as the command line is executed.</td>
</tr>
<tr>
<td>-s &lt;MDS_IP&gt;</td>
<td>Specifies the IP of the MDS Manager you want to connect to.</td>
</tr>
<tr>
<td>-u &lt;P1_Admin&gt; -p &lt;password&gt;</td>
<td>-u &lt;P1_Admin&gt; and -p &lt;password&gt; are used as a pair must specify a valid Provider-1 administrator and password for proper remote login. In addition, the computer on which the command is executed must be a valid MDS GUI Client. Beware not to expose your administrator password during remote login.</td>
</tr>
<tr>
<td>-d mdsdb</td>
<td>Edit the MDSDB database.</td>
</tr>
</tbody>
</table>

**Examples:**

**To edit the database that resides on the MDS Global database, use the following commands:**

mdsenv
dbedit -mds

**To edit the database that resides on the MDS MDSDB database, use the following commands:**

mdsenv
dbedit -mds -d mdsdb

**To edit the CMA database, use the following command:**

mdsenv CMA_Flower
dbedit 10.10.10.10 -mds

where 10.10.10.10 is the CMA IP.
To use `dbedit` on a remote MDS/CMA the computer that you are running the `dbedit` on must be defined as an authorized GUI Client of the MDS/CMA. The user must be a Provider-1 administrator and provide a user name and password:

```
dbedit -s 10.10.10.10 -u CANDACE -p ****
```

where 10.10.10.10 is the MDS or CMA IP, and **** is a password.

To edit the remote MDS MDSDB database:

```
dbedit -s 10.10.9.1 -d mdsdb -u ROGER -p ****
```

where 10.10.9.1 is the MDS IP, ROGER is an administrator and **** is a password.

To edit the remote CMA database:

```
dbedit -s 10.10.19.1 -u SAMANTHA -p ****
```

where 10.10.19.1 is the CMA IP, SAMANTHA is an administrator and **** is a password.

---

**export_database**

**Description** The `export_database` utility allows you to export an entire database into one .tgz file that can be imported into a different MDS machine. The following files can be exported:

- An entire CMA database
- An entire Security Management database
- An MDS Global Policy database

The `export_database` utility exports the database as one comprehensive file on the source machine, as opposed to `migrate_assist` which exports the database as multiple files to a remote location.

The `export_database` tool is supported on Linux, Secure Platform and Solaris 2. If you are running other platforms, use `migrate_assist` to export all files, including the Global Policy.

Before using the `export_database` utility, you must:

Copy the export tool .tgz file for your operating system to the source CMA or Security Management server. The export tool files can be found on your installation CD or on the Check Point support website, http://support.checkpoint.com.

Extract the export tool .tgz file to some path in the source machine.

A directory called `export_tools` is extracted.

Run the `export_database` commands from the `export_tools` directory.

After exporting the databases using `export_database`, transfer the .tgz files to the target machine. Import the CMA or Security Management files using `cma_migrate` and import the Global Policy file using `migrate_global_policies`.

**Usage** 

```
./export_database.sh [<path for the output file> -c <name of CMA> -h -b -l -m -g]
```

- **Exporting a CMA:**
  
  
  ```
  ./export_database.sh <path for the output file> -c <name of CMA>
  ```

- **Exporting a Security Management:**

  ```
  ./export_database.sh <path for the output file>
  ```

- **Exporting an MDS global database:**

  ```
  ./export_database.sh <path for the output file> -g
  ```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c</td>
<td>Export a CMA database</td>
</tr>
<tr>
<td>-g</td>
<td>Export a Global Policy database</td>
</tr>
<tr>
<td>-b</td>
<td>Batch mode - run command without asking anything</td>
</tr>
</tbody>
</table>
### Argument | Description
--- | ---
-m | Include the SmartMap database.
-l | Include the log database.
-h | Display usage

**Example**

To export the database of a CMA, **CMA1**, including its log database to a file path, **/var/tmp**, use the following command:

```
./export_database.sh /var/tmp -c CMA1 -l
```

To export the database of a Security Management, including its Smartmap database to a file path, **/var/tmp**, use the following command:

```
./export_database.sh /var/tmp -m
```

To export an MDS's Global Policy to a file path, **/var/for_export**, use the following command:

```
./export_database.sh /var/for_export -g
```

### mcd bin | scripts | conf

**Description**

This command provides a quick directory change to $FWDIR/<param>.

**Example**

```
mdsenv MyCma1
```

Brings you to: /opt/CPmds-R70/customers/MyCma1/CPsuite-R70/fw1/conf.

### mds_backup

The **mds_backup** command backs up binaries and data from your MDS to the working directory. This command requires superuser privileges.

**mds_backup** executes the **gtar** command on product root directories containing data and binaries, and backs up all files except those specified in **mds_exclude.d** ($MDSDIR/conf) file. The collected information is stored in a single .tgz file. This .tgz file name consists of the backup date and time, which is saved in the current working directory. For example: 13Sep2002-141437.mdsbk.tgz

**To perform a backup:**

1. Execute **mds_backup** from any location outside the product directory tree to be backed up. This becomes the working directory.
2. Upon completion of the backup process, copy the backup .tgz file, together with the **mds_restore**, **gtar** and gzip command files, to your external backup location.

**Usage**

```
mds_backup [-g -b { -d <target dir name> } -v -h]
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>-d</td>
<td>Specifies a directory store for the backup file. When not specified, the backup file is stored in the current directory. You cannot store the backup file in any location inside the product root directory tree.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>-v</code></td>
<td>Verbose mode - lists all files to be backed up, but do not perform the backup operation.</td>
</tr>
<tr>
<td><code>-l</code></td>
<td>Exclude logs from the backup.</td>
</tr>
<tr>
<td><code>-h</code></td>
<td>Help - displays help text.</td>
</tr>
</tbody>
</table>

**Comments**

When using the `-g` or `-b` options, make sure that no GUI clients or SmartReporter servers are connected. Otherwise, the backup file may contain inconsistencies due to database changes made during the backup process.

It is important not to run mds_backup from any of the directories that will be backed up. For example, when backing up an MDS, do not run mds_backup from `/opt/CPmds-R70` since it is a circular reference (backing up directory that you need to write into).

Active log files are not backed up, in order to avoid read-during-write inconsistencies. It is recommended to perform a log switch prior to the backup procedure.

**Further Info.** The MDS configuration can be backed up without backing up the log files. Such a backup will usually be significantly smaller in size than a full backup with logs. To backup without log files, add the following line to the file `$MDSDIR/conf/mds_exclude.dat`:

```
log/**
```

**mds_restore**

**Description**

Restores a MDS that was previously backed up with mds_backup. For correct operation, mds_restore should be restored onto a clean MDS installation.

**Usage**

```
./mds_restore <backup file>
```

**Note** - The mds_restore command must use the script that was created in the directory into which the backup file was created.

**mds_user_expdate**

**Description**

This command is used to modify the expiration date of the users defined in the CMAs.

**Usage**

```
mds_user_expdate
```

**Further Info.** After entering the command mds_user_expdate, you are required to choose between two modes:

- Run on all CMAs located on the MDS where the command is executed.
- Run on a specific CMA.

After selecting the run method, specify the expiration date in the following format: `<dd-mmm-yyyy>`, e.g., `24-Feb-2003`.

**Comments**

Make sure to disconnect any GUI client before running this utility so that the changes made by the command will not be overwritten by the client. This utility can work only on Active CMAs. After running this utility, you will need to manually synchronize your CMAs.

**mdscmd**

**Description**

This command is used to execute different commands on the MDS system. It connects to an MDS Manager as a CPMI client and causes it to execute one of the specified commands described below. Connection parameters `[\(-m \text{ MDS server} -u \text{ user} -p \text{ password}\)` are required in order to log into a remote MDS manager. If these arguments are omitted, mdscmd connects to the local machine. As the command is a CPMI client, it has an audit log.
Usage  mdscmd <sub command and sub command parameters> [-m MDS server -u user -p password]
mdscmd help

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-m MDS server</td>
<td>For remote login; specifies the name or IP address of the MDS Manager you want to connect to.</td>
</tr>
<tr>
<td>-u user -p password</td>
<td>Used as a pair, they must specify a valid Superuser administrator and password for remote login. In addition, the computer on which the command is executed must be a valid MDS GUI Client. Beware not to expose your administrator password during remote login.</td>
</tr>
<tr>
<td>help</td>
<td>Print the usage of an mdscmd command and a list of examples.</td>
</tr>
</tbody>
</table>

mdscmd addcustomer

Description  This command is used to create a Customer, locally or remotely. If run remotely, add login details. A first CMA can be created at the same time using this command.

Usage  mdscmd addcustomer <customerName> [-n cma_name] [-i IP] [-t target_mds] [-m mds -u user -p password]

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CustomerName</td>
<td>Specifies the name of the Customer to add.</td>
</tr>
<tr>
<td>-n cma_name</td>
<td>A first CMA is created when the customer is created, using the name you provide (cma_name).</td>
</tr>
<tr>
<td>-m mds</td>
<td>Specifies the name or IP of the MDS Manager you want to connect to.</td>
</tr>
<tr>
<td>-u user and -p password</td>
<td>Used as a pair, they must specify a valid Superuser administrator and password for remote login. In addition, the computer on which the command is executed must be a valid MDS GUI Client. Beware not to expose your administrator password during remote login.</td>
</tr>
<tr>
<td>-i IP</td>
<td>Specify the virtual IP address (VIP) assigned to the CMA. If -n cma_name is used but no IP address is specified, yet a VIP range has been defined for the MDS, the next available VIP is assigned to the CMA. If you use -i IP without -n cma_name, a name is automatically generated with the format: &lt;customer name&gt;_First_CMA.</td>
</tr>
<tr>
<td>-t target_mds</td>
<td>Specify the MDS to which the CMA is added. If not specified, the mdscmd attempts to add the CMA to the MDS to which it is connected.</td>
</tr>
</tbody>
</table>
Example Add a new Customer named BestCustomer without a CMA:
mdscmd addcustomer BestCustomer
Add a new Customer named BestCustomer with a CMA named BestCustomerCma, using the Virtual IP address 4.4.4.4:
mdscmd addcustomer BestCustomer -n BestCustomerCma -i 4.4.4.4

**mdscmd addcma**

**Description** A customer must already be created in order to use this command.

**Usage** mdscmd addcma <customerName> [-i IP] [-n cma_name] [-t target_mds] [-m mds -u user -p password]

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CustomerName</td>
<td>Specifies the name of the Customer to which the CMA is added.</td>
</tr>
<tr>
<td>-n cma_name</td>
<td>Create a CMA with this name. If you do not specify -n cma_name, cma_name is generated automatically in the format: &lt;customer name&gt;_First_CMA.</td>
</tr>
<tr>
<td>-i IP</td>
<td>Specify the virtual IP address (VIP) used by the CMA. If -n cma_name is used but no IP address is specified, yet a VIP range has been defined for the MDS, the next available VIP is assigned to the CMA. If you use -i IP without -n cma_name, a name is automatically generated with the format: &lt;customer name&gt;_First_CMA.</td>
</tr>
<tr>
<td>-t target_mds</td>
<td>Define the MDS to which the CMA is added. If you do not specify this parameter, the mdscmd attempts to add the CMA to the MDS to which it is connected.</td>
</tr>
<tr>
<td>-m mds</td>
<td>Specifies the name or IP of the MDS Manager you want to connect to.</td>
</tr>
<tr>
<td>-u user and -p password</td>
<td>Used as a pair, they must specify a valid Superuser administrator and password for remote login. In addition, the computer on which the command is executed must be a valid MDS GUI Client. Beware not to expose your administrator password during remote login.</td>
</tr>
</tbody>
</table>

Example Add a new CMA to the Customer BestCustomer using the Virtual IP address 4.4.4.4:
mdscmd addcma BestCustomer -i 4.4.4.4
Add a new CMA to the Customer BestCustomer named BestCustomerCma using the Virtual IP address 4.4.4.4:
mdscmd addcma BestCustomer BestCustomerCma -i 4.4.4.4
Add a new CMA to the Customer BestCustomer on host AnotherMds using the Virtual IP address 4.4.4.4:
mdscmd addcma BestCustomer -i 4.4.4.4 -t AnotherMds

**mdscmd addclm**

**Description** Use the addclm sub-command to add a CLM to an existing Customer. addclm adds either the first or any subsequent CLM of the Customer. To add a CLM to a Customer, it must already have at least one CMA.

**Usage** mdscmd addclm <customerName> [-i IP] [-t target_mds] [-m mds -u user -p password]
**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CustomerName</td>
<td>Specifies the name of the Customer to which the CLM is added.</td>
</tr>
<tr>
<td>-i IP</td>
<td>Specify this parameter to select the Virtual IP address (VIP) to be used by the CLM.</td>
</tr>
<tr>
<td>-t target_mds</td>
<td>Define the MDS to which the CLM is added. If you do not specify this parameter, the mdscmd attempts to add the CMA to the MDS to which it is connected.</td>
</tr>
<tr>
<td>-m mds</td>
<td>Specifies the name or IP of the MDS Manager you want to connect to.</td>
</tr>
<tr>
<td>-u user and -p password</td>
<td>Used as a pair, they must specify a valid Superuser administrator and password for remote login. In addition, the computer on which the command is executed must be a valid MDS GUI Client. Beware not to expose your administrator password during remote login.</td>
</tr>
</tbody>
</table>

**mdscmd deletecustomer**

**Description**

Use this command to delete an existing Customer. When deleting a Customer, you also delete the Customer's CMAs.

**Usage**

`mdscmd deletecustomer <customerName> -m mds -u user name -p password`

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CustomerName</td>
<td>Specifies the name of the Customer to be deleted.</td>
</tr>
<tr>
<td>-m mds</td>
<td>Specifies the name or IP of the MDS Manager you want to connect to.</td>
</tr>
<tr>
<td>-u user and -p password</td>
<td>Used as a pair, they must specify a valid Superuser administrator and password for remote login. In addition, the computer on which the command is executed must be a valid MDS GUI Client. Beware not to expose your administrator password during remote login.</td>
</tr>
</tbody>
</table>

**Example**

Delete the Customer BestCustomer

```
mdscmd deletecustomer BestCustomer
```

**mdscmd deletecma**

**Description**

Use this command to delete an existing CMA.

**Usage**

`mdscmd deletecma <customerName> [-n cma_name | -i IP ] [-m mds -u user -p password]`

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CustomerName</td>
<td>Specifies the name of the Customer whose CMA is deleted.</td>
</tr>
<tr>
<td>-n cma_name</td>
<td>Specify the name of the CMA to be deleted.</td>
</tr>
</tbody>
</table>
### mdscmd deletecma

**Description** Use this command to delete an existing CMA.

**Usage**
```
mdscmd deletecma <customerName> [-i IP] [-m mds -u user -p password]
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-i IP</td>
<td>Specify this parameter to delete the CMA by its Virtual IP address.</td>
</tr>
<tr>
<td>-m mds</td>
<td>Specifies the name or IP of the MDS Manager you want to connect to.</td>
</tr>
<tr>
<td>-u user and -p password</td>
<td>Used as a pair, they must specify a valid Superuser administrator and password for remote login.</td>
</tr>
</tbody>
</table>

**Comments**
- One or the other of the following parameters must be specified:
  - -i IP — specify this parameter to delete the CMA by its Virtual IP address.
  - -n cma_name — Specify this parameter to delete the CMA by its name (set in cma_name).

**Example**
Delete a CMA from the Customer BestCustomer (by stating its virtual IP address — 4.4.4.4):
```
mdscmd deletecma BestCustomer -i 4.4.4.4
```

Delete a CMA from the Customer BestCustomer, using the CMA's name — BestCustomerCMA, and running from the remote host AnotherMds (using user name: MyUser and password: MyPassword):
```
mdscmd deletecma BestCustomer -n BestCustomerCMA -m AnotherMds -u MyUser -p MyPassword
```

### mdscmd deleteclm

**Description** Use this command to delete an existing CLM.

**Usage**
```
mdscmd deleteclm <customerName> [-i IP] [-m mds -u user -p password]
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CustomerName</td>
<td>Specifies the name of the Customer to add.</td>
</tr>
<tr>
<td>-i IP</td>
<td>Specify this parameter to select the Virtual IP address (VIP) to be used by the CLM.</td>
</tr>
<tr>
<td>-m mds</td>
<td>Specifies the name or IP of the MDS Manager you want to connect to.</td>
</tr>
<tr>
<td>-u user and -p password</td>
<td>Used as a pair, they must specify a valid Superuser administrator and password for remote login.</td>
</tr>
</tbody>
</table>

### mdscmd enableglobaluse

**Description** Use this command to connect a customer gateway to a Global VPN Community. Executing this command with a customer's name and a gateway name, creates a global gateway object and a VPN Domain object for the specific customer gateway in the Global database.

The global name will be gGW1_of_CUST1 for the gateway GW1 and customer CUST1. The VPN domain object will receive the same name as the global gateway object with a '_Domain' extension.

**Usage**
```
mdscmd enableglobaluse <customerName> <gatewayName> [-g globalName] [-m mds -u user -p password]
```

**Syntax**
<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CustomerName</td>
<td>Specifies the name of the Customer to which the CMA belongs.</td>
</tr>
<tr>
<td>gatewayName</td>
<td>Specifies the name of the gateway.</td>
</tr>
<tr>
<td>-g global name</td>
<td>This command is used to determine the global gateway object name. If [-g global name] is omitted, the global name will be gGW1_of_CUST1 for the gateway GW1 and customer CUST1</td>
</tr>
<tr>
<td>-m mds</td>
<td>Specifies the name or IP of the MDS Manager you want to connect to.</td>
</tr>
<tr>
<td>-u user and -p password</td>
<td>Used as a pair, they must specify a valid Superuser administrator and password for remote login. In addition, the computer on which the command is executed must be a valid MDS GUI Client. Beware not to expose your administrator password during remote login.</td>
</tr>
</tbody>
</table>

**Comments:** mdscmd enableglobaluse is equivalent to enabling global use of a gateway from MDG.

**mdscmd disableglobaluse**

**Description** Use this command to remove a customer global gateway object and VPN Domain object from the global database.

**Usage** mdscmd disableglobaluse <customerName> <gatewayName> [-m mds -u user -p password]

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CustomerName</td>
<td>Specifies the name of the Customer to which the CMA belongs.</td>
</tr>
<tr>
<td>gatewayName</td>
<td>Specifies the name of the gateway.</td>
</tr>
<tr>
<td>-m mds</td>
<td>Specifies the name or IP of the MDS Manager you want to connect to.</td>
</tr>
<tr>
<td>-u user and -p password</td>
<td>Used as a pair, they must specify a valid Superuser administrator and password for remote login. In addition, the computer on which the command is executed must be a valid MDS GUI Client. Beware not to expose your administrator password during remote login.</td>
</tr>
</tbody>
</table>

**Comments** mdscmd disableglobaluse is equivalent to disabling the global use of a gateway from MDG.

**mdscmd startcma**

**Description** Use this command to start an existing CMA.

**Usage** mdscmd startcma <customerName> <-n cma_name | -i IP > -m mds -u user name -p password

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CustomerName</td>
<td>Specifies the name of the Customer to which the CMA belongs.</td>
</tr>
</tbody>
</table>
### Argument Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-n cma_name</td>
<td>Specify the name of the CMA to be started.</td>
</tr>
<tr>
<td>-i IP</td>
<td>Specify this parameter to select the CMA's Virtual IP address.</td>
</tr>
<tr>
<td>-m mds</td>
<td>Specifies the name or IP of the MDS Manager you want to connect to.</td>
</tr>
<tr>
<td>-u user and -p password</td>
<td>Used as a pair, they must specify a valid <strong>Superuser</strong> administrator and password for remote login. In addition, the computer on which the command is executed must be a valid MDS GUI Client. Beware not to expose your administrator password during remote login.</td>
</tr>
</tbody>
</table>

#### Comments

One or the other of the following parameters *must* be specified:

- -i IP — Specify this parameter to start the CMA by its Virtual IP address.
- -n cma_name — Specify this parameter to start the CMA by its name (`cma_name`).

#### Example

Run the CMA `BestCustomerCMA`, which is defined for the Customer `BestCustomer`:

```bash
mdscmd startcma BestCustomer -n BestCustomerCMA
```

### mdscmd stopcma

**Description**

Use this command to stop a running CMA.

**Usage**

```bash
mdscmd stopcma <customerName> <-n cma_name | -i IP > -m mds -u user name -p password
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CustomerName</td>
<td>Specifies the name of the Customer to which the CMA belongs.</td>
</tr>
<tr>
<td>-n cma_name</td>
<td>Specify the name of the CMA to be stopped.</td>
</tr>
<tr>
<td>-i IP</td>
<td>Specify this parameter to select the CMA's Virtual IP address.</td>
</tr>
<tr>
<td>-m mds</td>
<td>Specifies the name or IP of the MDS Manager you want to connect to.</td>
</tr>
<tr>
<td>-u user and -p password</td>
<td>Used as a pair, they must specify a valid <strong>Superuser</strong> administrator and password for remote login. In addition, the computer on which the command is executed must be a valid MDS GUI Client. Beware not to expose your administrator password during remote login.</td>
</tr>
</tbody>
</table>

#### Comments

One or the other of the following parameters *must* be specified:

- -i IP — Specify this parameter to stop the CMA using its Virtual IP address.
- -n cma_name — Specify this parameter to stop the CMA using its name (`cma_name`).

#### Example

Stop the CMA `BestCustomerCMA`, which is defined for the Customer `BestCustomer`:

```bash
mdscmd stopcma BestCustomer -n BestCustomerCMA
```

### mdscmd migratcma

**Description**

Use this command to migrate/import an existing source database (from a Security Management server or CMA) into another CMA.
You can use `mdscmd migratecma` to import files created using the `export_database` tool.

**Usage**

```
mdscmd migratecma <customerName> <-l cma_path> <-n cma_name>
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CustomerName</td>
<td>Specifies the name of the Customer to which the new CMA belongs.</td>
</tr>
<tr>
<td>-l cma_path</td>
<td>Specifies the path containing the <code>conf</code> directory migrated into the new CMA.</td>
</tr>
<tr>
<td>-n cma_name</td>
<td>Specifies the name of the new CMA into which the source database information is migrated.</td>
</tr>
</tbody>
</table>

**Example**

Migrate a source database from an NGX (R60) version CMA, named `MyFirstCMA`, into the CMA `BestCustomerCMA`, defined for the Customer `BestCustomer`:

```
mdscmd migratecma BestCustomer -l /opt/CPmds-R60/customers/ MyFirstCMA/CPfw1-R60 -n BestCustomerCMA
```

See also `cma_migrate` (on page 154).

### mdscmd mirrorcma

**Description**

Use this command to mirror the CMA configuration from one MDS to another MDS. This command is used to create CMA High Availability. This command parses all Customers and checks which Customers have a single CMA defined. If a Customer has a CMA on the source MDS, a secondary CMA is created on the target MDS.

**Usage**

```
mdscmd mirrorcma -s source_mds -t target_mds [ -m mds -u user -p password ]
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s source_mds</td>
<td>Specifies the name of the MDS the mirroring is performed from.</td>
</tr>
<tr>
<td>-t target_mds</td>
<td>Specifies the name of the MDS the mirroring is targeted toward.</td>
</tr>
<tr>
<td>-u user and -p password</td>
<td>Used as a pair, they must specify a valid Superuser administrator and password for remote login. In addition, the computer on which the command is executed must be a valid MDS GUI Client. Beware not to expose your administrator password during remote login.</td>
</tr>
</tbody>
</table>

**Example**

Mirror the configuration from the MDS `FirstMDS` to the MDS `SecondMDS`:

```
mdscmd mirrorcma -s FirstMDS -t SecondMDS
```

### mdsenv

**Description**

This command prepares the shell environment variables for running MDS level command lines or specific CMA command lines. Without an argument, the command sets the shell for MDS level commands (`mdsstart`, `mdsstop`, etc.).

**Usage**

```
mdsenv [ cma name ]
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cma name</td>
<td>With a CMA name, the command prepares the shell for the CMA's command line (fw load etc.)</td>
</tr>
</tbody>
</table>
**mdsquerydb**

**Description** The `mdsquerydb` command runs the Database Query Tool. The purpose of the Database Query Tool is to allow advanced users to create UNIX shell scripts which can easily access information stored inside the CheckPoint Security Management server databases. These include the Global Database (which are usually accessed from the Global SmartDashboard), MDS Database (usually accessed from the MDG) and the CMA databases (usually accessed from SmartDashboard). Just as the `mdscmd` tool allows users to write UNIX shell scripts that add, remove or alter specified Provider-1 database objects, the Database Query Tool allows users to access the information related to these database objects. The command is used with specific arguments to perform various queries on Security Management server databases.

**Usage** `mdsquerydb key_name [-f output_file_name]`

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>key_name</code></td>
<td>Query key, that must be defined in the pre-defined queries configuration file.</td>
</tr>
<tr>
<td><code>-f output_file_name</code></td>
<td>Write query results to file with the specified file name, instead of to the standard output.</td>
</tr>
</tbody>
</table>

**Example**

To retrieve list of all defined keys:

```
mdsquerydb
```

To send the list of customers in the MDS database to the standard output:

```
mdsenv
mdsquerydb Customers
```

To retrieve the list of network objects in the Global database and place the list in:

```
/tmp/gateways.txt:
mdsenv
mdsquerydb NetworkObjects -f /tmp/gateways.txt
```

To retrieve the list of gateways objects of the CMA called `cma1`:

```
mdsenv cma1
mdsquerydb Gateways -f /tmp/gateways.txt
```

**Comments** The purpose of the Database Query Tool is to provide advanced users of Provider-1 with means of querying different Security Management server databases from UNIX shell scripts. Some Database queries are pre-defined in the configuration file. The configuration file (`queries.conf`) can be found in `$MDSDIR/conf`. The file should not be edited by the end-users in any case.

**mdsstart**

**Description** This command starts the MDS server and all CMAs. You can reduce the time it takes to start and stop the MDS if you have many CMAs. To do so, set the variable `NUM_EXEC_SIMUL` to the number of CMAs to be launched or stopped simultaneously. When this variable is not defined, the system attempts to start or stop up to 10 CMAs simultaneously.

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

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-m</code></td>
<td>Starts only the MDS server and not the CMAs.</td>
</tr>
<tr>
<td><code>-s</code></td>
<td>Starts the CMAs sequentially: waits for each CMA to come up before starting the next.</td>
</tr>
</tbody>
</table>
mdsstat

**Description**  This command utility gives detailed information on the status of the processes of the MDS and CMAs, the up/down status per process.

**Usage**  mdsstat [-h] [-m] [<cma name>]

**Syntax**

<table>
<thead>
<tr>
<th>Argument</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 MDS only.</td>
</tr>
<tr>
<td>cma name</td>
<td>The name of the CMA whose status is tested.</td>
</tr>
</tbody>
</table>

**Further Info.**  Status Legend:

- **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 container MDS.

mdsstop

**Description**  This command stops the MDS server and all the CMAs. You can reduce the time it takes to start and stop the MDS if you have many CMAs. To do so, set the variable `NUM_EXEC_SIMUL` to the number of CMAs to be launched or stopped simultaneously. When this variable is not defined, the system attempts to start or stop up to 10 CMAs simultaneously.

**Usage**  mdsstop [-m]

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-m</td>
<td>Use the -m option to stop the MDS server without stopping CMAs.</td>
</tr>
</tbody>
</table>

merge_plug-in_tables

**Description**  The `merge_plug-in_tables` utility is included in the `export_database` utility. It searches for all CMA or Security Management plug-ins and merges the plug-in tables with the CMA or Security Management tables.

In Linux, the `merge_plug-in_tables` tool runs automatically when you run the `export_database` tool and its output becomes part of the CMA database .tgz file.

If you have a Security Management running on FreeBSD, IPSO 6.x, or Windows, you can and should use `merge_plug-in_tables` to consolidate your plug-in information before exporting files using `migrate_assist`.

**Before using the `merge_plug-in_tables` utility, you must:**

1. Copy the export tool .tgz file for your operating system to the source CMA or Security Management machine. The export tool files can be found on your installation CD.
2. Extract the export tool .tgz file to some path in the source machine.
   - A directory called `export_tools` is extracted.
3. Run the `merge_plug-in_tables` command from the `export_tools` directory.

**Usage**  merge_plug-in_tables -p conf_dir> [-s] [-h]

where `-p conf_dir>` is the path of `$FWDIR` directory of the CMA/Security Management, `-s` performs the utility in silent mode (default is interactive mode), and `-h` displays usage.
Example

To merge the plug-in tables of a CMA, CMA1, run the following commands:

```
mdsenv cma1
merge_plug-in_tables -p "$FWDIR"
```

**migrate_assist**

**Description**  
This utility is a helper utility for `cma_migrate`. It copies all relevant files from the original source database (from a Security Management server or CMA) to the MDS machine. It uses FTP to transfer the original source database directories to current disk storage. This file copy is NOT encrypted. Once finished with `migrate_assist`, you can run `cma_migrate`, whose input directory is the output directory of `migrate_assist`.

It is recommended to use the `export_database` tool instead of `migrate_assist` if your source machine is running on a running Linux.

**Usage**

```
$ migrate_assist
migrate_assist <source machine name/ip> <source FWDIR folder> <user name> <password> <target folder> <source CPDIR folder>
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;user name&gt; &lt;password&gt;</code></td>
<td>The user name and password are needed to gain access to the remote MDS via ftp.</td>
</tr>
<tr>
<td>source machine name/ip</td>
<td>The original Security Management server or CMA’s resolvable DNS name or IP.</td>
</tr>
<tr>
<td>source FWDIR folder</td>
<td>The original Security Management server or CMA’s source FWDIR folder path.</td>
</tr>
<tr>
<td>source CPDIR folder</td>
<td>If the source CPDIR parameter is specified, <code>migrate_assist</code> assumes the source database is NG or later, and imports the source CPDIR folder to the target folder as well.</td>
</tr>
</tbody>
</table>

**Further Info.**

You can run the `cma_migrate` utility (or use the Import Customer Management Add-on command in the MDG) after using this utility. The source folder for these actions should be the destination folder of `migrate_assist`.

When migrating from an NG source Security Management server or CMA, the Name and IP address of the Primary Security Management server/CMA object become the Name and IP address of the new CMA, and are adjusted accordingly by `cma_migrate`. An ftp server must be running on the source machine.

Before running `migrate_assist`, use the `merge_plug-in_tables` tool if you have plug-ins installed.

**migrate_global_policies**

**Description**  
This utility transfers (and upgrades, if necessary) the global policies database from one MDS to the global policies database of another MDS. `migrate_global_policies` replaces all existing Global Policies and Global Objects. Each of the existing Global Policies is saved with a `*.pre_migrate` extension.

If you only migrate the global policies (without the CMAs) to a new MDS, you should disable any gateways that are enabled for global use.

You can migrate global policies from the following Provider-1 versions:

- R60, R60A, R61, R62, R65, R70

You can use `migrate_global_policies` to import files created using the `export_database` tool.

**Usage**

```
migrate_global_policies <path>
```

**Syntax**
<table>
<thead>
<tr>
<th><strong>Argument</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>path</td>
<td>Specifies the <strong>fully qualified</strong> path to the directory where the global policies files, originally exported from the source MDS ($MDSDIR/conf), are located.</td>
</tr>
</tbody>
</table>

**Example**

migrate_global_policies /tmp/exported_global_db.22Jul2007-124547.tgz
A
A Distributed Provider-1 Network • 38
A Standalone Provider-1 Network • 37
A Typical Scenario • 37
Access Control at the Network Boundary • 95, 101
Access Control in Global VPN • 101
Activate Management Plug-ins • 67
Activating Plug-ins • 63
Active Versus Standby • 106
Add a CLM • 123
Add a Secondary CMA • 116
Add CMA License Details • 68
Adding a New MDS or MLM • 50
Adding another MDS • 114
Adding Licenses using the MDG • 48
Administrators • 21, 92, 134
Applying Global Rules to Gateways by Function • 76
Architecture and Processes • 139
Asking yourself the right questions... • 32
Assign Administrators to the Customer • 67
Assign Computers on which Administrators use the MDG • 67
Assign Global Policy • 67
Assign to Many Customers
   How To Assign/Install from a Global Policy Object • 87
Assign to One Customer
   Assign/Install from a Customer Object • 87
Assigning a CMA • 59
Assigning a Computer • 59
Assigning a Different Global Policy • 86
Assigning Global Policies to VPN Communities • 83
Assigning Global Policy • 83
Assigning Global Policy for the First Time • 83
Assigning Groups • 62
Assigning IPS Profiles to Gateways • 82
Assigning or Installing a Global Policy • 87
Assigning Policy for the First Time • 85
Audit Logging • 153
Authenticating the Administrator • 28
Authenticating via External Authentication Servers • 29
Authentication Between Gateways • 96
Automatic CMA Synchronization • 116
Automatic Gateway Policy Installation • 83
Automatic Log Export to Oracle Database • 121
Automatic Start of MDS Processes, Files in /etc/rc3.d, /etc/ini.t.d • 141
Automatic Synchronization for Global Policies Databases • 115
B
Basic Elements • 13
Blocking Suspicious Connections • 138
C
Changing Administrators • 69
Changing GUI Clients • 70
Changing the Status Collection Cycle • 144
Check Point Registry • 141
Check Point System Counters • 138
Checking a CMA's Policy • 132
Checking a Gateway's Current Policy • 133
Checking CMA Status • 71
Checking the Status of Components in the System • 129
Choosing Fields to Export • 122
Choosing Log Export Fields • 124
Choosing the Right Environment • 33
Choosing the Right Platform • 33
Choosing your deployment for MDS Managers and Containers • 35
CMA Backup using Security Management Server • 107
CMA Database • 143
CMA Database Synchronization • 112
CMA High Availability • 21, 104
CMA Level Processes • 142
cma_migrate • 153
Collection of Changes in Objects • 144
Command Line Reference • 153
Commands and Utilities • 147
Configuration • 66, 87, 114
Configuring a CMA • 70
Configuring a New Customer • 66
Configuring an MDS to Enable Log Export • 124
Configuring Global VPN Communities • 102
Configuring Log Export Profiles • 124
Connected Administrators • 135
Connecting to a Customer Network • 60
Connecting to a Remaining MDS • 117
Connection Between MDSs • 145
Connections to a Customer Network • 98
Connectivity Between Different Processes • 144
Consider the Following Scenario... • 33
Considerations • 40, 101
Considerations For Global Policy Assignment • 85
Conversion Considerations • 99
Copying Search Results • 148
CPM Protocol • 31
cpmiquerybin • 159
CPPerfmon - Solaris only • 153
CPPerfmon hw - Solaris only • 153
CPPerfmon mdscconfig - Solaris only • 156
CPPerfmon monitor - Solaris only • 156
CPPerfmon off - Solaris only • 158
CPPerfmon procmem - Solaris only • 155
CPPerfmon summary - Solaris only • 158
CPPerfPack • 158
Create the CMA • 68
Creating a Global Policy through Global SmartDashboard • 78
Creating a Mirror of an Existing MDS • 114
Creating a New IPS Profile • 80
Creating a Primary MDS Manager • 47
Creating Administrator and Customer Groups • 68
Creating Administrator Selection Groups • 68
Creating Customer Policies • 93
Creating Customer Selection Groups • 68
Creating Customers
A Sample Deployment • 57
Creating more Customers • 61
Creating more MDSs • 62
Cross Domain Logging • 122
Cross-CMA Search • 147
Cross-MDS Synchronization • 113
Customer Details • 67
Customer Log Module • 20
Customer Log Module (CLM) Licenses • 42
Customer Management • 56
Customer Management Add-on (CMA) • 91
Customer Management Add-on (CMA) Licenses • 41
Customer Policies • 132

D
Data Centers • 10
dbedit • 160
Defining a Security Policy for the Gateway • 54
Deleting a CLM • 123
Deleting a CMA • 71
Deleting a Customer • 70
Deleting an MDS • 53
Dynamic Objects and Dynamic Global Objects • 76

E
Editing an IPS Profile • 81
Enabling a Customer Gateway to Join a Global VPN Community • 102
Enabling Connections Between Different Components of the System • 54
Enabling OPSEC • 44
Environment Variables • 141
Example • 149
Enterprise Deployment • 14
MSP Deployment • 13
Export Profiles • 122
export_database • 161
Exporting Logs • 121
Exporting the List Pane's Information to an External File • 128

F
Failure Recovery in High Availability Deployments • 117
File Constraints for P1Shell Commands • 150
Filtering • 129
Footnotes: • 114
Further Licensing Detail • 41

G
Gateway Global Names • 100
Gateway Licenses • 42
Gateway Policies • 133
General Provider-1 Commands • 150
Global IPS • 79
Global Names Format • 90
Global Object Transfer Method • 86
Global or Neighbor VPN Gateway • 100
Global Policies • 132
Global Policies and the Global Rule Base • 74
Global Policies Database • 110
Global Policies Database Synchronization • 111
Global Policies Tab • 89
Global Policy Database • 143
Global Policy History File • 86
Global Policy Management • 72
Global Services • 75
Global SmartDashboard • 75
Global VPN Communities • 99, 134
GUI Clients • 136

H
Hardware Requirements and Recommendations • 39
High Availability • 21, 33, 104, 133
High Availability Mode • 65
High Availability Scenarios • 145
How Synchronization Works • 111
How VPN Works • 96

I
ICA (Internal Certificate Authority) Database for CMAs • 110
ICA (Internal Certificate Authority) Database for MDSs • 110
Initializing Synchronization between MDSs • 115
Installing and Configuring Security Gateways • 92
Installing Plug-ins • 63
Installing the VSX Bundle License • 43
Introducing Management Plug-ins • 63
Introduction • 8
Introduction to Considerations for Global Policy Assignment • 85
Introduction to Creating Customers
A Sample Deployment • 57
Introduction to Global IPS • 79
Introduction to Global SmartDashboard • 75
Introduction to Security Policies in Provider-1 • 72
Introduction to the Management Model • 21
Introduction to the Trust Model • 25
IP Allocation & Routing • 43
IP Allocation for CMAs • 62
IPS in Global SmartDashboard • 80
IPS Profiles • 80
Issues Relating to Different Platforms • 145

J
Joining a Gateway to a Global VPN Community • 101

L
Large Enterprises • 10
Large Scale Management Processes • 145
Launching the MDG • 47
License Violations • 42
Licensing • 33
Provisioning Provider-1 • 46

R

Real-Time Network Monitoring with SmartView Monitor • 137
Re-assigning Global Policies • 83
Re-assigning Global Policies to Multiple Customers • 84
Re-assigning Global Policy to an Individual Customer • 84
Reassigning/Installing a Global Policy on Customers • 87
Re-authenticating when using SmartConsole Clients • 30
Recovery from Failure of the Only Manager MDS • 118
Recovery with a Functioning Manager MDS • 117
Recreating the Provider-1 Deployment • 118
Reinstalling a Customer Policy on Customer Gateways • 88
Remove a Global Policy from a Single Customer • 89
Remove a Global Policy from Multiple Customers • 89
Removing Global IPS from a CMA • 82
Replacing the Trial Period License • 42
Reporting Server Processes • 145
Resetting Customer CMAs • 117
Restoring the High Availability Deployment • 118
Revision Control • 94
Routing Issues in a Distributed Environment • 33

S

Safety comes first • 32
Sample Deployment - Administrator Setups • 24
Secure Internal Communication (SIC) • 26
Security Management backup server Setup Procedure • 107
Security Policies in Provider-1 • 21, 72
Selecting a Different MDS to be the Active MDS • 115
Selecting MDS and CMA Licenses • 40
Setting up a Mirror CMA • 106
Setting up a New MDS and Initiating Synchronization • 109
Setting Up Administrators • 33
Setting up Customer Gateway to Send Logs to the CLM • 123
Setting Up External Authentication • 29
Setting Up Logging • 122
Setting up MDS Managers and Containers in Mirror Sites • 35
Setting up Synchronization • 113
Setting up the Provider-1 Environment • 36
Setting Up Your Network Topology • 47
Setup Considerations • 62
Showing and Hiding Selected List Pane Columns • 129
Simplified VPN • 98
SmartConsole Client Applications • 23, 92
SmartReporter Reports • 138
Standalone Gateway/Security Management • 53
Standard Check Point Environment Variables • 141
Start the Add Customer Wizard • 66
Starting or stopping a CLM • 123
Starting or Stopping a CMA • 70
Starting P1Shell • 149
Status Collection • 144
Step 1 - In the MDG • 102
Step 2 - In Global SmartDashboard • 102
Step 3 - In the MDG • 102
Structure of CMA Directory Trees • 140
Subscribing Customers to IPS Service • 81
Subsequent Synchronization for MDSs • 115
Synchronize ClusterXL Gateways • 116
Synchronizing Clocks • 50
Synchronizing the CLM Database with the CMA Database • 124
Synchronizing the Global Policy Database • 77

T

The Check Point Solution • 12
The Global Policy as a Template • 74
The Management Model • 21
The MDS Container's Databases • 110
The MDS Manager's Databases • 110
The Need for Global Policies • 21, 73
The Need for Provider-1 • 8
The Provider-1 Trust Model • 25
The Trial Period • 40
To assign to many customers at one time • 103
To assign to one customer at a time • 102
To Change the Active MDS • 115
To Reassign/Install a Global Policy for a Specific Customer who already has been Assigned a Global Policy • 87
To Reassign/Install a Global Policy for Multiple Customers • 88
To Synchronize a Group of MDSs • 115
To Synchronize a Single MDS with an MDS Manager • 115
Tracking Logs using SmartView Tracker • 136
Traditional VPN • 98
Traffic Flow and Virtual Link Monitoring • 138
Trust Between a CLM and its Customer Network • 27
Trust Between a CMA and its Customer Network • 26
Trust Between MDS to MDS • 28

U

Using SmartConsole to Monitor Provider-1 Components • 136
Using SmartReporter • 126
Using the MDG for the First Time • 47
Using the MDG to Synchronize the MDSs • 113
Using Thresholds • 138
UTM-1 Edge Appliances • 93
UTM-1 Edge Processes • 145

V

Viewing Status Details • 130
Viewing the Customer's Global Policy History File • 89
Viewing the Status of Global Policy Assignments • 86